开发人员指南

AWS Config

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Config: 开发人员指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什么是 AWS Config？ 1
注意事项 1
使用方式 AWS Config 1
资源管理 1
审计与合规性 2
对配置更改进行管理与故障排除 2
安全分析 2
合作伙伴解决方案 2
功能 2
AWS Config 工作原理 3
资源发现 4
资源跟踪 4
配置项目的交付 5
控制对的访问权限 AWS Config 7
概念 8
AWS Config 接口 9
资源管理 9
配置记录器 10
传输通道 5
AWS Config 规则 11
合规包 13
聚合器 14
区域支持 15
Service Limits 19
AWS 服务集成 20
AWS Organizations 20
AWS Control Tower 21
AWS CloudTrail 21
AWS Security Hub 21
AWS Audit Manager 21
AWS Systems Manager 21
AWS Firewall Manager 22
Amazon EC2 专属主机 22
应用程序负载均衡器 22

AWS CodeBuild ... 22
AWS X-Ray ... 23
AWS 服务管理连接器 ... 23
Amazon API Gateway ... 23
补充信息 ... 23
AWS 软件开发套件适用于 AWS Config ... 24
开始使用 ... 26
报名参加 AWS ... 26
注册获取 AWS 账户 ... 26
创建具有管理访问权限的用户 ... 26
入门方法 AWS Config ... 28
设置 AWS Config （控制台） ... 28
设置 ... 28
一键设置 ... 29
手动设置 ... 31
设置 AWS Config (AWS CLI) ... 37
设置 ... 37
先决条件 ... 38
正在启动 AWS Config ... 97
验证 ... 106
使用 AWS 软件开发工具包 ... 107
配置记录器 ... 109
管理配置记录器 (控制台) ... 109
管理配置记录器 (AWS CLI) ... 110
配置记录器的偏离检测 ... 113
传输通道 ... 114
术语 ... 114
更新传递通道 ... 115
重命名传递通道 ... 119
配置项的组成部分 ... 120
传送配置快照 ... 121
交付配置快照 ... 121
示例配置快照来自 AWS Config ... 122
验证传送状态 ... 127
查看 Amazon S3 存储桶中的配置快照 ... 128
示例通知 ... 129

示例配置项变更通知 130
示例配置历史记录传输通知 144
示例配置快照传输开始通知 145
示例配置快照传输通知 146
示例合规性变更通知 147
示例规则评估开始通知 150
示例过大配置项变更通知 151
示例传输失败通知 152
资源管理 154
AWS Config 仪表板 154
合规性和资源清单 155
AWS Config 使用情况和成功指标 156
支持的资源类型 158
Amazon AppStream 159
Amazon AppFlow 159
..... 159
Amazon API Gateway 160
Amazon Athena 160
Amazon CloudFront 161
Amazon CloudWatch 161
Amazon CodeGuru 162
Amazon Cognito 163
Amazon Connect 163
Amazon Detective 164
Amazon DynamoDB 164
Amazon EC2 164
Amazon ECR 172
Amazon ECS 172
Amazon EFS 173
Amazon EKS 173
Amazon EMR 174
Amazon EventBridge 174
Amazon Forecast 175
Amazon Fraud Detector 176
Amazon GuardDuty 176
Amazon Inspector 177

Amazon IVS 177
Amazon Keyspaces 177
亚马逊 OpenSearch 服务 178
Amazon Personalize 178
Amazon Pinpoint 179
Amazon QLDB 180
Amazon Kendra 180
Amazon Kinesis 180
Amazon Lex 181
Amazon Lightsail 182
Amazon Lookout for Metrics 182
Amazon Lookout for Vision 182
Amazon Managed Grafana 183
Amazon Managed Service for Prometheus 183
适用于 Redis 的 Amazon MemoryDB 183
Amazon MQ 183
Amazon MSK 184
Amazon Redshift 184
Amazon RDS 186
Amazon Route 53 187
Amazon SageMaker 188
Amazon SES 189
Amazon SNS 190
Amazon SQS 190
Amazon S3 190
Amazon WorkSpaces 192
AWS Amplify 192
AWS AppConfig 193
AWS App Runner 194
AWS App Mesh 194
AWS AppSync 195
AWS Audit Manager 195
AWS Auto Scaling 195
AWS Backup 196
AWS Batch 197
AWS Budgets 197

AWS Certificate Manager 198
AWS CloudFormation 198
AWS CloudTrail 198
AWS Cloud9 198
AWS Cloud Map 199
AWS CodeArtifact 199
AWS CodeBuild 200
AWS CodeDeploy 200
AWS CodePipeline 201
AWS Config 201
AWS DMS 202
AWS DataSync 203
AWS Device Farm 204
AWS Elastic Beanstalk 205
AWS FIS 205
AWS Global Accelerator 206
AWS Glue 206
AWS Ground Station 207
AWS HealthLake 207
AWS IAM 207
AWS IoT 209
AWS KMS 212
AWS Lambda 213
AWS Mainframe Modernization 213
AWS Network Firewall 213
AWS Network Manager 214
AWS Panorama 215
AWS Private CA 215
AWS Resilience Hub 216
AWS 资源探索器 216
AWS RoboMaker 217
AWS Signer 217
AWS Secrets Manager 217
AWS Service Catalog 218
AWS Shield 218
AWS Step Functions 219

AWS Systems Manager 219
AWS Transfer Family 220
AWS WAF 220
AWS X-Ray 222
Elastic Load Balancing 222
MediaConnect 223
MediaPackage 224
MediaTailor 224
按区域可用性列出的资源覆盖范围 225
北美洲和南美洲 225
欧洲 295
亚太地区 351
中国 405
非洲和中东 440
GovCloud 487
录制 AWS 资源 531
注意事项 531
区域性资源和全局资源 532
记录资源（控制台） 535
录制资源 (AWS CLI) 538
记录频率 552
停止记录 553
未记录的资源 553
AWS Config 规则和全局资源类型 554
记录第三方资源 555
步骤 1：设置开发环境 556
步骤 2：资源建模 556
步骤 3：生成构件 558
步骤 4：注册资源 558
步骤 5：发布资源配置 558
使用记录和删除第三方资源的配置状态 AWS CLI 559
使用 API 管理第三方资源类型的配置状态 561
录制软件配置 562
管理记录的 资源 564
资源清单 564
合规信息和评估结果 566

配置和合规性历史记录 578
标记您的资源 586
与标记相关的限制 587
使用 AWS Config API 操作管理标签 587
AWS Config 规则 588
与成本相关的注意事项 589
区域支持 590
规则的组成部分 595
规则元数据 596
规则结构 597
评估模式 614
触发器类型 614
评估模式 615
规则评估 619
托管规则 619
与成本相关的注意事项 589
触发器类型 620
评估模式 621
托管规则的列表 622
按评估模式划分的托管规则列表 905
按触发器类型划分的托管规则列表 921
按区域可用性列出的托管规则列表 936
服务相关规则 1272
使用 AWS CloudFormation 模板创建托管规则 1273
自定义规则 1275
自定义策略规则 1275
自定义 Lambda 规则 1275
与成本相关的注意事项 589
触发器类型 1276
评估模式 1277
管理已删除的资源 1278
创建自定义策略规则 1279
创建自定义 Lambda 规则 1282
添加、更新和删除规则 1312
使用 控制台 1312
使用 AWS 软件开发工具包 1318

使用 Security Hub 1329
使用规则评估资源 1330
删除评估结果 1334
删除评估结果（控制台） 1334
删除评估结果 (CLI) 1334
删除评估结果 (API) 1334
管理组织规则 1335
注意事项 1335
部署 1336
区域支持 1336
修复 1339
先决条件 1339
设置手动修正（控制台） 1339
设置自动修正（控制台） 1340
删除修正操作（控制台） 1341
管理修正 (API) 1342
区域支持 1343
故障排除 1346
合规包 1348
先决条件 1348
开始 AWS Config 录制 1348
将一致性包与修正结合使用的先决条件 1349
使用带有一条或多 AWS Config 条规则的一致性包的先决条件 1349
Organization 一致性包的先决条件 1352
区域支持 1353
流程检查 1358
用于创建流程检查的样本合规包模板 1359
在合规包中包括流程检查 1359
更改流程检查的合规性状态 1360
查看和编辑流程检查（控制台） 1361
一致性包示例模板 1362
AWS Control Tower 探测防护机制合规包 1366
ABS CCIG 2.0 重要工作负载操作最佳实践 1366
ABS CCIG 2.0 标准工作负载操作最佳实践 1498
ACSC Essential 8 操作最佳实践 1597
ACSC ISM 操作最佳实践 1611

人工智能和机器学习操作最佳实践 1692
Amazon API Gateway 操作最佳实践 1692
Amazon 最佳运营实践 CloudWatch 1692
Amazon DynamoDB 操作最佳实践 1692
Amazon S3 操作最佳实践 1692
APRA CPG 234 操作最佳实践 1692
资产管理操作最佳实践 1832
AWS Backup操作最佳实践 1832
AWS Identity And Access Management 操作最佳实践 1832
Well-Architecte AWS d 框架可靠性支柱的运营最佳实践 1832
Well-Architecte AWS d Framework 安全支柱的运营最佳实践 1868
BCP 和 DR 操作最佳实践 1971
BNM RMiT 操作最佳实践 1972
加拿大网络安全中心 (CCCS) Medium Cloud Control Profile 操作最佳实践 2142
CIS AWS 基金会运营最佳实践基准 v1.4 第 1 级 3051
CIS AWS 基金会运营最佳实践基准 v1.4 第 2 级 3075
CIS 关键安全控制 v8 IG1 操作最佳实践 3108
CIS 关键安全控制 v8 IG2 操作最佳实践 3163
CIS 关键安全控制 v8 IG3 操作最佳实践 3261
CIS Top 20 操作最佳实践 3366
CISA 网络基本要素操作最佳实践 3415
刑事司法信息服务 (CJIS) 操作最佳实践 3530
CMMC Level 1 操作最佳实践 3606
CMMC Level 2 操作最佳实践 3674
CMMC Level 3 操作最佳实践 3847
CMMC Level 4 操作最佳实践 4099
CMMC Level 5 操作最佳实践 4372
CMMC 2.0 Level 1 操作最佳实践 4684
CMMC 2.0 Level 2 操作最佳实践 4751
计算服务操作最佳实践 4987
数据弹性操作最佳实践 4987
数据库服务操作最佳实践 4987
数据湖和分析服务操作最佳实践 4987
DevOps 操作最佳实践 4987
EC2 操作最佳实践 4988
加密和密钥管理操作最佳实践 4988

适用于 SME 的 ENISA 网络安全指南操作最佳实践 4988
Esquema Nacional de Seguridad (ENS) Low 操作最佳实践 5098
Esquema Nacional de Seguridad (ENS) Medium 操作最佳实践 5164
Esquema Nacional de Seguridad (ENS) High 操作最佳实践 5239
FDA 联邦法规第 21 篇第 11 部分操作最佳实践 5320
FedRAMP(Low) 操作最佳实践 5531
FedRAMP(Moderate) 操作最佳实践 5683
FFIEC 操作最佳实践 6003
德国云计算合规性条件目录 (C5) 操作最佳实践 6133
《格雷姆-里奇-布里利法案》(GLBA) 操作最佳实践 6183
GxP 欧盟附件 11 操作最佳实践 6210
HIPAA 安全操作最佳实践 6298
IRS 1075 操作最佳实践 6587
K-ISMS 操作最佳实践 6702
负载平衡操作最佳实践 6754
日志记录操作最佳实践 6754
管理和治理服务操作最佳实践 6755
MAS 第 655 号通知操作最佳实践 6755
MAS TRMG 操作最佳实践 6779
监控操作最佳实践 6916
NBC TRMG 操作最佳实践 6916
NERC CIP BCSI 操作最佳实践 7186
NCSC 云安全原则操作最佳实践 7216
NCSC 网络评估框架操作最佳实践 7280
联网和内容交付服务操作最佳实践 7385
NIST 800-53 rev 4 操作最佳实践 7386
NIST 800-53 rev 5 操作最佳实践 7573
NIST 800 171 操作最佳实践 8037
NIST 800 172 操作最佳实践 8236
NIST 800 181 操作最佳实践 8277
NIST 1800 25 操作最佳实践 8578
NIST CSF 操作最佳实践 8678
NIST 隐私框架 v1.0 操作最佳实践 8897
NYDFS 23 操作最佳实践 9042
NZISM 操作最佳实践 9150
PCI DSS 3.2.1 操作最佳实践 9200

可公开访问资源操作最佳实践 9441
印度储备银行 UCB 网络安全框架操作最佳实践 9441
RBI MD-ITF 操作最佳实践 9472
安全性、身份和合规性操作最佳实践 9559
无服务器操作最佳实践 9559
存储服务操作最佳实践 9560
SWIFT CSP 操作最佳实践 9560
Amazon Elastic Container Service (Amazon ECS) 安全最佳实践 9582
Amazon Elastic File System (Amazon EFS) 安全最佳实践 9582
Amazon Elastic Kubernetes Service (Amazon EKS) 安全最佳实践 9583
Amazon 安全最佳实践 CloudFront 9583
Amazon OpenSearch 服务安全最佳实践 9583
Amazon Redshift 安全最佳实践 9583
Amazon Relational Database Service (Amazon RDS) 安全最佳实践 9583
AWS Auto Scaling安全最佳实践 9584
AWS CloudTrail安全最佳实践 9584
AWS CodeBuild安全最佳实践 9584
Amazon ECR 安全最佳实践 9584
AWS Lambda安全最佳实践 9585
AWS Network Firewall安全最佳实践 9585
Amazon 安全最佳实践 SageMaker 9585
AWS Secrets Manager安全最佳实践 9585
AWS WAF安全最佳实践 9585
具有修正操作的示例模板 9586
自定义合规包 9586
术语 9586
自定义模板 9586
部署自定义合规包 9591
“合规包”控制面板 9591
浏览合规包主页 9591
了解更多信息 9592
查看合规性历史记录 9592
查看合规性时间线 9592
查询合规性历史记录 9593
部署合规包（控制台） 9595
使用模板部署合规包 9595

编辑一致性包 9596
删除一致性包 9596
部署一致性包 (AWS CLI) 9597
部署一致性包 9597
查看一致性包 9599
查看一致性包状态 9599
查看一致性包的合规状态 9600
获取特定一致性包的合规详细信息 9600
删除一致性包 9601
管理合规包 (API) 9602
管理组织合规包 9602
注意事项 9602
部署 9603
区域支持 9604
故障排除 9606
一致性包的失败状态 9606
一致性包中的悬挂规则 9607
聚合器 9609
应用场景 9609
术语 9610
如何聚合数据 9610
区域支持 9611
故障排除 9614
聚合器控制面板 9615
使用聚合器控制面板 9615
合规性控制面板 9618
清单控制面板 9619
设置聚合器 (控制台) 9621
创建聚合器 9621
编辑聚合器 9623
删除聚合器 9623
设置聚合器 (AWS CLI) 9624
使用个人账户添加聚合器 9624
使用 AWS Organizations 添加聚合器 9626
注册委派管理员 9627
查看聚合器 9629

编辑聚合器 9630
删除聚合器 9631
授权聚合器账户 (控制台) 9632
注意事项 9632
为聚合器账户和区域添加授权 9632
授权针对聚合器账户的待处理请求 9633
删除对现有聚合器账户的授权 9633
授权聚合器账户 (AWS CLI) 9634
注意事项 9634
为聚合器账户和区域添加授权 9635
删除授权账户 9635
高级查询 9636
功能 9636
查询组件 9637
摘要 9637
参数 9637
示例 9637
示例查询 9638
关系查询示例 9644
限制 9645
区域支持 9648
查询编辑器（控制台） 9651
注意事项 9651
使用 AWS 示例查询 9652
创建您的自定义查询 9652
查询编辑器 (AWS CLI) 9653
注意事项 9653
查询资源配置数据 9654
保存查询 9656
查看所有已保存的查询 9656
获取已保存的查询的详细信息 9657
删除已保存的查询 9657
自然语言查询处理器 9658
注意事项 9658
使用自然语言查询处理器进行查询 9652
提示示例 9659

提供反馈 9663
区域支持 9663
删除 数据 9664
设置数据保留期（控制台） 9666
安全性 9667
数据保护 9667
传输中的数据的加密 9668
传输中的数据的加密 9668
Identity and Access Management 9668
受众 9669
使用身份进行身份验证 9669
使用策略管理访问 9672
如何 AWS Config 与 IAM 配合使用 9674
基于身份的策略示例 9680
AWS 托管策略 9697
IAM 角色的权限 9833
更新 IAM 角色 9837
亚马逊 S3 存储桶的权限 9838
KMS 密钥的权限 9842
Amazon SNS 主题的权限 9844
故障排除 9847
使用服务相关角色 9849
事件响应 9851
合规性验证 9851
弹性 9852
基础架构安全性 9852
配置和脆弱性分析 9853
防止跨服务混淆座席 9853
最佳实操 9853
日志记录和监控 9855
日志记录 9855
AWS Config 中的信息 CloudTrail 9855
了解 AWS Config 日志文件条目 9856
示例日志文件 9856
监控 9864
使用 Amazon SQS 9864

使用亚马逊 EventBridge 9866
Amazon VPC 端点 9871
为创建 VPC 终端节点 AWS Config 9871
常见问题解答 9872
看不到我最新的配置更改 9872
我可以立即查看我的配置更改吗？ 9872
中的间接关系 AWS Config 9872
什么是资源关系？ 9872
什么是与资源的直接关系和间接关系？ 9873
AWS Config 支持哪些间接关系？ 9873
由于直接关系和间接关系，配置项是如何创建的？ 9875
由于间接关系而生成的配置项有哪些？ 9875
如何检索与间接关系相关的配置数据？ 9876
代码示例 9878
操作 9878
DeleteConfigRule 9879
DescribeComplianceByConfigRule 9881
DescribeComplianceByResource 9883
DescribeConfigRuleEvaluationStatus 9884
DescribeConfigRules 9886
DescribeConfigurationRecorderStatus 9889
DescribeConfigurationRecorders 9891
DescribeDeliveryChannels 9892
GetComplianceDetailsByConfigRule 9893
GetComplianceDetailsByResource 9896
GetComplianceSummaryByConfigRule 9897
GetComplianceSummaryByResourceType 9899
PutConfigRule 9901
PutDeliveryChannel 9905
文档历史记录 9907
早期更新 9997
..... 10050

什么是 AWS Config？

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

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

注意事项

- AWS 账户: 你需要一个活跃 AWS 账户的。有关更多信息，请参阅注册 AWS。
- Amazon S3 存储桶：您需要一个 S3 存储桶才能接收配置快照和历史记录的数据。有关更多信息，请参阅 Amazon S3 存储桶的权限。
- Amazon SNS 主题：当您的配置快照和历史记录发生变化时，您需要一个 Amazon SNS 才能收到通知。有关更多信息，请参阅 Amazon SNS 主题的权限。
- IAM 角色：您需要一个具有必要访问权限的 IAM 角色 AWS Config。有关更多信息，请参阅 IAM 角色的权限。
- 资源类型：您可以决定 AWS Config 要记录哪些资源类型。有关更多信息，请参阅录制 AWS 资源。

使用方式 AWS Config

在上运行应用程序时 AWS，通常会使用 AWS 资源，而这些资源必须共同创建和管理。随着对应用程序的需求不断增长，您跟踪 AWS 资源的需求也在不断增长。 AWS Config 旨在帮助您在以下情况下监督应用程序资源：

资源管理

为了更好地管理您的资源配置并检测资源的错误配置，您需随时详细了解存在哪些资源以及这些资源的配置方式。无论何时创建、修改或删除资源，您都可以使用 AWS Config 通知您，而不必通过轮询对每个资源的调用来监控这些更改。

您可以使用 AWS Config 规则来评估 AWS 资源的配置设置。当 AWS Config 检测到某个资源违反了您的某条规则中的条件时，会将该资源 AWS Config 标记为不合规并发送通知。 AWS Config 在创建、更改或删除您的资源时持续对其进行评估。

审计与合规性

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

对配置更改进行管理与故障排除

当您使用相互依赖的多个 AWS 资源时，更改一个资源的配置可能会对相关资源产生意想不到的后果。使用 AWS Config，您可以查看您打算修改的资源与其他资源的关系，并评估更改的影响。

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

安全分析

要分析潜在的安全漏洞，您需要有关 AWS 资源配置的详细历史信息，例如授予用户的 AWS Identity and Access Management (IAM) 权限，或控制资源访问权限的 Amazon EC2 安全组规则。

您可以使用 AWS Config 查看在任何时候分配给用户、群组或角色的 IAM 策略，该策略 AWS Config 正在记录中。这一信息可以帮助您确定用户在特定时间内具备的权限：例如，您可以查看用户 John Doe 在 2015 年 1 月 1 日是否拥有修改 Amazon VPC 设置的权限。

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

合作伙伴解决方案

AWS 与第三方日志和分析专家合作，提供使用 AWS Config 输出的解决方案。欲了解更多信息，请访问 AWS Config 详情页面，网址为AWS Config。

功能

设置后 AWS Config，您可以完成以下操作：

资源管理

- 指定 AWS Config 要记录的资源类型。

- 设置 Amazon S3 桶以接收配置快照（按需）和配置历史记录。

- 设置 Amazon SNS 以发送配置流通知。
- 授予 AWS Config 其访问 Amazon S3 存储桶和 Amazon SNS 主题所需的权限。

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

规则和合规包

- 指定要 AWS Config 用来评估所记录资源类型的合规性信息的规则。
- 使用一致性包或一系列可作为单个实体部署和监控的 AWS Config 规则和补救措施。 AWS 账户

  有关更多信息，请参阅使用 AWS Config 规则和一致性包评估资源。

聚合器

- 使用聚合器集中查看您的资源清单和合规性。聚合器将来自多个 AWS 账户 和 AWS 地区的 AWS Config 配置和合规性数据收集到单个账户和区域中。

  有关更多信息，请参阅多账户多区域数据聚合。

高级查询

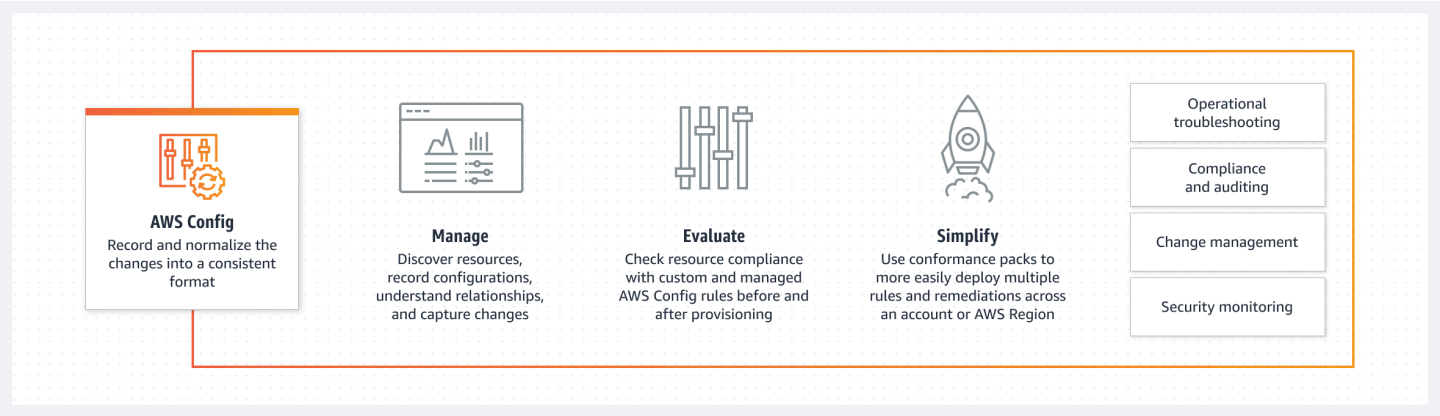
- 使用其中一个示例查询，或者参考 AWS 资源的配置架构编写自己的查询。

  有关更多信息，请参阅查询 AWS 资源的当前配置状态。

AWS Config 工作原理

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

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



资源发现

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

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

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

资源跟踪

AWS Config 通过对账户中的每个资源调用 Describe 或 List API 调用，跟踪资源的所有更改。该服务使用相同的 API 调用来捕获所有相关资源的配置详细信息。

例如，从 VPC 安全组中移除出口规则会导致 AWS Config 在该安全组上调用 Describe API 调用。AWS Config 然后在与安全组关联的所有实例上调用 Describe API 调用。安全组（资源）以及每个实例（相关资源）的更新后配置将被记录为配置项，并以配置流的形式传送到 Amazon Simple Storage Service (Amazon S3) 存储桶。

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

如果您使用的是 AWS Config 规则，请 AWS Config 持续评估您的 AWS 资源配置以确定所需的设置。根据规则， AWS Config 将根据配置更改或定期评估您的资源。每个规则都与一个 AWS Lambda 函

数关联，其中包含规则的评估逻辑。在 AWS Config 评估您的资源时，它会调用规则的函数。 AWS Lambda 该函数会返回被评估资源的合规性状态。如果资源违反了规则的条件，则会将该资源和规则 AWS Config 标记为不合规。当资源的合规状态发生变化时， AWS Config 会向您的 Amazon SNS 主题发送通知。

配置项目的交付

AWS Config 可以通过以下渠道之一交付配置项目：

Amazon S3 存储桶

AWS Config 跟踪 AWS 资源配置的变化，并定期将更新的配置详细信息发送到您指定的 Amazon S3 存储桶。对于每种 AWS Config 记录的资源类型，它每六小时发送一次配置历史记录文件。每个配置历史记录文件中都包含前 6 小时内发生更改的资源的详细信息。每个文件均包含一种类型的资源，例如 Amazon EC2 实例或 Amazon EBS 卷。如果没有发生配置更改，则 AWS Config 不发送文件。

AWS Config 当您在 CLI 中使用 d eliver-config-snapshot 命令或在 AP AWS I 中使用快照操作时，会将配置DeliverConfig快照发送到您的 Amazon S3 存储桶。 AWS Config 配置快照包含 AWS Config 记录在中的所有资源的配置详细信息 AWS 账户。配置历史记录文件和配置快照均采用 JSON 格式。

> **Note**
>
> AWS Config 仅将配置历史文件和配置快照传送到指定的 S3 存储桶； AWS Config 不会修改 S3 存储桶中对象的生命周期策略。您可以使用生命周期策略指定是删除对象，还是将对象存档到 Amazon S3 Glacier。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的管理生命周期配置。您还可以查看将 Amazon S3 数据存档到 S3 Glacier 博客文章。

Amazon SNS 主题

Amazon Simple Notification Service (Amazon SNS) 主题是一个沟通渠道，Amazon SNS 使用它将消息（或通知）传送到订阅端点，例如电子邮箱地址或客户端。其他类型的 Amazon SNS 通知包括传送到手机应用程序上的推送通知消息、传送到支持短信服务功能的手机上的短信服务 (SMS) 通知以及 HTTP POST 请求。为了获得最佳效果，请使用 SQS 作为 SNS 主题的通知端点，然后以编程方式处理通知中的信息。

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

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

通知可以是以下任何一种消息类型。

消息类型	描述
ComplianceChange通知	AWS Config 评估的资源的合规性类型已更改。合规性类型表示资源是否符合特定 AWS Config 规则，它由消息中的`ComplianceType` 密钥表示。消息中包含 `newEvaluationResult` 和 `oldEvaluationResult` 对象，以便进行比较。
ConfigRulesEvaluationStarted	AWS Config 已开始根据指定资源评估您的规则。
ConfigurationSnapshotDeliveryStarted	AWS Config 已开始将配置快照传送到您的 Amazon S3 存储桶。Amazon S3 存储桶的名称是为消息中的 `s3Bucket` 键提供的。
ConfigurationSnapshotDeliveryCompleted	AWS Config 已成功将配置快照传送到您的 Amazon S3 存储桶。
ConfigurationSnapshotDeliveryFailed	AWS Config 未能将配置快照传送到您的 Amazon S3 存储桶。
ConfigurationHistoryDeliveryCompleted	AWS Config 已成功将配置历史记录传送到您的 Amazon S3 存储桶。
ConfigurationItemChangeNotification	某个资源的已被创建、删除或更改配置。此消息包括为此更改 AWS Config 创建的配置项目的详细信息，还包括更改的类型。上述通知均在发生更改后的几分钟内传送，统称为配置流。
OversizedConfigurationItemChange通知	当配置项变更通知超出了 Amazon SNS 允许的最大大小时，会传送此消息类型。消息中包括配置项摘要。除短信外，Amazon SNS 消息最多可以包含 256 KB 的文本数据，包括

消息类型	描述
	XML、JSON 和未格式化的文本。您可以在指定的 Amazon S3 存储桶位置查看完整通知。
OversizedConfigurationItemChangeDeliveryFailed	AWS Config 未能将超大配置项目变更通知传送到您的 Amazon S3 存储桶。

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

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

控制对的访问权限 AWS Config

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

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

概念

AWS Config 提供了与您关联的资源的详细视图 AWS 账户，包括它们的配置方式、它们之间的关系，以及配置及其关系如何随着时间的推移而发生变化。让我们详细了解一下 AWS Config的概念。

目录

- AWS Config 接口
  - AWS Config 控制台
  - AWS Config CLI
  - AWS Config API
  - AWS Config 软件开发工具包
- 资源管理
  - AWS Resources
  - 资源关系
- 配置记录器
- 传输通道
  - 配置项
  - 配置历史
  - 配置快照
  - 配置流
- AWS Config 规则
  - AWS Config 托管规则
  - AWS Config 自定义规则
  - 触发器类型
  - 评估模式
- 合规包
- 多账户多区域数据聚合
  - 源账户
  - 源区域
  - 聚合器
  - 聚合器账户
  - 授权

AWS Config 接口

AWS Config 控制台

您可以使用 AWS Config 控制台管理服务。有关更多信息 AWS Management Console，请参阅AWS Management Console。

AWS Config CLI

AWS Command Line Interface 是一个统一的工具，可用于 AWS Config 从命令行与之交互。有关更多信息，请参阅 AWS Command Line Interface 《用户指南》。有关 C AWS Config LI 命令的完整列表，请参阅可用命令。

AWS Config API

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

AWS Config 软件开发工具包

除了使用 AWS Config API 之外，您还可以使用其中一个 AWS SDK。每个软件开发工具包均包含适用于各种编程语言和平台的库和示例代码。这些开发工具包提供了一种简便方法，以使用编程方式访问 AWS Config。例如，您可以使用开发工具包以加密方式对请求进行签名，管理错误并自动重试请求。有关更多信息，请参阅用于 Amazon Web Services 的工具页面。

资源管理

了解的基本组成部分 AWS Config 将有助于您跟踪资源清单和更改，并评估 AWS 资源的配置。

AWS Resources

AWS 资源是您使用、 AWS Command Line Interface (CLI) AWS Management Console、 AWS 软件开发工具包或 AWS 合作伙伴工具创建和管理的实体。 AWS 资源示例包括亚马逊 EC2 实例、安全组、亚马逊 VPC 和亚马逊弹性区块存储。 AWS Config 使用其唯一标识符来指代每种资源，例如资源 ID 或 A mazon 资源名称 (ARN)。有关 AWS Config 支持的资源类型的列表，请参阅支持的资源类型。

资源关系

AWS Config 发现您账户中的 AWS 资源，然后创建 AWS 资源之间的关系图。例如，关系可能包括附加到与安全组 `sg-ef678hk` 关联的 Amazon EC2 实例 `i-a1b2c3d4` 的 Amazon EBS 卷 `vol-123ab45d`。

有关更多信息，请参阅 支持的资源类型。

配置记录器

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

默认情况下，配置记录器会记录 AWS Config 正在运行的区域中所有支持的资源。您可以创建一个自定义配置记录器，仅记录您指定的资源类型。有关更多信息，请参阅 录制 AWS 资源。

如果您使用 AWS Management Console 或 CLI 开启服务，则 AWS Config 会自动为您创建并启动配置记录器。

传输通道

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

配置项

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

有关更多信息，请参阅Components of a Configuration Item和选择所记录的资源 | 记录频率。

配置历史

配置历史记录是指定资源在某个时间段的配置项集合。配置历史记录包含多种信息，例如资源首次创建的时间、过去一个月的资源配置情况以及昨天上午 9 点发生了哪些配置更改等。配置历史记录有多种格式可供您使用。 AWS Config 自动将正在记录的每种资源类型的配置历史记录文件传输到您指定的 Amazon S3 存储桶。您可以在 AWS Config 控制台中选择给定资源，然后使用时间轴导航到该资源的所有先前配置项目。此外，您还可以从 API 访问资源的历史配置项。

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

配置快照

配置快照是您账户中受支持资源的配置项的集合。配置快照可以完整展示被记录的资源及其配置的相关信息。配置快照是验证您的配置的有效工具。例如，您可以定期检查配置快照，以便找出配置错误

的资源或可能不应存在的资源。配置快照具有多种格式。您可以将配置快照传输到您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶。此外，您还可以在 AWS Config 控制台中选择一个时间点，并使用资源之间的关系浏览配置项目的快照。

配置流

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

AWS Config 规则

AWS Config 规则代表您为特定 AWS 资源或整个资源所需的配置设置 AWS 账户。如果资源未通过规则检查，则将该资源和规则 AWS Config 标记为不合规，并通过 Amazon SNS AWS Config 通知您。以下是 AWS Config 规则可能的评估结果：

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

有两种类型的规则： AWS Config 托管规则和 AWS Config 自定义规则。有关规则定义和规则元数据结构的更多信息，请参阅AWS Config 规则的组成部分。

AWS Config 托管规则

AWS Config 托管规则是由创建的预定义的、可自定义的规则 AWS Config。有关托管规则的列表，请参阅 AWS Config 托管规则列表。

AWS Config 自定义规则

AWS Config 自定义规则是您从头开始创建的规则。有两种方法可以创建 AWS Config 自定义规则：使用 Lambda 函数（AWS Lambda 开发者指南）和使用 Guard（Guard GitHub存储库）（一种 policy-as-code 语言）。 AWS Config 使用创建的 AWS Lambda 自定义规则称为AWS Config 自定义 Lambda 规则，使用 Guard 创建的 AWS Config 自定义规则称为AWS Config 自定义策略规则。

有关如何创建 AWS Config 自定义策略规则的演练，请参阅创建 AWS Config 自定义策略规则。有关如何创建自定义 Lambda 规则的演练，请参阅 AWS Config 创建 AWS Config 自定义 Lamb da 规则。

触发器类型

向账户添加规则后， AWS Config 将您的资源与规则的条件进行比较。在这次初始评估之后，每次触发评估时都会 AWS Config 继续运行评估。评估触发器被定义为规则的一部分，它们可以包括以下类型。

触发器类型	描述
配置更改	AWS Config 当存在与规则范围匹配的资源并且资源的配置发生变化时，会对规则进行评估。评估将在 AWS Config 发送配置项目变更通知后运行。 通过定义规则的范围来选择哪些资源启动评估。范围可以包括： • 一个或多个资源类型 • 资源类型和资源 ID 的组合 • 标签键和值的组合 • 当创建、更新或删除任何记录的资源时 AWS Config 当它检测到与规则范围相匹配的资源发生变化时，就会运行评估。您可以使用范围来定义哪些资源启动评估。
定期	AWS Config 按您选择的频率对规则进行评估；例如，每 24 小时运行一次。
混合	有些规则既有配置更改也有定期触发器。对于这些规则，它 AWS Config 会在检测到配置更改时以及按照您指定的频率评估您的资源。

评估模式

AWS Config 规则有两种评估模式。

评估模式	描述
主动	使用主动评估在资源部署之前对其进行评估。这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。 有关更多信息，请参阅评估模式。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。
侦查	使用侦查评估来评估已部署的资源。这允许您评估现有资源的配置设置。

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

合规包

一致性包是 AWS Config 规则和补救措施的集合，可以轻松地将其作为单个实体部署到一个账户和一个区域或整个组织中 AWS Organizations。

通过编写一个包含 AWS Config 规则（托管或自定义）和修复操作列表的 YAML 模板，可以创建一致性包。您可以使用 AWS Config 控制台或 AWS CLI部署模板。

要快速入门并评估您的 AWS 环境，请使用其中一个样本一致性包模板。您也可以基于自定义合规包，从头开始创建合规包 YAML 文件。自定义一致性包是唯一的 AWS Config 规则和补救措施集合，您可以将它们一起部署到一个账户和一个 AWS 区域，或者跨组织部署。 AWS Organizations

流程检查是一种 AWS Config 规则，允许您跟踪需要作为一致性包一部分进行验证的外部和内部任务。可以将这些检查添加到现有合规包或新的合规包中。您可以在一个位置跟踪所有合规性，包括 AWS Config持续时间和手动检查。

多账户多区域数据聚合

中的多账户多区域数据聚合 AWS Config 允许您将来自多个账户和地区的 AWS Config 配置和合规性数据聚合到一个账户中。多账户多区域数据聚合对于中央 IT 管理员监控企业 AWS 账户 中多个账户的合规性非常有用。使用聚合器不会产生任何额外费用。

源账户

源账户是您要 AWS 账户 从中汇总 AWS Config 资源配置和合规性数据的账户。源账户可以是 AWS Organizations中的个人账户或组织。您可以单独提供源帐户，也可以通过它们进行检索 AWS Organizations。

源区域

来源区域是您要从中汇总 AWS Config 配置和合规性数据的 AWS 区域。

聚合器

聚合器从多个来源账户和区域收集 AWS Config 配置和合规性数据。在要查看聚合 AWS Config 配置和合规性数据的区域中创建聚合器。

> **Note**
>
> 聚合器通过将数据从源账户复制到聚合器账户，提供对源账户和区域的只读视图，聚合器有权查看这些账户和区域。聚合器不提供对源账户或区域的变更访问权限。例如，这意味着您不能通过聚合器部署规则，也不能通过聚合器将快照文件推送到源账户或区域。

聚合器账户

聚合账户是您在其中创建聚合器的账户。

授权

作为源账户所有者，授权是指您向聚合器账户和区域授予的收集 AWS Config 配置和合规性数据的权限。如果要聚合的源账户是 AWS Organizations的一部分，则不需要授权。

区域支持

> **Note**
>
> 的某些功能 AWS Config 仅在支持的部分 AWS 区域中 AWS Config 受支持。
>
> 资源管理
>
> - 有关哪些区域支持哪些 AWS 资源类型的列表，请参阅按区域可用性划分的资源覆盖率。
>
> AWS Config 规则
>
> - 有关哪些区域支持哪些 AWS Config 规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。
> - 有关支持组织部署规则的区域列表，请参阅组织 AWS Config 规则 | Region Suppor t。
> - 有关支持 AWS Config 规则修正操作的区域列表，请参阅修正操作 | Region Supp ort。
>
> 合规包
>
> - 有关支持合规包和组织部署合规包的区域列表，请参阅合规包 | 区域支持。
>
> 聚合器
>
> - 有关支持聚合器的区域列表，请参阅聚合器 | 区域支持。
>
> 高级查询
>
> - 有关支持高级查询的区域列表，请参阅高级查询 | 区域支持。
> - 有关支持适用于高级查询的自然语言查询处理器的区域列表，请参阅适用于高级查询的自然语言查询处理器 | 区域支持。

下表列出了您可以启用的 AWS 区域 AWS Config。

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

区域名称	区域	端点	协议
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

Service Limits

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

有关 AWS 中的其他限制的信息，请参阅 AWS 服务限制。

AWS Config 服务限制

描述	限制值	能否增加
最大 AWS Config 规则数（每个区域、每个账户）	1000	否
每个资源的最大标签数	50	不可以

单个账户一致性包

描述	限制值	能否增加
每个账户的最大一致性包数	50	不可以
每个一致性包最多 AWS Config 条规则	130	否

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

组织一致性包

描述	限制值	能否增加
每个组织的最大一致性包数	50	不可以
每个组织一致性包的最大 AWS Config 规则数	130	否

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

聚合器

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

高级查询

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

AWS 服务集成 AWS Config

AWS Config 支持与其他几项 AWS 服务的集成。

AWS Organizations

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

AWS Control Tower

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

AWS CloudTrail

AWS Config 与集成 AWS CloudTrail ，将配置更改与您账户中的特定事件相关联。您可以使用 CloudTrail 日志来获取引发变更的事件的详细信息，包括谁发出了请求、何时以及来自哪个 IP 地址。您可以从 CloudTrail 控制台导航到 AWS Config 时间轴，查看与您的 AWS API 活动相关的配置更改。

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

AWS Security Hub

AWS Security Hub 集中来自其他 AWS 服务（包括 AWS Config 规则）的安全检查。Security Hub 启用并控制 AWS Config 规则，以验证您的资源配置是否符合最佳实践。 AWS Config 在 Security Hub 要对环境资源进行安全检查的所有区域的所有账户上启用。有关更多信息，请参阅AWS Security Hub 用户指南中的向 Sec urity Hub 发送调查结果的AWS 服务。

AWS Audit Manager

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

AWS Systems Manager

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

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

AWS Firewall Manager

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

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

Amazon EC2 专属主机

AWS Config 与 Amazon EC2 专用主机集成以评估许可证合规性。 AWS Config 记录实例何时在专用主机上启动、停止或关闭，并将此信息与与软件许可相关的主机和实例级别信息（例如主机 ID、Amazon 机器映像 (AMI) ID、套接字数量和物理内核）配对。这可以帮助您 AWS Config 用作许可证报告的数据源。您可以从 Amazon EC2 专用主机控制台导航到 AWS Config 时间轴，查看您的 Amazon EC2 专用主机的配置更改。

有关更多信息，请参阅 Linux 实例的亚马逊弹性计算云用户指南中的跟踪配置更改或适用于 Windows 实例的亚马逊弹性计算云用户指南中的跟踪配置更改。

应用程序负载均衡器

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

AWS CodeBuild

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

AWS X-Ray

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

AWS 服务管理连接器

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

Amazon API Gateway

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

补充信息和相关资源

下列相关资源在您使用此服务的过程中会有所帮助。

- AWS Config— 有关信息的主要网页 AWS Config。
- AWS Config 定价
- 技术方面常见问题
- AWS Config 规则开发套件 (RDK) — 一种开源工具，可帮助您设置 AWS Config、编写规则，然后使用各种 AWS 资源类型对其进行测试。
- 合作伙伴 — 指 AWS Config 向与之完全集成的合作伙伴产品的链接，可帮助您可视化、监控和管理配置流、配置快照或配置历史记录中的数据。

- 课程和研讨会 — 指向基于角色的课程和专业课程的链接，以及自定进度的实验室，可帮助您提高 AWS 技能并获得实践经验。
- AWS 开发者中心 — 浏览教程、下载工具并了解 AWS 开发者活动。
- AWS 开发者工具-指向开发者工具、SDK、IDE 工具包和命令行工具的链接，用于开发和管理 AWS 应用程序。
- 入门资源中心 — 了解如何设置你的 AWS 账户、加入 AWS 社区和启动你的第一个应用程序。

- 动手教 step-by-step 程 — 按照教程启动您的第一个应用程序 AWS。
- AWS 白皮书 — 由 AWS 解决方案架构师或其他技术专家撰写的技术 AWS 白皮书完整列表的链接，这些白皮书涵盖架构、安全和经济学等主题。
- AWS Support 中心 — 创建和管理 AWS Support 案例的中心。还包括指向其他有用资源的链接，例如论坛、技术常见问题解答、服务运行状况和 AWS Trusted Advisor。
- AWS Support— 提供有关 AWS Support快速响应支持渠道信息的主要网页 one-on-one，该渠道可帮助您在云中构建和运行应用程序。
- 联系我们 – 用于查询有关 AWS 账单、账户、事件、滥用和其他问题的中央联系点。
- AWS 网站条款 — 有关我们的版权和商标、您的帐户、许可证和网站访问权限以及其他主题的详细信息。

AWS 软件开发套件适用于 AWS Config

AWS 软件开发套件 (SDK) 可以更轻松地构建可访问经济高效、可扩展且可靠 AWS 的基础架构服务的应用程序。 AWS 软件开发工具包是可下载的单个软件包，其中包含库、代码示例和参考文档，您可以在几分钟内开始使用。下表列出了可用的 SDK 和第三方库，您可以使用这些软件开发工具包和第三方库进行 AWS Config 编程访问。

访问类型	描述
AWS 软件开发工具包	AWS 提供了以下 SDK： • AWS 适用于 C++ 的 SDK 文档 • AWS Mobile SDK for iOS 文档 • 适用于 Go 文档的AWS 开发工具包 • AWS SDK for Java 文档 • AWS 用于 JavaScript 文档的 SDK • AWS SDK for .NET 文档 • AWS SDK for PHP 文档 • AWS SDK for Python (Boto) 文档 • AWS SDK for Ruby 文档
第三方库	开发 AWS 者社区中的开发者还提供自己的库，您可以在以下 AWS 开发者中心找到这些库：

访问类型	描述
	• AWS Java 开发人员中心 • AWS JavaScript 开发人员中心 • AWS PHP 开发人员中心 • AWS Python 开发者中心 • AWS Ruby 开发者中心 • AWS Windows 和.NET 开发者中心

入门 AWS Config

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

报名参加 AWS

主题

- 注册获取 AWS 账户
- 创建具有管理访问权限的用户

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

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

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

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

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

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

保护你的 AWS 账户根用户

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

   要获取使用根用户登录方面的帮助，请参阅 《AWS 登录 用户指南》中的以根用户身份登录。

2. 为您的根用户启用多重身份验证 (MFA)。

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

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

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

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

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

以具有管理访问权限的用户身份登录

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

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

将访问权限分配给其他用户

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

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

入门方法 AWS Config

注册后 AWS 账户，您可以开始使用 AWS Management Console、 AWS CLI 或 AWS SDK。 AWS Config

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

使用控制 AWS Config 台进行设置

AWS Management Console 提供了一个快速、简化的设置流程 AWS Config。

设置

使用控制台 AWS Config 进行设置

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 如果这是您首次打开 AWS Config 控制台或在新区域进行设置 AWS Config ，则 AWS Config 控制台页面将如下所示：

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

主题

- 一键设置
- 手动设置

一键设置

AWS Config 通过减少手动选择的数量，一键设置有助于简化 AWS Config 主机客户的入门流程。要查看设置过程的所有手动选择，请参阅手动设置。

使用 “ AWS Config 一键设置” 在主机上进行设置

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 选择一键设置。

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

- 设置：选择 AWS Config 控制台记录资源和角色的方式，并选择配置历史记录和配置快照文件的发送位置。
- 规则：对于支持规则的区域，本小节可供您配置可以添加到账户的初始 AWS 托管规则。

  设置完成后， AWS Config 将根据您选择的规则评估您的 AWS 资源。设置完成后，可以创建其他规则，您账户中的现有规则也会更新。有关规则的更多信息，请参阅管理您的 AWS Config 规则。
- 查看：验证您的设置细节。

设置

记录策略

为您选择了使用可自定义覆盖项记录所有资源类型的选项。 AWS Config 将记录该区域所有当前和 future 支持的资源类型。有关更多信息，请参阅支持的资源类型。

- 默认设置

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

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

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

- 覆盖设置 – 可选

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

记录资源时的注意事项

AWS Config 评估次数多

与随后的几个月相比，您可能会注意到，在使用 AWS Config 记录的最初一个月中，您的账户活动有所增加。在初始引导过程中， AWS Config 会对您账户中您选择 AWS Config 要记录的所有资源进行评估。

如果您运行的是临时工作负载，则可能会看到 AWS Config 中的活动增加，因为它会记录与创建和删除这些临时资源相关的配置更改。临时工作负载 是临时使用在需要时加载和运行的计算资源。示例包括 Amazon Elastic Compute Cloud (Amazon EC2) 竞价型实例、Amazon EMR 任务和 AWS Auto Scaling。如果要避免因运行临时工作负载而增加的活动，则可以设置配置记录器以将这些资源类型排除在记录之外，或者在 AWS Config 关闭的情况下在单独的帐户中运行这些类型的工作负载，以避免增加配置记录和规则评估。

全局资源类型 | Aurora 全局集群最初包含在记录范围内

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

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

全局资源类型 | IAM 资源类型最初不包含在记录范围内

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

美国东部（弗吉尼亚州北部）除外。全局 IAM 资源类型最初包含在美国东部（弗吉尼亚州北部）区域内，因为该区域是全局 IAM 资源类型的主区域。

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

数据治理

本节为您选择了将 AWS Config 数据保留7年（2557天）的默认数据保留期。

已为您选择 “使用现有 AWS Config 服务相关角色” 选项并将其设置为该AWS Config 角色。服务相关角色由服务预定义 AWS Config ，包括该服务调用其他 AWS 服务所需的所有权限。

传送方式

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

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

规则

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

审核

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

手动设置

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

AWS Config 使用开始使用控制台进行设置

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 选择开始。

设置页面包括三个步骤。下文详细介绍了您选择入门之后的该过程。

- 设置：选择 AWS Config 控制台记录资源和角色的方式，并选择配置历史记录和配置快照文件的发送位置。
- 规则：对于支持规则的区域，本小节可供您配置可以添加到账户的初始 AWS 托管规则。

  设置完成后， AWS Config 将根据您选择的规则评估您的 AWS 资源。设置完成后，可以创建其他规则，您账户中的现有规则也会更新。有关规则的更多信息，请参阅管理您的 AWS Config 规则。
- 查看：验证您的设置细节。

设置

记录策略

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

All resource types with customizable overrides

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

- 默认设置

  为所有当前和未来支持的资源类型配置默认记录频率。有关更多信息，请参阅记录频率。
  - 连续录制 — AWS Config 每当发生更改时，都会持续记录配置更改。
  - 每日记录 - 您会收到代表过去 24 小时内资源的最新状态的配置项 (CI)，前提是它与之前记录的 CI 不同。

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

- 覆盖设置

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

Specific resource types

设置 AWS Config 为仅记录您指定的资源类型的配置更改。

- 特定的资源类型

  选择要记录的资源类型及其频率。有关更多信息，请参阅记录频率。

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

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

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

记录资源时的注意事项

AWS Config 评估次数多

与随后的几个月相比，您可能会注意到，在使用 AWS Config 记录的最初一个月中，您的账户活动有所增加。在初始引导过程中， AWS Config 会对您账户中您选择 AWS Config 要记录的所有资源进行评估。

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

Considerations: All resource types with customizable overrides

全局记录的资源类型 | Aurora 全局集群最初包含在记录范围内

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

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

全局资源类型 | IAM 资源类型最初不包含在记录范围内

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

美国东部（弗吉尼亚北部）除外。全局 IAM 资源类型最初包含在美国东部（弗吉尼亚州北部）区域内，因为该区域是全局 IAM 资源类型的主区域。

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

限制

您可以添加最多 100 项频率覆盖和 600 项排除覆盖。

以下资源类型不支持每日记录：

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

Considerations: Specific resource types

区域可用性

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

限制

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

以下资源类型不支持“每日”频率：

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

数据治理

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

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

    > **Note**
    >
    > 推荐：使用服务关联角色
    > 建议您使用服务相关角色。服务相关角色添加了按预期运行所需 AWS Config 的所有必要权限。

  - 否则，请从您先前存在的角色和权限策略中选择一个 IAM 角色。

    > **Note**
    >
    > AWS Organizations 可以阻止访问的授权策略
    > 如果您使用预先存在的 IAM 角色，请确保没有 AWS Organizations AWS Config 禁止您有权记录资源的授权策略。有关授权策略的更多信息 AWS Organizations，请参阅《AWS Organizations 用户指南》 AWS Organizations中的管理策略。
    > 重复使用 IAM 角色时保留最低权限
    > 如果您使用的是使用 AWS Security Hub 或之类的 AWS 服务 AWS Config AWS Control Tower，并且已经创建了 IAM 角色，请确保您在设置时使用的 IAM 角色 AWS Config 保持

与先前存在的 IAM 角色相同的最低权限。您必须这样做才能确保其他 AWS 服务继续按预期运行。
例如，如果 AWS Control Tower 拥有允许 AWS Config 读取 S3 对象的 IAM 角色，请确保向设置时使用的 IAM 角色授予相同的权限 AWS Config。否则，它可能会干扰 AWS Control Tower 操作方式。

传送方式

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

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

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

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

    > **Note**
    >
    > 亚马逊 SNS 主题的区域

Amazon SNS 主题必须与您设置的区域位于同一区域。 AWS Config

规则

如果您在支持规则 AWS Config 的地区进行设置，请选择下一步。有关更多信息，请参阅 添加、更新和删除 AWS Config 规则。

否则，请选择确认。

审核

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

有关更多信息

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

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

AWS Config 使用进行设置 AWS CLI

AWS CLI 是用于管理您的 AWS 服务的统一工具。只需下载和配置一个工具，您就可以从命令行控制多项 AWS 服务，并使用脚本自动执行这些服务。有关 AWS CLI 和 AWS CLI 工具安装说明的更多信息，请参阅《AWS Command Line Interface 用户指南》中的以下内容。

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

如有必要，`aws configure`请输入配置 AWS CLI 为使用可用的 AWS 区域 AWS Config 。

设置

要进行设置 AWS Config ，请参阅以下主题 AWS CLI。

主题

- 先决条件
- AWS Config 从 AWS CLI

- 验证 AWS Config 是否已成功启动 AWS CLI

先决条件

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

目录

- 创建 Amazon S3 存储桶
- 创建 Amazon SNS 主题
- 创建 IAM 角色

创建 Amazon S3 存储桶

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

使用 S3 控制台

创建存储桶

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

   桶名称必须满足以下要求：

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

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

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

4. 在区域中，选择您想要存储桶所在的 AWS 区域。

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

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

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

6. （可选）如果要启用 S3 对象锁定：

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

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

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

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

7. 选择 创建存储桶 。

使用 AWS 软件开发工具包

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

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

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

这些 AWS SDK 代码示例执行以下任务：

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

以下代码示例演示如何使用 `CreateBucket`。

.NET

AWS SDK for .NET

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

```
        /// <summary>
        /// Shows how to create a new Amazon S3 bucket.
        /// </summary>
```

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

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

创建一个启用对象锁定的存储桶。

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

```
            var request = new PutBucketRequest
            {
                BucketName = bucketName,
                UseClientRegion = true,
                ObjectLockEnabledForBucket = enableObjectLock,
            };

            var response = await _amazonS3.PutBucketAsync(request);

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

- 有关 API 的详细信息，请参阅 AWS SDK for .NET API 参考CreateBucket中的。

Bash

AWS CLI 使用 Bash 脚本

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

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

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

##############################################################################
# function create-bucket
#
# This function creates the specified bucket in the specified AWS Region, unless
# it already exists.
#
# Parameters:
#       -b bucket_name  -- The name of the bucket to create.
#       -r region_code  -- The code for an AWS Region in which to
#                          create the bucket.
#
# Returns:
#       The URL of the bucket that was created.
#     And:
#       0 - If successful.
#       1 - If it fails.
##############################################################################
function create_bucket() {
  local bucket_name region_code response
  local option OPTARG # Required to use getopts command in a function.

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

  # Retrieve the calling parameters.
  while getopts "b:r:h" option; do
```

```
    case "${option}" in
      b) bucket_name="${OPTARG}" ;;
      r) region_code="${OPTARG}" ;;
      h)
        usage
        return 0
        ;;
      \?)
        echo "Invalid parameter"
        usage
        return 1
        ;;
    esac
  done

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

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

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

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

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

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

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

C++

SDK for C++

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

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

    //TODO(user): Change the bucket location constraint enum to your target
 Region.
    if (clientConfig.region != "us-east-1") {
        Aws::S3::Model::CreateBucketConfiguration createBucketConfig;
        createBucketConfig.SetLocationConstraint(

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

    Aws::S3::Model::CreateBucketOutcome outcome = client.CreateBucket(request);
    if (!outcome.IsSuccess()) {
        auto err = outcome.GetError();
        std::cerr << "Error: CreateBucket: " <<
```

```
                    err.GetExceptionName() << ": " << err.GetMessage() <<
 std::endl;
    }
    else {
        std::cout << "Created bucket " << bucketName <<
                    " in the specified AWS Region." << std::endl;
    }

    return outcome.IsSuccess();
}
```

- 有关 API 的详细信息，请参阅 AWS SDK for C++ API 参考CreateBucket中的。

CLI

AWS CLI

示例 1：创建存储桶

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

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region us-east-1
```

输出：

```
{
    "Location": "/my-bucket"
}
```

有关更多信息，请参阅《Amazon S3 用户指南》中的创建存储桶。

示例 2：创建带有强制拥有者的存储桶

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

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region us-east-1 \
```

```
    --object-ownership BucketOwnerEnforced
```

输出：

```
{
    "Location": "/my-bucket"
}
```

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

示例 3：在“us-east-1”区域之外创建存储桶

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

```
aws s3api create-bucket \
    --bucket my-bucket \
    --region eu-west-1 \
    --create-bucket-configuration LocationConstraint=eu-west-1
```

输出：

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

有关更多信息，请参阅《Amazon S3 用户指南》中的创建存储桶。

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

Go

适用于 Go V2 的 SDK

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

```
// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3)
 actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform
 bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}



// CreateBucket creates a bucket with the specified name in the specified Region.
func (basics BucketBasics) CreateBucket(name string, region string) error {
 _, err := basics.S3Client.CreateBucket(context.TODO(), &s3.CreateBucketInput{
  Bucket: aws.String(name),
  CreateBucketConfiguration: &types.CreateBucketConfiguration{
   LocationConstraint: types.BucketLocationConstraint(region),
  },
 })
 if err != nil {
  log.Printf("Couldn't create bucket %v in Region %v. Here's why: %v\n",
   name, region, err)
 }
 return err
}
```

- 有关 API 的详细信息，请参阅 AWS SDK for Go API 参考CreateBucket中的。

Java

适用于 Java 2.x 的 SDK

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

创建存储桶。

```
import software.amazon.awssdk.core.waiters.WaiterResponse;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.CreateBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketRequest;
import software.amazon.awssdk.services.s3.model.HeadBucketResponse;
import software.amazon.awssdk.services.s3.model.S3Exception;
import software.amazon.awssdk.services.s3.waiters.S3Waiter;
import java.net.URISyntaxException;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
 */

public class CreateBucket {
    public static void main(String[] args) throws URISyntaxException {
        final String usage = """

                Usage:
                    <bucketName>\s

                Where:
                    bucketName - The name of the bucket to create. The bucket
 name must be unique, or an error occurs.
                """;

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

        String bucketName = args[0];
        System.out.format("Creating a bucket named %s\n", bucketName);
        Region region = Region.US_EAST_1;
        S3Client s3 = S3Client.builder()
                .region(region)
                .build();
```

```
        createBucket(s3, bucketName);
        s3.close();
    }

    public static void createBucket(S3Client s3Client, String bucketName) {
        try {
            S3Waiter s3Waiter = s3Client.waiter();
            CreateBucketRequest bucketRequest = CreateBucketRequest.builder()
                    .bucket(bucketName)
                    .build();

            s3Client.createBucket(bucketRequest);
            HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
                    .bucket(bucketName)
                    .build();

            // Wait until the bucket is created and print out the response.
            WaiterResponse<HeadBucketResponse> waiterResponse =
 s3Waiter.waitUntilBucketExists(bucketRequestWait);
            waiterResponse.matched().response().ifPresent(System.out::println);
            System.out.println(bucketName + " is ready");

        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
}
```

创建一个启用对象锁定的存储桶。

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

        getClient().createBucket(bucketRequest);
```

```
        HeadBucketRequest bucketRequestWait = HeadBucketRequest.builder()
            .bucket(bucketName)
            .build();

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

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

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

创建存储桶。

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

const client = new S3Client({});

export const main = async () => {
  const command = new CreateBucketCommand({
    // The name of the bucket. Bucket names are unique and have several other
 constraints.
    // See https://docs.aws.amazon.com/AmazonS3/latest/userguide/
bucketnamingrules.html
    Bucket: "bucket-name",
  });

  try {
    const { Location } = await client.send(command);
    console.log(`Bucket created with location ${Location}`);
  } catch (err) {
    console.error(err);
```

```
  }
};
```

- 有关更多信息，请参阅 AWS SDK for JavaScript 开发人员指南。
- 有关 API 的详细信息，请参阅 AWS SDK for JavaScript API 参考CreateBucket中的。

Kotlin

适用于 Kotlin 的 SDK

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

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

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

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

PHP

适用于 PHP 的 SDK

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

创建存储桶。

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

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

- 有关 API 的详细信息，请参阅 AWS SDK for PHP API 参考CreateBucket中的。

Python

SDK for Python (Boto3)

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

使用默认设置创建存储桶。

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

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


    def create(self, region_override=None):
        """
        Create an Amazon S3 bucket in the default Region for the account or in
 the
        specified Region.

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

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

使用生命周期配置创建版本控制的桶。

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

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

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

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

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
```

```
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

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

Ruby

适用于 Ruby 的 SDK

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

```
require "aws-sdk-s3"

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

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

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

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      "None. You must create a bucket before you can get its location!"
    else
```

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

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

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

run_demo if $PROGRAM_NAME == __FILE__
```

- 有关 API 的详细信息，请参阅 AWS SDK for Ruby API 参考CreateBucket中的。

Rust

适用于 Rust 的 SDK

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

```
pub async fn create_bucket(
    client: &Client,
    bucket_name: &str,
    region: &str,
) -> Result<CreateBucketOutput, SdkError<CreateBucketError>> {
    let constraint = BucketLocationConstraint::from(region);
    let cfg = CreateBucketConfiguration::builder()
        .location_constraint(constraint)
```

```
        .build();
    client
        .create_bucket()
        .create_bucket_configuration(cfg)
        .bucket(bucket_name)
        .send()
        .await
}
```

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

SAP ABAP

SDK for SAP ABAP

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

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

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

Swift

SDK for Swift

> **Note**
>
> 这是预览版 SDK 的预发布文档。本文档随时可能更改。

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

```
public func createBucket(name: String) async throws {
    let config = S3ClientTypes.CreateBucketConfiguration(
        locationConstraint: .usEast2
    )
    let input = CreateBucketInput(
        bucket: name,
        createBucketConfiguration: config
    )
    _ = try await client.createBucket(input: input)
}
```

- 如需了解 API 的详细信息，请参阅适用CreateBucket于 S wift 的AWS SDK API 参考。

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

创建 Amazon SNS 主题

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

使用 SNS 控制台

创建 Amazon SNS 主题

1. 通过 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 请执行以下操作之一：
   - 如果 AWS 账户 之前未在您的主题下创建过任何主题，请阅读主页上对 Amazon SNS 的描述。
   - 如果 AWS 账户 之前在您的下方创建过主题，请在导航面板上选择主题。
3. 在 Topics（主页）页面上，选择 Create topic（创建主题）。
4. 在 Create topic（创建主题）页面上，在 Details（详细信息）部分中，执行以下操作：
   a. 对于 Type（类型），选择主题类型（标准或者FIFO）。
   b. 输入主题的名称。对于 FIFO 主题，将 .fifo 添加到名称的末尾。
   c. （可选）输入主题的显示名称。
   d. （可选）对于 FIFO 主题，您可以选择基于内容的消息重复数据删除以启用默认的消息重复数据删除。有关更多信息，请参阅 FIFO 主题的消息重复数据删除。
5. （可选）展开加密部分并执行以下操作。有关更多信息，请参阅静态加密。
   a. 选择 Enable encryption（启用加密）。
   b. 指定客户主密钥 (CMK)。有关更多信息，请参阅关键术语。

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

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

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

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

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

> **Note**
>
> 有关创建自定义 CMK 的说明，请参阅 AWS Key Management Service 开发人员指南中的创建密钥

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

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

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

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

10. 选择创建主题。

    创建主题并显示***MyTopic***页面。

    主题的名称、ARN、（可选）显示名称和主题所有者的 AWS 账户 ID 将显示在 Details（详细信息）部分中。

11. 将主题 ARN 复制到剪贴板，例如：

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

使用电子邮件地址订阅 Amazon SNS 主题

1. 通过 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 在左侧导航窗格中，选择订阅。
3. 在 Subscriptions（订阅）页面上，选择 Create subscription（创建订阅）。
4. 在 Create subscription（创建订阅）页上的 Details（详细信息）部分中，执行以下操作：

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

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

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

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

      - AWS Lambda
      - 平台应用程序终端节点
      - 短信

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

d. 仅限 Firehose 终端节点：对于订阅角色 ARN，请指定您为写入 Firehose 交付流而创建的 IAM 角色的 ARN。有关更多信息，请参阅将 Firehose 传输流订阅 Amazon SNS 的先决条件主题。

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

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

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

h. 选择创建订阅。

   控制台将创建订阅并打开订阅的 Details（详细信息）页面。

使用 AWS 软件开发工具包

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

以下代码示例演示如何使用 `CreateTopic`。

.NET

AWS SDK for .NET

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

使用特定的名称创建主题。

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

/// <summary>
```

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

            IAmazonSimpleNotificationService client = new
 AmazonSimpleNotificationServiceClient();

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

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

            var response = await client.CreateTopicAsync(request);

            return response.TopicArn;
        }
    }
```

创建一个包含名称以及特定 FIFO 和重复数据消除属性的新主题。

```
    /// <summary>
```

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

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

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

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

- 有关 API 的详细信息，请参阅 AWS SDK for .NET API 参考CreateTopic中的。

C++

SDK for C++

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

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

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

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

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

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

```
    return outcome.IsSuccess();
}
```

- 有关 API 的详细信息，请参阅 AWS SDK for C++ API 参考CreateTopic中的。

CLI

AWS CLI

创建 SNS 主题

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

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

输出：

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

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

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

Go

适用于 Go V2 的 SDK

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

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



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

 return topicArn, err
}
```

- 有关 API 的详细信息，请参阅 AWS SDK for Go API 参考CreateTopic中的。

Java

适用于 Java 2.x 的 SDK

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

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

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

                Usage:    <topicName>

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

                """;

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

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

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

    public static String createSNSTopic(SnsClient snsClient, String topicName) {
        CreateTopicResponse result;
        try {
            CreateTopicRequest request = CreateTopicRequest.builder()
                    .name(topicName)
                    .build();

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

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

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

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

在单独的模块中创建客户端并将其导出。

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

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

导入 SDK 和客户端模块，然后调用 API。

```
import { CreateTopicCommand } from "@aws-sdk/client-sns";
import { snsClient } from "../libs/snsClient.js";

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

- 有关更多信息，请参阅 AWS SDK for JavaScript 开发人员指南。
- 有关 API 的详细信息，请参阅 AWS SDK for JavaScript API 参考CreateTopic中的。

Kotlin

适用于 Kotlin 的 SDK

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

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

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

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

PHP

适用于 PHP 的 SDK

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

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

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

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

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

$topicname = 'myTopic';

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

- 有关更多信息，请参阅 AWS SDK for PHP 开发人员指南。
- 有关 API 的详细信息，请参阅 AWS SDK for PHP API 参考CreateTopic中的。

Python

SDK for Python (Boto3)

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

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

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


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

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

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

Ruby

适用于 Ruby 的 SDK

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

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

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

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

  puts "Creating the topic '#{topic_name}'..."
  unless sns_topic_creator.create_topic(topic_name)
    puts "The topic was not created. Stopping program."
    exit 1
  end
end
```

- 有关更多信息，请参阅 AWS SDK for Ruby 开发人员指南。
- 有关 API 的详细信息，请参阅 AWS SDK for Ruby API 参考CreateTopic中的。

Rust

适用于 Rust 的 SDK

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

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

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

    Ok(())
}
```

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

SAP ABAP

SDK for SAP ABAP

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

```
    TRY.
        oo_result = lo_sns->createtopic( iv_name = iv_topic_name ). " oo_result
 is returned for testing purposes. "
        MESSAGE 'SNS topic created' TYPE 'I'.
      CATCH /aws1/cx_snstopiclimitexcdex.
```

```
        MESSAGE 'Unable to create more topics. You have reached the maximum
number of topics allowed.' TYPE 'E'.
   ENDTRY.
```

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

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

创建 IAM 角色

使用 IAM 控制台

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

> **Note**
>
> 如果您使用的是使用的 AWS 服务 AWS Config （例如 Sec AWS urity Hub 或 Cont AWS rol Tower），并且已经创建了角色，则应确保在设置时使用的 IAM 角色与已创建的 AWS Config 角色 AWS Config 保持相同的最低权限，以便其他 AWS 服务继续按预期运行。 AWS Config 例如，如果 Cont AWS rol Tower 有一个 AWS Config 允许读取 Amazon S3 对象的 IAM 角色，则应保证在设置时使用的 IAM 角色中授予的权限相同 AWS Config。否则，它可能会干扰 AWS 控制塔的运行。
>
> 有关的 IAM 角色的更多信息 AWS Config，请参阅 Ident AWS ity and Access 管理。

为 AWS 服务创建角色

1. 登录 AWS Management Console 并打开 IAM 控制台，网址为 https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。

3. 对于选择可信实体，选择 AWS 服务。
4. 选择你想要的用例 AWS Config：Config-可自定义、Config-Organizations、Con fig 或 Config-Conformance Packs。然后选择下一步。
5. 在命名、查看和创建页面上，查看有关您的角色的详细信息，然后选择创建角色。

使用 AWS 软件开发工具包

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

以下代码示例演示如何使用 `CreateRole`。

.NET

AWS SDK for .NET

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

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

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

- 有关 API 的详细信息，请参阅 AWS SDK for .NET API 参考CreateRole中的。

Bash

AWS CLI 使用 Bash 脚本

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

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

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

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

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

if [[ -z "$role_name" ]]; then
  errecho "ERROR: You must provide a role name with the -n parameter."
  usage
  return 1
fi

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

response=$(aws iam create-role \
  --role-name "$role_name" \
  --assume-role-policy-document "$policy_document" \
  --output text \
```

```
    --query Role.Arn)

  local error_code=${?}

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

  echo "$response"

  return 0
}
```

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

C++

SDK for C++

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

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

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

    Aws::IAM::Model::CreateRoleOutcome outcome = client.CreateRole(request);
    if (!outcome.IsSuccess()) {
        std::cerr << "Error creating role. " <<
                  outcome.GetError().GetMessage() << std::endl;
```

```
    }
    else {
        const Aws::IAM::Model::Role iamRole = outcome.GetResult().GetRole();
        std::cout << "Created role " << iamRole.GetRoleName() << "\n";
        std::cout << "ID: " << iamRole.GetRoleId() << "\n";
        std::cout << "ARN: " << iamRole.GetArn() << std::endl;
    }

    return outcome.IsSuccess();
}
```

- 有关 API 的详细信息，请参阅 AWS SDK for C++ API 参考CreateRole中的。

CLI

AWS CLI

示例 1：创建 IAM 角色

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

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

输出：

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

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

要将权限策略附加到角色，请使用 `put-role-policy` 命令。

有关更多信息，请参阅《AWS IAM 用户指南》中的创建 IAM 角色。

示例 2：创建具有指定最长会话持续时间的 IAM 角色

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

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

输出：

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

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

示例 3：创建带有标签的 IAM 角色

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

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

输出：

```
{
    "Role": {
        "Path": "/",
        "RoleName": "Test-Role",
        "RoleId": "AKIAIOSFODNN7EXAMPLE",
        "Arn": "arn:aws:iam::123456789012:role/Test-Role",
        "CreateDate": "2023-05-25T23:29:41+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Statement1",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": "arn:aws:iam::123456789012:root"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        },
        "Tags": [
            {
                "Key": "Department",
                "Value": "Accounting"
            },
            {
                "Key": "Location",
                "Value": "Seattle"
            }
```

```
        ]
    }
}
```

有关更多信息，请参阅《AWS IAM 用户指南》中的标记 IAM 角色。

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

Go

适用于 Go V2 的 SDK

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

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



// CreateRole creates a role that trusts a specified user. The trusted user can
 assume
// the role to acquire its permissions.
// PolicyDocument shows how to work with a policy document as a data structure
 and
// serialize it to JSON by using Go's JSON marshaler.
func (wrapper RoleWrapper) CreateRole(roleName string, trustedUserArn string)
 (*types.Role, error) {
 var role *types.Role
 trustPolicy := PolicyDocument{
  Version:   "2012-10-17",
  Statement: []PolicyStatement{{
   Effect: "Allow",
   Principal: map[string]string{"AWS": trustedUserArn},
```

```
    Action: []string{"sts:AssumeRole"},
   }},
  }
  policyBytes, err := json.Marshal(trustPolicy)
  if err != nil {
   log.Printf("Couldn't create trust policy for %v. Here's why: %v\n",
  trustedUserArn, err)
   return nil, err
  }
  result, err := wrapper.IamClient.CreateRole(context.TODO(),
  &iam.CreateRoleInput{
   AssumeRolePolicyDocument: aws.String(string(policyBytes)),
   RoleName:                 aws.String(roleName),
  })
  if err != nil {
   log.Printf("Couldn't create role %v. Here's why: %v\n", roleName, err)
  } else {
   role = result.Role
  }
  return role, err
 }
```

- 有关 API 的详细信息，请参阅 AWS SDK for Go API 参考CreateRole中的。

Java

适用于 Java 2.x 的 SDK

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

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

```
import software.amazon.awssdk.services.iam.IamClient;
import java.io.FileReader;

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

public class CreateRole {
    public static void main(String[] args) throws Exception {
        final String usage = """
                Usage:
                    <rolename> <fileLocation>\s

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

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

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

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

```
    }

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

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

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

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

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

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

创建角色。

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

const client = new IAMClient({});

/**
 *
 * @param {string} roleName
 */
export const createRole = (roleName) => {
  const command = new CreateRoleCommand({
    AssumeRolePolicyDocument: JSON.stringify({
      Version: "2012-10-17",
      Statement: [
        {
          Effect: "Allow",
          Principal: {
            Service: "lambda.amazonaws.com",
          },
          Action: "sts:AssumeRole",
        },
      ],
    }),
    RoleName: roleName,
  });

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

- 有关 API 的详细信息，请参阅 AWS SDK for JavaScript API 参考CreateRole中的。

PHP

适用于 PHP 的 SDK

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

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

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

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

- 有关 API 的详细信息，请参阅 AWS SDK for PHP API 参考CreateRole中的。

PowerShell

用于 PowerShell

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

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

输出：

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

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

```
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考CreateRole中的。

Python

SDK for Python (Boto3)

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

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

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

    try:
        role = iam.create_role(
            RoleName=role_name, AssumeRolePolicyDocument=json.dumps(trust_policy)
        )
```

```
        logger.info("Created role %s.", role.name)
    except ClientError:
        logger.exception("Couldn't create role %s.", role_name)
        raise
    else:
        return role
```

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

Ruby

适用于 Ruby 的 SDK

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

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

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

```
    end

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

- 有关 API 的详细信息，请参阅 AWS SDK for Ruby API 参考CreateRole中的。

Rust

适用于 Rust 的 SDK

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

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

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

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

Swift

SDK for Swift

> **Note**
>
> 这是预览版 SDK 的预发布文档。本文档随时可能更改。

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

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

- 如需了解 API 的详细信息，请参阅适用CreateRole于 S wift 的AWS SDK API 参考。

AWS Config 从 AWS CLI

> **Note**
>
> 在设置 AWS Config 之前 AWS CLI，您需要创建一个 S3 存储桶、一个 SNS 主题和一个附有策略的 IAM 角色作为先决条件。然后，您可以使用 AWS CLI 为指定存储桶、主题和角色 AWS Config。要设置的先决条件 AWS Config，请参阅先决条件。

首先，请使用 put-configurat AWS Config ion-rec order AWS CLI、put-delivery-channel 和 start-configuration-rec order 命令，如下所示：

- `put-configuration-recorder` 命令可创建新的配置记录器以记录您指定的资源配置。
- `put-delivery-channel` 命令可创建传输通道对象，将配置信息传输到 S3 存储桶和 SNS 主题。
- 创建传输通道后，`start-configuration-recorder` 开始记录您选择的资源配置，您可以在您的 AWS 账户中看到这些配置。

> **Note**
>
> 您账户中的每个 AWS 区域都只能有一个配置记录器和一个传输通道。

您可以指定记录器的名称以及配置记录器担任 AWS Config 和使用的 IAM 角色的 Amazon 资源名称 (ARN)。 AWS Config 创建配置记录器时会自动分配 “默认” 的名称。配置记录器在创建后，不能更改其名称。要更改配置记录器的名称，您必须删除该配置记录器，然后使用新名称创建一个新配置记录器。

要使用设置 AWS Config 多账户多区域数据聚合 AWS CLI，请参阅使用 AWS 命令行界面设置聚合器。您必须为要记录配置项目的每个区域创建单独 AWS 账户 的配置记录器。

目录

- put-configuration-recorder
- put-delivery-channel
- start-configuration-recorder

put-configuration-recorder

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

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

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

> **Note**
>
> 录制组和配置记录器
> `--recording-group` 字段指定要记录哪些资源类型。
> 该`--configuration-recorder`字段指定`name`和`roleArn`以及配置记录器的默认录制频率 (`recordingMode`)。您也可以使用此字段来覆盖特定资源类型的记录频率。

记录组

put-configuration-recorder 为 `--recording-group` 参数使用以下选项：

- `allSupported=true`— AWS Config 记录所有支持的资源类型的配置更改，不包括全球 IAM 资源类型。 AWS Config 添加对新资源类型的支持后， AWS Config 会自动开始记录该类型的资源。
- `includeGlobalResourceTypes=true` – 此选项是一个捆绑包，仅适用于全局 IAM 资源类型：IAM 用户、组、角色和客户管理型策略。这些全球 IAM 资源类型只能在 2022 年 2 月之前可用的 AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后，您无法在支持的区域中记录全球 IAM 资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

> **Important**
>
> Aurora 全局集群记录在所有已启用的区域中
> `AWS::RDS::GlobalCluster`资源类型将记录在启用配置记录器的所有支持 AWS Config 区域，即使设置`includeGlobalResourceTypes`为`false`。`includeGlobalResourceTypes` 选项是一个捆绑包，仅适用于 IAM 用户、组、角色和客户管理型策略。
> 如果您不想在所有已启用的区域中记录 `AWS::RDS::GlobalCluster`，请使用以下记录策略之一：
>
> 1. 记录所有当前和未来的资源类型，排除项除外 (`EXCLUSION_BY_RESOURCE_TYPES`)，或者
> 2. 记录特定的资源类型 (`INCLUSION_BY_RESOURCE_TYPES`)。

有关更多信息，请参阅选择将记录的资源。

Important

包含GlobalResourceTypes 和排除记录策略

该includeGlobalResourceTypes字段对EXCLUSION_BY_RESOURCE_TYPES录制策略没有影响。这意味着，当设置为exclusionByResourceTypes时includeGlobalResourceTypes，全球 IAM 资源类型（IAM 用户、群组、角色和客户托管策略）不会自动添加为排除项。false

该includeGlobalResourceTypes字段只能用于修改该AllSupported字段，因为该字段的默认设置是记录除全球 IAM 资源类型之AllSupported外的所有受支持资源类型的配置更改。要在设置为时AllSupported包括全局 IAM 资源类型true，请确保将设置includeGlobalResourceTypes为true。

要排除EXCLUSION_BY_RESOURCE_TYPES录制策略的全球 IAM 资源类型，您需要手动将其添加到的resourceTypes字段中exclusionByResourceTypes。

Note

必填字段和可选字段

将 includeGlobalResourceTypes 设置为 true 之前，请先将 allSupported 字段设置为 true。

也可以将 RecordingStrategy 的 useOnly 字段设置为 ALL_SUPPORTED_RESOURCE_TYPES。

Note

覆盖字段

如果您在的字段中设置includeGlobalResourceTypes为false但列出了全局 IAM 资源类型 RecordingGroup，则无论您是否 AWS Config 将该resourceTypes字段设置为 false，仍会记录这些指定资源类型的配置更改。includeGlobalResourceTypes

如果您不想记录对全局 IAM 资源类型（IAM 用户、组、角色和客户管理型策略）的配置更改，那么除了将 includeGlobalResourceTypes 字段设置为 false 之外，切勿在 resourceTypes 字段中列出这些内容。

- `recordingStrategy` – 指定配置记录器的记录策略。`recordingGroup.json` 文件指定了 AWS Config 将记录的资源类型：
  - 如果将的`useOnly`字段设置RecordingStrategy为`ALL_SUPPORTED_RESOURCE_TYPES`，则会 AWS Config 记录所有支持的资源类型的配置更改，不包括全球 IAM 资源类型。或者，您可以将的`allSupported`字段设置RecordingGroup为`true`。 AWS Config 添加对新资源类型的支持后，AWS Config 会自动开始记录该类型的资源。
  - 如果将的`useOnly`字段设置RecordingStrategy为`INCLUSION_BY_RESOURCE_TYPES`，则仅 AWS Config 记录您在`resourceTypes`字段中指定的资源类型的配置更改RecordingGroup。
  - 如果将的`useOnly`字段设置RecordingStrategy为`EXCLUSION_BY_RESOURCE_TYPES`，则会 AWS Config 记录所有支持的资源类型的配置更改，但您指定要排除在`resourceTypes`字段中记录的资源类型除外ExclusionByResourceTypes。

> **Note**
>
> 必填字段和可选字段
>
> 当您将 `--recording-group` 的 `allSupported` 字段设置为 `true` 时，`recordingStrategy` 字段是可选的。
>
> 当您在 `--recording-group` 的 `resourceTypes` 字段中列出资源类型时，`recordingStrategy` 字段是可选的。
>
> 如果您在 `exclusionByResourceTypes` 的 `resourceTypes` 字段中列出了要从记录中排除的资源类型，`recordingStrategy` 字段为必填字段。

> **Note**
>
> 覆盖字段
>
> 如果您对记录策略选择 `EXCLUSION_BY_RESOURCE_TYPES`，则 `exclusionByResourceTypes` 字段将覆盖请求中的其他属性。
>
> 例如，即使您将 `includeGlobalResourceTypes` 设置为 false，全局 IAM 资源类型仍将自动记录在此选项中，除非这些资源类型在 `exclusionByResourceTypes` 的 `resourceTypes` 字段中被明确列为排除项。

> **Note**
>
> 全局资源类型和资源排除记录策略
>
> 默认情况下，如果您选择`EXCLUSION_BY_RESOURCE_TYPES`录制策略，则在设置配置记录器的区域中 AWS Config 添加对新资源类型（包括全局资源类型）的支持时，会自动 AWS Config 开始记录该类型的资源。
>
> 除非特别列为排除项，否则`AWS::RDS::GlobalCluster`将在启用配置记录器的所有受支持 AWS Config 区域中自动记录。
>
> IAM 用户、群组、角色和客户托管策略将记录在您设置配置记录器的区域（如果该区域在 2022 年 2 月之前可用）。 AWS Config 2022 年 2 月 AWS Config 之后，您无法在支持的区域中记录全球 IAM 资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

以下示例显示 `recordingGroup.json` 的请求语法：

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

> **Note**
>
> AWS Organizations 可以阻止访问的授权策略
>
> 如果您使用预先存在的 IAM 角色，请确保没有 AWS Organizations AWS Config 禁止您有权记录资源的授权策略。有关授权策略的更多信息 AWS Organizations，请参阅《AWS Organizations 用户指南》 AWS Organizations中的管理策略。
>
> 重复使用 IAM 角色时保留最低权限
>
> 如果您使用的是使用 AWS Security Hub 或之类的 AWS 服务 AWS Config AWS Control Tower，并且已经创建了 IAM 角色，请确保您在设置时使用的 IAM 角色 AWS Config 保持与

先前存在的 IAM 角色相同的最低权限。您必须这样做才能确保其他 AWS 服务继续按预期运行。

例如，如果 AWS Control Tower 拥有允许 AWS Config 读取 S3 对象的 IAM 角色，请确保向设置时使用的 IAM 角色授予相同的权限 AWS Config。否则，它可能会干扰 AWS Control Tower 操作方式。

> **Note**
>
> AWS Config 评估次数多
>
> 与随后的几个月相比，您可能会注意到，在使用 AWS Config 记录的最初一个月中，您的账户活动有所增加。在初始引导过程中， AWS Config 会对您账户中您选择 AWS Config 要记录的所有资源进行评估。
>
> 如果您运行的是临时工作负载，则可能会看到活动增加， AWS Config 因为它记录了与创建和删除这些临时资源相关的配置更改。临时工作负载 是临时使用在需要时加载和运行的计算资源。示例包括亚马逊弹性计算云 (Amazon EC2) 竞价型实例、亚马逊 EMR 任务和。 AWS Auto Scaling如果要避免因运行临时工作负载而增加的活动，则可以设置配置记录器以将这些资源类型排除在记录之外，或者在 AWS Config 关闭的情况下在单独的帐户中运行这些类型的工作负载，以避免增加配置记录和规则评估。

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

配置记录器

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

- `name`— 配置记录器的名称。 AWS Config 创建配置记录器时会自动分配 “默认” 的名称。
- `roleARN`— 由配置记录器担任 AWS Config 和使用的 IAM 角色的 Amazon 资源名称 (ARN)。

- `recordingMode`— 指定用于记录配置更改的 AWS Config 默认录制频率。 AWS Config 支持连续录制和每日录制。连续记录可让您在每次发生配置更改时连续记录更改。使用每日记录，您将收到代表过去 24 小时内资源的最新状态的配置项 (CI)，前提是它与之前记录的 CI 不同。
  - `recordingFrequency`— AWS Config 用于记录配置更改的默认录制频率。

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

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

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

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

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

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

put-delivery-channel

以下代码示例演示如何使用 PutDeliveryChannel。

CLI

AWS CLI

创建配送渠道

以下命令以 JSON 代码的形式提供传送渠道的设置：

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

该deliveryChannel.json文件指定了配送渠道属性：

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

```
    }
}
```

此示例设置了以下属性：

name-配送渠道的名称。默认情况下， AWS Config 会`default`将名称分配给新的交付渠道。您无法使用命令更新传递渠道名称。`put-delivery-channel`有关更改名称的步骤，请参阅重命名配送渠道。 `s3BucketName`- AWS Config 向其发送配置快照和配置历史记录文件的 Amazon S3 存储桶的名称。如果您指定的存储桶属于另一个 AWS 账户，则该存储桶必须具有授予对 Config AWS 的访问权限的策略。有关更多信息，请参阅 Amazon S3 存储桶的权限。

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

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

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

- 有关 API 的详细信息，请参阅《AWS CLI 命令参考》中的 “PutDelivery频道”。

PowerShell

用于 PowerShell

示例 1：此示例更改了现有配送渠道的 deliveryFrequency 属性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考中的PutDelivery频道。

start-configuration-recorder

要完成开启 AWS Config，请使用`start-configuration-recorder`命令。

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

验证 AWS Config 是否已成功启动 AWS CLI

启动后 AWS Config，您可以使用 AWS CLI 命令检查是否 AWS Config 正在运行以及是否 AWS Config 已创建配置记录器和传送渠道。您也可以确认 AWS Config 已开始录制配置并将其传送到交付渠道。

目录

- 检查是否已创建传输通道
- 检查是否已创建配置记录器
- 检查是否 AWS Config 已开始录制

检查是否已创建传输通道

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

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

当您使用 CLI、服务 API 或软件开发工具包配置您的交付渠道但未指定名称时， AWS Config 会自动分配名称 “” `default`。

检查是否已创建配置记录器

使用 `describe-configuration-recorders` 命令检查是否已创建配置记录器，以及该配置记录器是否已代入 IAM 角色。有关更多信息，请参阅 创建 IAM 角色。

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

检查是否 AWS Config 已开始录制

使用describe-configuration-recorder-status命令检查是否 AWS Config 已开始记录您账户中现有受支持 AWS 资源的配置。记录的配置会传递到指定的传递通道。

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

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

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

AWS Config 与 AWS SDK 一起使用

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

SDK 文档	代码示例
AWS SDK for C++	AWS SDK for C++ 代码示例
AWS CLI	AWS CLI 代码示例
AWS SDK for Go	AWS SDK for Go 代码示例
AWS SDK for Java	AWS SDK for Java 代码示例
AWS SDK for JavaScript	AWS SDK for JavaScript 代码示例
AWS SDK for Kotlin	AWS SDK for Kotlin 代码示例
AWS SDK for .NET	AWS SDK for .NET 代码示例
AWS SDK for PHP	AWS SDK for PHP 代码示例
AWS Tools for PowerShell	PowerShell 代码示例工具
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 代码示例
AWS SDK for Ruby	AWS SDK for Ruby 代码示例
AWS SDK for Rust	AWS SDK for Rust 代码示例
适用于 SAP ABAP 的 AWS SDK	适用于 SAP ABAP 的 AWS SDK 代码示例
AWS SDK for Swift	AWS SDK for Swift 代码示例

示例可用性

找不到所需的内容？ 通过使用此页面底部的提供反馈链接请求代码示例。

管理配置记录器

AWS Config 使用配置记录器来检测资源配置中的更改，并将这些更改捕获为配置项目。必须先创建配置记录器，然后 AWS Config 才能跟踪您的资源配置。启动配置记录器时， AWS Config 会清点您账户中的所有 AWS 资源。

每个 AWS 区域只能有一个配置记录器频道 AWS 账户，并且需要使用传送渠道 AWS Config。

如果您使用控制台或 AWS CLI AWS Config 进行设置，则 AWS Config 会自动为您创建配置记录器，然后启动配置记录器。有关更多信息，请参阅 入门 AWS Config。

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

AWS Config 开始记录配置时，您需要支付服务使用费。有关定价信息，请参阅 AWS Config 定价。

> **Important**
>
> 如果配置记录器关闭，已删除资源的评估结果可能会持续显示
> 如果配置记录器已关闭，它将禁用跟踪资源配置更改（包括资源删除）的功能。 AWS Config 这意味着，如果您关闭配置记录器，可能会看到先前已删除的资源的评估结果。

管理配置记录器 (控制台)

您可以使用 AWS Config 控制台停止或启动配置记录器。您也可以更改配置记录器的记录频率。

To stop or start the configuration recorder

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在导航窗格中，选择设置。
3. 停止或启动配置记录器：
   - 如果您要停止记录，请选择 Recording is on 下的 Turn off。系统提示时，请选择继续。
   - 如果您要开始记录，请选择 Recording is off (记录已关闭) 下的 Turn on (开启)。系统提示时，请选择继续。

To change the recording frequency

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

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在导航窗格中，选择设置。
3. 选择编辑，以查看“记录频率”下的选项。

管理配置记录器 (AWS CLI)

您可以使用 AWS CLI 来停止或启动配置记录器。您也可以使用 AWS CLI、 AWS Config API 或其中一个 AWS SDK 重命名或删除配置记录器。以下步骤可帮助您使用 AWS CLI。

To stop the configuration recorder

使用 `stop-configuration-recorder` 命令：

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

To start the configuration recorder

使用 `start-configuration-recorder` 命令：

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

To change the recording frequency

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

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

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

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

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

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

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

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

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

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

To delete the configuration recorder

使用 delete-configuration-recorder 命令：

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

To rename the configuration recorder

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

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

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

```
        }
    ]
}
```

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

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

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

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

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

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

配置记录器的偏离检测

`AWS::Config::ConfigurationRecorder` 资源类型是配置记录器的配置项 (CI)，用于跟踪配置记录器的所有状态更改。您可以使用此 CI 来检查配置记录器的状态是否与其先前的状态不同或已经偏离。例如，此 CI 会跟踪您是否允许 AWS Config 跟踪资源类型更新、是否已停止或启动配置记录器，或者是否删除或卸载了配置记录器。发生偏离的配置记录器表示您没有准确检测到预期资源类型的更改。如果您的配置记录器发生偏离，则可能导致漏报或误报合规性结果。

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

管理传递通道

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

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

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

> **Note**
>
> AWS Config 支持对使用的 Amazon S3 存储桶进行 AWS KMS 加密 AWS Config
> 您可以提供 AWS Key Management Service (AWS KMS) 密钥或别名亚马逊资源名称 (ARN) 来加密传输到您的亚马逊简单存储服务 (Amazon S3) 存储桶的数据。默认情况下，将配置历史记录和快照文件 AWS Config 传送到您的 Amazon S3 存储桶，并使用 S3 AES-256 服务器端加密 SSE-S3 对静态数据进行加密。但是，如果您提供 AWS Config 了 KMS 密钥或别名 ARN，则 AWS Config 使用该 KMS 密钥而不是 AES-256 加密。
> AWS Config 不支持向 Amazon S3 存储桶的传送渠道，其中启用了对象锁定并启用了默认保留。有关更多信息，请参阅 S3 对象锁定的工作原理。

主题

- 术语
- 更新传递通道
- 重命名传递通道
- 配置项的组成部分
- 将配置快照传送到 Amazon S3 存储桶
- AWS Config 发送到 Amazon SNS 主题的通知

术语

配置项目表示您账户中存在的受支持 AWS 资源的各种属性的 point-in-time 视图。配置项目的组件包括元数据、属性、关系、当前配置和相关事件。 AWS Config 每当它检测到正在记录的资源类型发生变化

时，都会创建一个配置项目。例如，如果 AWS Config 正在记录 Amazon S3 存储桶，则每当创建、更新或删除存储桶时，都会 AWS Config 创建一个配置项目。您也可以选择 AWS Config 以您设置的录制频率创建配置项目。

配置历史记录是指定资源在某个时间段的配置项集合。配置历史记录包含多种信息，例如资源首次创建的时间、过去一个月的资源配置情况以及昨天上午 9 点发生了哪些配置更改等。配置历史记录有多种格式可供您使用。 AWS Config 自动将正在记录的每种资源类型的配置历史记录文件传送到您指定的 Amazon S3 存储桶。您可以在 AWS Config 控制台中选择给定资源，然后使用时间轴导航到该资源的所有先前配置项目。此外，您还可以从 API 访问资源的历史配置项。

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

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

更新传递通道

更新传递通道时，您可以设置以下选项：

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

更新配送渠道（控制台）

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

控制台不提供用于重命名传递通道、设置配置快照频率或删除传递通道的选项。要执行这些任务，必须使用 AWS CLI、 AWS Config API 或其中一个 AWS 软件开发工具包。

更新配送渠道 (AWS SDK)

以下代码示例演示如何使用 `PutDeliveryChannel`。

CLI

AWS CLI

创建配送渠道

以下命令以 JSON 代码的形式提供传送渠道的设置：

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

该`deliveryChannel.json`文件指定了配送渠道属性：

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

此示例设置了以下属性：

`name`-配送渠道的名称。默认情况下， AWS Config 会`default`将名称分配给新的交付渠道。您无法使用命令更新传递渠道名称。`put-delivery-channel`有关更改名称的步骤，请参阅重命名配送渠道。 `s3BucketName`- AWS Config 向其发送配置快照和配置历史记录文件的 Amazon S3 存储桶的名称。如果您指定的存储桶属于另一个 AWS 账户，则该存储桶必须具有授予对 Config AWS 的访问权限的策略。有关更多信息，请参阅 Amazon S3 存储桶的权限。

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

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

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

- 有关 API 的详细信息，请参阅《AWS CLI 命令参考》中的 “PutDelivery频道”。

PowerShell

用于 PowerShell

示例 1：此示例更改了现有配送渠道的 deliveryFrequency 属性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考中的PutDelivery频道。

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

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

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

CLI

AWS CLI

获取有关配送渠道的详细信息

以下命令返回有关交付渠道的详细信息：

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

输出：

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

- 有关 API 的详细信息，请参阅《AWS CLI 命令参考》中的 “DescribeDelivery频道”。

PowerShell

用于 PowerShell

示例 1：此示例检索该地区的配送渠道并显示详细信息。

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

输出：

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

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考中的DescribeDelivery频道。

重命名传递通道

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

AWS Config 控制台不提供删除传送渠道的选项，因此您必须使用 AWS CLI、 AWS Config API 或其中一个 AWS SDK。

重命名传递通道 (AWS CLI)

使用重命名配送渠道 AWS CLI

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

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

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

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

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

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

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

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

deliveryChannel.json 文件指定了传递通道的属性：

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

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

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

配置项的组成部分

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

配置项由以下部分组成。

组件	描述	包含
元数据	有关此配置项的信息	• 版本 ID • 捕获配置项的时间 • 表明项目是否成功捕获的配置项状态 • 表明资源配置项排序的状态 ID
Attributes	资源属性	• 资源 ID • 此资源的键值标签列表 • 资源类型（请参阅支持的资源类型） • Amazon 资源名称 (ARN)

组件	描述	包含
		• 包含此资源的可用区（如果适用） • 资源创建的时间
关系	该资源和与账户关联的其他资源的关系	关系描述，例如 Amazon EBS 卷 `vol-1234567` 附加到 Amazon EC2 实例 `i-a1b2c3d4`
当前配置	通过对资源进行 Describe 或 List API 调用返回的信息	例如，`DescribeVolumes` API 会返回有关卷的以下信息： • 卷所在的可用区 • 卷挂载的时间 • 卷挂载到的 EC2 实例的 ID • 卷的当前状态 • 国 DeleteOnTermination 旗国 • 卷挂载到的设备 • 卷类型，例如 `gp2`, `io1`, 或 `standard`

注意

1. 配置项关系不包含网络流或数据流依赖关系。无法自定义配置项来表示您的应用程序架构。
2. 从 1.3 版开始，relatedEvents 字段为空。您可以访问 LookupEvents API 参考中的AWS CloudTrail API 来检索资源的事件。
3. 从 1.3 版开始，configurationItemMD5Hash 字段为空。您可以使用该 configurationStateId 字段来确保您拥有最新的配置项目。

将配置快照传送到 Amazon S3 存储桶

AWS Config 将记录到您在配置交付渠道时指定 AWS Config 的 Amazon S3 存储桶中的 AWS 资源的配置快照。

主题

• 交付配置快照

- 示例配置快照来自 AWS Config
- 验证传送状态
- 查看 Amazon S3 存储桶中的配置快照

交付配置快照

AWS Config 当您调用 Snapsho DeliverConfigt 操作或运行 AWS CLIdeliver-config-snapshot命令时，会生成配置快照。 AWS Config 将配置快照存储在您在启用时指定的 Amazon S3 存储桶中 AWS Config。

通过指定配置传送渠道 AWS Config 时分配的名称来键入deliver-config-snapshot命令，例如：

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

示例配置快照来自 AWS Config

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

> **Note**
>
> 配置快照中可能会引用不支持的资源类型和资源 ID。

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "configurationItemVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
```

```
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
```

```
        {
            "configurationItemVersion": "1.0",
            "resourceId": "i-344c463d",
            "accountId": "12345678910",
            "arn": "arn:aws:ec2:us-west-2b:123456789012:instance/i-344c463d",
            "configurationItemCaptureTime": "2014-03-07T23:47:09.523Z",
            "configurationStateID": "cdb571fa-ce7a-4ec5-8914-0320466a355e",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Instance",
            "resourceCreationTime": "2014-02-26T22:56:35.000Z",
            "tags": {
                "Name": "integ-test-1",
                "examplename": "examplevalue"
            },
            "relationships": [
                {
                    "resourceId": "vol-ce676ccc",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume"
                },
                {
                    "resourceId": "vol-ef0e06ed",
                    "resourceType": "AWS::EC2::Volume",
                    "name": "Attached Volume",
                    "direction": "OUT"
                },
                {
                    "resourceId": "subnet-47b4cf2c",
                    "resourceType": "AWS::EC2::SUBNET",
                    "name": "Is contained in Subnet",
                    "direction": "IN"
                }
            ],
            "configuration": {
                "instanceId": "i-344c463d",
                "imageId": "ami-ccf297fc",
                "state": {
                    "code": 16,
                    "name": "running"
```

```
                },
                "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                "publicDnsName": "ec2-54-218-4-189.us-west-2.compute.amazonaws.com",
                "stateTransitionReason": "",
                "keyName": "configDemo",
                "amiLaunchIndex": 0,
                "productCodes": [],
                "instanceType": "t1.micro",
                "launchTime": "2014-02-26T22:56:35.0000+0000",
                "placement": {
                    "availabilityZone": "us-west-2b",
                    "groupName": "",
                    "tenancy": "default"
                },
                "kernelId": "aki-fc8f11cc",
                "monitoring": {
                    "state": "disabled"
                },
                "subnetId": "subnet-47b4cf2c",
                "vpcId": "vpc-41b4cf2a",
                "privateIpAddress": "172.31.21.63",
                "publicIpAddress": "54.218.4.189",
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/sda1",
                "blockDeviceMappings": [
                    {
                        "deviceName": "/dev/sda1",
                        "ebs": {
                            "volumeId": "vol-ef0e06ed",
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:38.0000+0000",
                            "deleteOnTermination": true
                        }
                    },
                    {
                        "deviceName": "/dev/sdf",
                        "ebs": {
                            "volumeId": "vol-ce676ccc",
                            "status": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    }
```

```
                ],
                "virtualizationType": "paravirtual",
                "clientToken": "aBCDe123456",
                "tags": [
                    {
                        "key": "Name",
                        "value": "integ-test-1"
                    },
                    {
                        "key": "examplekey",
                        "value": "examplevalue"
                    }
                ],
                "securityGroups": [
                    {
                        "groupName": "launch-wizard-2",
                        "groupId": "sg-892adfec"
                    }
                ],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [
                    {
                        "networkInterfaceId": "eni-55c03d22",
                        "subnetId": "subnet-47b4cf2c",
                        "vpcId": "vpc-41b4cf2a",
                        "description": "",
                        "ownerId": "12345678910",
                        "status": "in-use",
                        "privateIpAddress": "172.31.21.63",
                        "privateDnsName": "ip-172-31-21-63.us-west-2.compute.internal",
                        "sourceDestCheck": true,
                        "groups": [
                            {
                                "groupName": "launch-wizard-2",
                                "groupId": "sg-892adfec"
                            }
                        ],
                        "attachment": {
                            "attachmentId": "eni-attach-bf90c489",
                            "deviceIndex": 0,
                            "status": "attached",
                            "attachTime": "2014-02-26T22:56:35.0000+0000",
                            "deleteOnTermination": true
```

```
                        },
                        "association": {
                            "publicIp": "54.218.4.189",
                            "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                            "ipOwnerId": "amazon"
                        },
                        "privateIpAddresses": [
                            {
                                "privateIpAddress": "172.31.21.63",
                                "privateDnsName": "ip-172-31-21-63.us-
west-2.compute.internal",
                                "primary": true,
                                "association": {
                                    "publicIp": "54.218.4.189",
                                    "publicDnsName": "ec2-54-218-4-189.us-
west-2.compute.amazonaws.com",
                                    "ipOwnerId": "amazon"
                                }
                            }
                        ]
                    }
                ],
                "ebsOptimized": false
            }
        }
    ]
}
```

下一步是验证配置快照是否成功传送到了传递通道。

验证传送状态

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

```
$ aws configservice describe-delivery-channel-status
{
    "DeliveryChannelsStatus": [
        {
            "configStreamDeliveryInfo": {
                "lastStatusChangeTime": 1415138614.125,
                "lastStatus": "SUCCESS"
```

```
            },
            "configHistoryDeliveryInfo": {
                "lastSuccessfulTime": 1415148744.267,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415148744.267
            },
            "configSnapshotDeliveryInfo": {
                "lastSuccessfulTime": 1415333113.4159999,
                "lastStatus": "SUCCESS",
                "lastAttemptTime": 1415333113.4159999
            },
            "name": "default"
        }
    ]
}
```

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

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

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

查看 Amazon S3 存储桶中的配置快照

1. 登录 AWS Management Console 并打开亚马逊 S3 控制台，网址为 https://console.aws.amazon.com/s3/。
2. 在 Amazon S3 控制台的所有存储桶列表中，单击您的 Amazon S3 存储桶名称。
3. 单击查看您的存储桶中的嵌套文件夹，找到快照 ID 与由命令返回的 ID 相匹配的 `ConfigSnapshot` 对象。下载并打开对象以查看配置快照。

   S3 存储桶还包含一个名为的空文件`ConfigWritabilityCheckFile`。 AWS Config 创建此文件以验证服务是否可以成功写入 S3 存储桶。

AWS Config 发送到 Amazon SNS 主题的通知

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

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

AWS Config 针对以下事件发送通知：

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

主题

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

示例配置项变更通知

AWS Config 使用 Amazon SNS 向订阅终端节点发送通知。这些通知提供配置快照和配置历史记录的交付状态，并提供记录 AWS 资源的配置发生变化时 AWS Config 创建的每个配置项目。 AWS Config 还会发送通知，显示您的资源是否符合您的规则。如果您选择通过电子邮件发送通知，则可在您的电子邮件客户端应用程序中，根据电子邮件的主题行和消息正文使用筛选条件。

以下是一个 Amazon SNS 通知示例负载，当 AWS Config 检测到 Amazon Elastic Block Store 卷 `vol-ce676ccc` 已附加到 ID 为 `i-344c463d` 的实例时，会生成该通知。此通知包含针对资源的配置项变更。

```
{
    "Type": "Notification",
    "MessageId": "8b945cb0-db34-5b72-b032-1724878af488",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:example",
    "Message": {
        "MessageVersion": "1.0",
        "NotificationCreateTime": "2014-03-18T10:11:00Z",
        "messageType": "ConfigurationItemChangeNotification",
        "configurationItem": [
            {
                "configurationItemVersion": "1.0",
                "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
                "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
                "resourceId": "vol-ce676ccc",
                "accountId": "123456789012",
                "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
                "configurationItemStatus": "OK",
                "relatedEvents": [],
                "availabilityZone": "us-west-2b",
                "resourceType": "AWS::EC2::VOLUME",
                "resourceCreationTime": "2014-02-27T21:43:53.885Z",
                "tags": {},
                "relationships": [
                    {
                        "resourceId": "i-344c463d",
                        "resourceType": "AWS::EC2::INSTANCE",
                        "name": "Attached to Instance"
                    }
                ],
                "configuration": {
                    "volumeId": "vol-ce676ccc",
```

```
                    "size": 1,
                    "snapshotId": "",
                    "availabilityZone": "us-west-2b",
                    "state": "in-use",
                    "createTime": "2014-02-27T21:43:53.0885+0000",
                    "attachments": [
                        {
                            "volumeId": "vol-ce676ccc",
                            "instanceId": "i-344c463d",
                            "device": "/dev/sdf",
                            "state": "attached",
                            "attachTime": "2014-03-07T23:46:28.0000+0000",
                            "deleteOnTermination": false
                        }
                    ],
                    "tags": [],
                    "volumeType": "standard"
                }
            }
        ],
        "configurationItemDiff": {
            "changeType": "UPDATE",
            "changedProperties": {
                "Configuration.State": {
                    "previousValue": "available",
                    "updatedValue": "in-use",
                    "changeType": "UPDATE"
                },
                "Configuration.Attachments.0": {
                    "updatedValue": {
                        "VolumeId": "vol-ce676ccc",
                        "InstanceId": "i-344c463d",
                        "Device": "/dev/sdf",
                        "State": "attached",
                        "AttachTime": "FriMar0723: 46: 28UTC2014",
                        "DeleteOnTermination": "false"
                    },
                    "changeType": "CREATE"
                }
            }
        }
    },
    "Timestamp": "2014-03-07T23:47:10.001Z",
    "SignatureVersion": "1",
```

```
    "Signature": "LgfJNB5aOk/w3omqsYrv5cUFY8yvIJvO5ZZh46/
KGPApk6HXRTBRlkhjacnxIXJEWsGI9mxvMmoWPLJGYEAR5FF/+/Ro9QTmiTNcEjQ5kB8wGsRWVrk/
whAzT2lVtofc365En2T1Ncd9iSFFXfJchgBmI7EACZ28t
+n2mWFgo57n6eGDvHTedslzC6KxkfWTfXsR6zHXzkB3XuZImktflg3iPKtvBb3Zc9iVbNsBEI4FITFWktSqqomYDjc5h0kg
+qZhMzEbHWpzFlEzvFl55KaZXxDbznBD1ZkqPgno/WufuxszCiMrsmV8pUNUnkU1TA==",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
e372f8ca30337fdb084e8ac449342c77.pem",
    "UnsubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456789012:example:a6859fee-3638-407c-907e-879651c9d143"
}
```


存在关系的资源的配置项

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

1. 您有一个 ID 为 `i-007d374c8912e3e90` 的 Amazon EC2 实例，该实例与 Amazon EC2 安全组 `sg-c8b141b4` 关联。
2. 您更新 EC2 实例，将安全组变更为另一安全组 `sg-3f1fef43`。
3. 由于 EC2 实例与其他资源相关，因此 AWS Config 会创建多个配置项目，如下例所示：

更换安全组时，此通知包含针对 EC2 实例的配置项变更。


```
{
    "Type": "Notification",
    "MessageId": "faeba85e-ef46-570a-b01c-f8b0faae8d5d",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::Instance i-007d374c8912e3e90 Updated
 in Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {
                "Configuration.NetworkInterfaces.0": {
                    "previousValue": {
                        "networkInterfaceId": "eni-fde9493f",
                        "subnetId": "subnet-2372be7b",
                        "vpcId": "vpc-14400670",
                        "description": "",
                        "ownerId": "123456789012",
                        "status": "in-use",
```

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

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

```
                    "changeType": "CREATE"
                },
                "Relationships.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "resourceId": "sg-3f1fef43",
                        "resourceName": null,
                        "resourceType": "AWS::EC2::SecurityGroup",
                        "name": "Is associated with SecurityGroup"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.1": {
                    "previousValue": null,
                    "updatedValue": {
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    },
                    "changeType": "CREATE"
                },
                "Configuration.SecurityGroups.0": {
                    "previousValue": {
                        "groupName": "example-security-group-1",
                        "groupId": "sg-c8b141b4"
                    },
                    "updatedValue": null,
                    "changeType": "DELETE"
                }
            },
            "changeType": "UPDATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [
                {
                    "resourceId": "eni-fde9493f",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::NetworkInterface",
                    "name": "Contains NetworkInterface"
                },
                {
                    "resourceId": "sg-3f1fef43",
                    "resourceName": null,
                    "resourceType": "AWS::EC2::SecurityGroup",
```

```
                "name": "Is associated with SecurityGroup"
            },
            {
                "resourceId": "subnet-2372be7b",
                "resourceName": null,
                "resourceType": "AWS::EC2::Subnet",
                "name": "Is contained in Subnet"
            },
            {
                "resourceId": "vol-0a2d63a256bce35c5",
                "resourceName": null,
                "resourceType": "AWS::EC2::Volume",
                "name": "Is attached to Volume"
            },
            {
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
                "name": "Is contained in Vpc"
            }
        ],
        "configuration": {
            "instanceId": "i-007d374c8912e3e90",
            "imageId": "ami-9be6f38c",
            "state": {
                "code": 16,
                "name": "running"
            },
            "privateDnsName": "ip-172-31-16-84.ec2.internal",
            "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
            "stateTransitionReason": "",
            "keyName": "ec2-micro",
            "amiLaunchIndex": 0,
            "productCodes": [],
            "instanceType": "t2.micro",
            "launchTime": "2017-01-09T20:13:28.000Z",
            "placement": {
                "availabilityZone": "us-east-2c",
                "groupName": "",
                "tenancy": "default",
                "hostId": null,
                "affinity": null
            },
            "kernelId": null,
```

```
                "ramdiskId": null,
                "platform": null,
                "monitoring": {"state": "disabled"},
                "subnetId": "subnet-2372be7b",
                "vpcId": "vpc-14400670",
                "privateIpAddress": "172.31.16.84",
                "publicIpAddress": "54.175.43.43",
                "stateReason": null,
                "architecture": "x86_64",
                "rootDeviceType": "ebs",
                "rootDeviceName": "/dev/xvda",
                "blockDeviceMappings": [{
                    "deviceName": "/dev/xvda",
                    "ebs": {
                        "volumeId": "vol-0a2d63a256bce35c5",
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:03.000Z",
                        "deleteOnTermination": true
                    }
                }],
                "virtualizationType": "hvm",
                "instanceLifecycle": null,
                "spotInstanceRequestId": null,
                "clientToken": "bIYqA1483990561516",
                "tags": [{
                    "key": "Name",
                    "value": "value"
                }],
                "securityGroups": [{
                    "groupName": "example-security-group-2",
                    "groupId": "sg-3f1fef43"
                }],
                "sourceDestCheck": true,
                "hypervisor": "xen",
                "networkInterfaces": [{
                    "networkInterfaceId": "eni-fde9493f",
                    "subnetId": "subnet-2372be7b",
                    "vpcId": "vpc-14400670",
                    "description": "",
                    "ownerId": "123456789012",
                    "status": "in-use",
                    "macAddress": "0e:36:a2:2d:c5:e0",
                    "privateIpAddress": "172.31.16.84",
                    "privateDnsName": "ip-172-31-16-84.ec2.internal",
```

```
                    "sourceDestCheck": true,
                    "groups": [{
                        "groupName": "example-security-group-2",
                        "groupId": "sg-3f1fef43"
                    }],
                    "attachment": {
                        "attachmentId": "eni-attach-85bd89d9",
                        "deviceIndex": 0,
                        "status": "attached",
                        "attachTime": "2017-01-09T19:36:02.000Z",
                        "deleteOnTermination": true
                    },
                    "association": {
                        "publicIp": "54.175.43.43",
                        "publicDnsName": "ec2-54-175-43-43.compute-1.amazonaws.com",
                        "ipOwnerId": "amazon"
                    },
                    "privateIpAddresses": [{
                        "privateIpAddress": "172.31.16.84",
                        "privateDnsName": "ip-172-31-16-84.ec2.internal",
                        "primary": true,
                        "association": {
                            "publicIp": "54.175.43.43",
                            "publicDnsName":
"ec2-54-175-43-43.compute-1.amazonaws.com",
                            "ipOwnerId": "amazon"
                        }
                    }]
                }],
                "iamInstanceProfile": null,
                "ebsOptimized": false,
                "sriovNetSupport": null,
                "enaSupport": true
            },
            "supplementaryConfiguration": {},
            "tags": {"Name": "value"},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:14.328Z",
            "configurationStateId": 1484002214328,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "OK",
            "resourceType": "AWS::EC2::Instance",
            "resourceId": "i-007d374c8912e3e90",
            "resourceName": null,
```

```
            "ARN": "arn:aws:ec2:us-east-2:123456789012:instance/i-007d374c8912e3e90",
            "awsRegion": "us-east-2",
            "availabilityZone": "us-east-2c",
            "configurationStateMd5Hash": "8d0f41750f5965e0071ae9be063ba306",
            "resourceCreationTime": "2017-01-09T20:13:28.000Z"
        },
        "notificationCreationTime": "2017-01-09T22:50:15.928Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.358Z",
    "SignatureVersion": "1",
    "Signature": "lpJTEYOSr8fUbiaaRNw1ECawJFVoD7I67mIeEkfAWJkqvvpak1ULHLlC
+I0sS/01A4P1Yci8GSK/cOEC/O2XBntlw4CAtbMUgTQvb345Z2YZwcpK0kPNi6v6N51DuZ/6DZA8EC
+gVTNTO09xtNIH8aMlvqyvUSXuh278xayExC5yTRXEg+ikdZRd4QzS7obSK1kgRZWI6ipxPNL6rd56/
VvPxyhcbS7Vm40/2+e0nVb3bjNHBxjQTXSs1Xhuc9eP2gEsC4Sl32bGqdeDU1Y4dFGukuzPYoHuEtDPh
+GkLUq3KeiDAQshxAZLmOIRcQ7iJ/bELDJTN9AcX6lqlDZ79w==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


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


```
{
    "Type": "Notification",
    "MessageId": "564d873e-711e-51a3-b48c-d7d064f65bf4",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::EC2::SecurityGroup sg-3f1fef43 Created in
 Account 123456789012",
    "Message": {
        "configurationItemDiff": {
            "changedProperties": {},
            "changeType": "CREATE"
        },
        "configurationItem": {
            "relatedEvents": [],
            "relationships": [{
                "resourceId": "vpc-14400670",
                "resourceName": null,
                "resourceType": "AWS::EC2::VPC",
```

```
                "name": "Is contained in Vpc"
            }],
            "configuration": {
                "ownerId": "123456789012",
                "groupName": "example-security-group-2",
                "groupId": "sg-3f1fef43",
                "description": "This is an example security group.",
                "ipPermissions": [],
                "ipPermissionsEgress": [{
                    "ipProtocol": "-1",
                    "fromPort": null,
                    "toPort": null,
                    "userIdGroupPairs": [],
                    "ipRanges": ["0.0.0.0/0"],
                    "prefixListIds": []
                }],
                "vpcId": "vpc-14400670",
                "tags": []
            },
            "supplementaryConfiguration": {},
            "tags": {},
            "configurationItemVersion": "1.2",
            "configurationItemCaptureTime": "2017-01-09T22:50:15.156Z",
            "configurationStateId": 1484002215156,
            "awsAccountId": "123456789012",
            "configurationItemStatus": "ResourceDiscovered",
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-3f1fef43",
            "resourceName": null,
            "ARN": "arn:aws:ec2:us-east-2:123456789012:security-group/sg-3f1fef43",
            "awsRegion": "us-east-2",
            "availabilityZone": "Not Applicable",
            "configurationStateMd5Hash": "7399608745296f67f7fe1c9ca56d5205",
            "resourceCreationTime": null
        },
        "notificationCreationTime": "2017-01-09T22:50:16.021Z",
        "messageType": "ConfigurationItemChangeNotification",
        "recordVersion": "1.2"
    },
    "Timestamp": "2017-01-09T22:50:16.413Z",
    "SignatureVersion": "1",
    "Signature": "GocX31Uu/zNFo85hZqzsNy30skwmLnjPjj+UjaJzkih
+dCP6gXYGQ0bK7uMzaLL2C/ibYOOsT7I/XY4NW6Amc5T46ydyHDjFRtQi8UfUQTqLXYRTnpOO/
```

```
hyK9lMFfhUNs4NwQpmx3n3mYEMpLuMs8DCgeBmB3AQ+hXPhNuNuR3mJVgo25S8AqphN9O0okZ2MKNUQy8iJm/
CVAx70TdnYsfUMZ24n88bUzAfiHGzc8QTthMdrFVUwXxa1h/7Zl8+A7BwoGmjo7W8CfLDVwaIQv1Uplgk3qd95Z0AXOzXVx
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


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

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

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

UPDATE-CREATE 和 UPDATE-UPDATE

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

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

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

更改类型组合：

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

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

```
{
    "configurationItemDiff": {
        "changedProperties": {
            "Relationships.0": {
                "previousValue": null,
```

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

UPDATE-DELETE

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

已执行的操作：已从 IAM 用户分离账户中存在的托管策略。

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

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

UPDATE-DELETE `configurationItemDiff` 通知示例：

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Configuration.UserPolicyList.0": {
        "previousValue": {
          "policyName": "Test2",
          "policyDocument": "{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
```

```
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/VPCId": "*"
                }
            }
        }
    ]
}"
        },
        "updatedValue": null,
        "changeType": "DELETE"                        >>>>>>>>>>>>>>>>>>>> 3
      }
    },
    "changeType": "UPDATE"
  }
}
```

DELETE-DELETE

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

已执行的操作：已删除账户中存在的 IAM 角色。

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

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

DELETE-DELETE `configurationItemDiff` 通知示例：

```
{
  "configurationItemDiff": {
    "changedProperties": {
      "Relationships.0": {
        "previousValue": {
          "resourceId": "ANPAIJ5MXUKK*********",
          "resourceName": "AWSCloudTrailAccessPolicy",
          "resourceType": "AWS::IAM::Policy",
          "name": "Is attached to CustomerManagedPolicy"
        },
        "updatedValue": null,
```

```
        "changeType": "DELETE"
      },
      "Configuration": {
        "previousValue": {
          "path": "/",
          "roleName": "CloudTrailRole",
          "roleId": "AROAJITJ6YGM*********",
          "arn": "arn:aws:iam::123456789012:role/CloudTrailRole",
          "createDate": "2017-12-06T10:27:51.000Z",
          "assumeRolePolicyDocument": "{"Version":"2012-10-17","Statement":
[{"Sid":"","Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"sts:AssumeRole","Condition":
{"StringEquals":{"sts:ExternalId":"123456"}}}]}",
          "instanceProfileList": [],
          "rolePolicyList": [],
          "attachedManagedPolicies": [
            {
              "policyName": "AWSCloudTrailAccessPolicy",
              "policyArn": "arn:aws:iam::123456789012:policy/AWSCloudTrailAccessPolicy"
            }
          ],
          "permissionsBoundary": null,
          "tags": [],
          "roleLastUsed": null
        },
        "updatedValue": null,
        "changeType": "DELETE"
      }
    },
    "changeType": "DELETE"
}
```

示例配置历史记录传输通知

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

```
{
    "Type": "Notification",
    "MessageId": "ce49bf2c-d03a-51b0-8b6a-ef480a8b39fe",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration History Delivery Completed for
 Account 123456789012",
```

```
    "Message": {
        "s3ObjectKey": "AWSLogs/123456789012/Config/us-east-2/2016/9/27/
ConfigHistory/123456789012_Config_us-
east-2_ConfigHistory_AWS::CloudTrail::Trail_20160927T195818Z_20160927T195818Z_1.json.gz",
        "s3Bucket": "config-bucket-123456789012-ohio",
        "notificationCreationTime": "2016-09-27T20:37:05.217Z",
        "messageType": "ConfigurationHistoryDeliveryCompleted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-09-27T20:37:05.315Z",
    "SignatureVersion": "1",
    "Signature": "OuIcS5RAKXTR6chQEJp3if4KJQVlBz2kmXh7QE1/
RJQiCPsCNfG0J0rUZ1rqfKMqpps/Ka+zF0kg4dUCWV9PF0dliuwnjfbtYmDZpP4EBOoGmxcTliUn1AIe/
yeGFDuc6P3EotP3zt02rhmxjezjf3c11urstFZ8rTLVXp0z0xeyk4da0UetLsWZxUFEG0Z5uhk09mBo5dg/4mryIOovidhr
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


示例配置快照传输开始通知

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


```
{
    "Type": "Notification",
    "MessageId": "a32d0487-94b1-53f6-b4e6-5407c9c00be6",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Configuration Snapshot Delivery Started for
 Account 123456789012",
    "Message": {
        "configSnapshotId": "108e0794-84a7-4cca-a179-76a199ddd11a",
        "notificationCreationTime": "2016-10-18T17:26:09.572Z",
        "messageType": "ConfigurationSnapshotDeliveryStarted",
        "recordVersion": "1.1"
    },
    "Timestamp": "2016-10-18T17:26:09.840Z",
    "SignatureVersion": "1",
    "Signature": "BBA0DeKsfteTpYyZH5HPANpOLmW/jumOMBsghRq/kimY9tjNlkF/
V3BpLG1HVmDQdQzBh6oKE0h0rxcazbyGf5KF5W5r1zKKlEnS9xugFzALPUx//
olSJ4neWalLBKNIq1xvAQgu9qHfDR7dS2aCwe4scQfqOjn1Ev7PlZqxmT+ux3SR/
C54cbfcduDpDsPwdo868+TpZvMtaU30ySnX04fmOgxoiA8AJO/EnjduQ08/zd4SYXhm
```

```
+H9wavcwXB9XECelHhRW70Y+wHQixfx40S1SaSRzvnJE+m9mHphFQs64YraRDRv6tMaenTk6CVPO
+81ceAXIg2E1m7hZ7lz4PA==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


示例配置快照传输通知

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


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

```
}
```

示例合规性变更通知

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

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

```
{
    "Type": "Notification",
    "MessageId": "11fd05dd-47e1-5523-bc01-55b988bb9478",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] AWS::::Account 123456789012 is COMPLIANT with
 cloudtrail-enabled in Accoun...",
    "Message": {
        "awsAccountId": "123456789012",
        "configRuleName": "cloudtrail-enabled",
        "configRuleARN": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-9rpvxc",
        "resourceType": "AWS::::Account",
        "resourceId": "123456789012",
        "awsRegion": "us-east-2",
        "newEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T19:48:40.619Z"
            },
            "complianceType": "COMPLIANT",
            "resultRecordedTime": "2016-09-27T19:48:41.405Z",
            "configRuleInvokedTime": "2016-09-27T19:48:40.914Z",
            "annotation": null,
            "resultToken": null
        },
        "oldEvaluationResult": {
            "evaluationResultIdentifier": {
                "evaluationResultQualifier": {
                    "configRuleName": "cloudtrail-enabled",
                    "resourceType": "AWS::::Account",
```

```
                    "resourceId": "123456789012"
                },
                "orderingTimestamp": "2016-09-27T16:30:49.531Z"
            },
            "complianceType": "NON_COMPLIANT",
            "resultRecordedTime": "2016-09-27T16:30:50.717Z",
            "configRuleInvokedTime": "2016-09-27T16:30:50.105Z",
            "annotation": null,
            "resultToken": null
        },
        "notificationCreationTime": "2016-09-27T19:48:42.620Z",
        "messageType": "ComplianceChangeNotification",
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-09-27T19:48:42.749Z",
    "SignatureVersion": "1",
    "Signature": "XZ9FfLb2ywkW9yj0yBkNtIP5q7Cry6JtCEyUiHmG9gpOZi3seQ41udhtAqCZoiNiizAEi
+6gcttHCRV1hNemzp/
YmBmTfO6azYXt0FJDaEvd86k68VCS9aqRlBBjYlNo7ILi4Pqd5rE4BX2YBQSzcQyERGkUfTZ2BIFyAmb1Q/
y4/6ez8rDyi545FDSlgcGEb4LKLNR6eDi4FbKtMGZHA7Nz8obqs1dHbgWYnp3c80mVLl7ohP4hilcxdywAgXrbsN32ekYr1
+BIZ21ZtkcUtY5B3ImgRlUO7Yhn3L3c6rZxQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```


示例：Config 配置项变更 | Amazon EventBridge


```
{
  "version": "0",
  "id": "00bdf13e-1111-b2f5-cef0-e9cbbe7cd533",
  "detail-type": "Config Configuration Item Change",
  "source": "aws.config",
  "account": "123456789012",
  "time": "2022-03-16T01:10:51Z",
  "region": "us-east-1",
  "resources": ["arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95"],
  "detail": {
    "recordVersion": "1.3",
    "messageType": "ConfigurationItemChangeNotification",
```

```
    "configurationItemDiff": {
      "changedProperties": {
        "Configuration.FileSystemTags.0": {
          "updatedValue": {
            "Key": "test",
            "Value": "me"
          },
          "changeType": "CREATE"
        },
        "Tags.2": {
          "updatedValue": "me",
          "changeType": "CREATE"
        }
      },
      "changeType": "UPDATE"
    },
    "notificationCreationTime": "2022-03-16T01:10:51.976Z",
    "configurationItem": {
      "relatedEvents": [],
      "relationships": [],
      "configuration": {
        "FileSystemId": "fs-01f0d526165b57f95",
        "Arn": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
        "Encrypted": true,
        "FileSystemTags": [{
          "Key": "Name",
          "Value": "myname"
        }, {
          "Key": "test",
          "Value": "me"
        }],
        "PerformanceMode": "generalPurpose",
        "ThroughputMode": "bursting",
        "LifecyclePolicies": [{
          "TransitionToIA": "AFTER_30_DAYS"
        }, {
          "TransitionToPrimaryStorageClass": "AFTER_1_ACCESS"
        }],
        "BackupPolicy": {
          "Status": "ENABLED"
        },
        "FileSystemPolicy": {},
```

```
        "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/0e6c91d5-e23b-4ed3-
bd36-1561fbbc0a2d"
      },
      "supplementaryConfiguration": {},
      "tags": {
        "aws:elasticfilesystem:default-backup": "enabled",
        "test": "me",
        "Name": "cloudcontroltest1"
      },
      "configurationItemVersion": "1.3",
      "configurationItemCaptureTime": "2022-03-16T01:10:50.837Z",
      "configurationStateId": 1647393050837,
      "awsAccountId": "123456789012",
      "configurationItemStatus": "OK",
      "resourceType": "AWS::EFS::FileSystem",
      "resourceId": "fs-01f0d526165b57f95",
      "resourceName": "fs-01f0d526165b57f95",
      "ARN": "arn:aws:elasticfilesystem:us-east-1:123456789012:file-system/
fs-01f0d526165b57f95",
      "awsRegion": "us-east-1",
      "availabilityZone": "Regional",
      "configurationStateMd5Hash": ""
    }
  }
}
```

示例规则评估开始通知

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

```
{
    "Type": "Notification",
    "MessageId": "358c8e65-e27a-594e-82d0-de1fe77393d7",
    "TopicArn": "arn:aws:sns:us-east-2:123456789012:config-topic-ohio",
    "Subject": "[AWS Config:us-east-2] Config Rules Evaluation Started for Account
 123456789012",
    "Message": {
        "awsAccountId": "123456789012",
        "awsRegion": "us-east-2",
        "configRuleNames": ["iam-password-policy"],
        "notificationCreationTime": "2016-10-13T21:55:21.339Z",
        "messageType": "ConfigRulesEvaluationStarted",
```

```
        "recordVersion": "1.0"
    },
    "Timestamp": "2016-10-13T21:55:21.575Z",
    "SignatureVersion": "1",
    "Signature": "DE431D+24zzFRboyPY2bPTsznJWe8L6TjDC+ItYlLFkE9jACSBl3sQ1uSjYzEhEbN7Cs
+wBoHnJ/DxOSpyCxt4giqgKd+H2I636BvrQwHDhJwJm7qI6P8IozEliRvRWbM38zDTvHqkmmXQbdDHRsK/
MssMeVTBKuW0x8ivMrj+KpwuF57tE62eXeFhjBeJ0DKQV+aC+i3onsuT7HQvXQDBPdOM
+cSuLrJaMQJ6TcMU5G76qg/
gl494ilb4Vj4udboGWpHSgUvI3guFsc1SsTrlWXQKXabWtsCQPfdOhkKgmViCfMZrLRp8Pjnu
+uspYQELkEfwBchDVVzd15iMrAzQ==",
    "SigningCertURL": "https://sns.us-east-2.amazonaws.com/SimpleNotificationService-
b95095beb82e8f6a046b3aafc7f4149a.pem",
    "UnsubscribeURL": "https://sns.us-east-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-east-2:123456789012:config-topic-
ohio:956fe658-0ce3-4fb3-b409-a45f22a3c3d4"
}
```

示例过大配置项变更通知

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

下面的示例通知显示了 Amazon EC2 实例的一个配置项。通知中包含变更摘要以及通知在 Amazon S3 存储桶中的位置。

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

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

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

```
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "8f1ee69b287895a0f8bc5753eca68e96",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": "my-bucket/AWSLogs/123456789012/Config/
us-west-2/2016/10/6/OversizedChangeNotification/AWS::EC2::Instance/
resourceId_14b76876-7969-4097-ab8e-a31942b02e80/123456789012_Config_us-
west-2_ChangeNotification_AWS::EC2::Instance_resourceId_14b76876-7969-4097-ab8e-
a31942b02e80_20161006T164616Z_0.json.gz",
        "errorCode": null,
        "errorMessage": null
      },
      "notificationCreationTime": "2016-10-06T16:46:16.261Z",
      "messageType": "OversizedConfigurationItemChangeNotification",
      "recordVersion": "1.0"
    }
```

示例传输失败通知

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

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

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

    New State Record Summary:
```

```
    ----------------------------
    {
      "configurationItemSummary": {
        "changeType": "UPDATE",
        "configurationItemVersion": "1.2",
        "configurationItemCaptureTime": "2016-10-06T16:46:13.749Z",
        "configurationStateId": 0,
        "awsAccountId": "123456789012",
        "configurationItemStatus": "OK",
        "resourceType": "AWS::EC2::Instance",
        "resourceId": "test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "resourceName": null,
        "ARN": "arn:aws:ec2:us-west-2:123456789012:instance/
test_resourceId_014b953d-75e3-40ce-96b9-c7240b975457",
        "awsRegion": "us-west-2",
        "availabilityZone": null,
        "configurationStateMd5Hash": "6de64b95eacd30e7b63d4bba7cd80814",
        "resourceCreationTime": "2016-10-06T16:46:10.489Z"
      },
      "s3DeliverySummary": {
        "s3BucketLocation": null,
        "errorCode": "NoSuchBucket",
        "errorMessage": "Failed to deliver notification to bucket: bucket-example for
 account 123456789012 in region us-west-2."
      },
      "notificationCreationTime": "2016-10-06T16:46:13.749Z",
      "messageType": "OversizedConfigurationItemChangeDeliveryFailed",
      "recordVersion": "1.0"
    }
```

使用管理和查看 AWS 资源配置 AWS Config

AWS Config 允许您评估、审计和评估 AWS 资源的配置。

AWS 资源是您使用、 AWS Command Line Interface (CLI) AWS Management Console、 AWS 软件开发工具包或 AWS 合作伙伴工具创建和管理的实体。 AWS 资源示例包括亚马逊 EC2 实例、安全组、亚马逊 VPC 和亚马逊弹性区块存储。 AWS Config 使用其唯一标识符来指代每种资源，例如资源 ID 或 A mazon 资源名称 (ARN)。

一些常见的用例包括：

- 云管理员：您可以跟踪和管理资源配置，以帮助确保合规性、解决问题并保持对 AWS 环境的了解
- 安全分析师：您可以根据所需状态评估资源配置，以帮助识别漏洞和评估安全状况。
- 合规官员：您可以持续审核和监控资源配置，以帮助确保遵守组织政策和行业标准。

主题

- 查看 AWS Config 控制面板
- 支持的资源类型
- 按区域可用性列出的资源覆盖范围
- 录制 AWS 资源
- 记录第三方资源的配置
- 记录托管实例的软件配置
- 查看 资源配置和历史记录
- 标记您的 AWS Config 资源

查看 AWS Config 控制面板

使用控制面板查看您的资源、规则、合规包及其合规状态的概览，并可视化您在 Amazon CloudWatch 上的 AWS Config 使用情况和成功指标。此页面可帮助您快速识别账户中的热门资源、您的 AWS 账户中合规性最低的一致性包 AWS 账户、您的哪些规则或资源不合规 AWS 账户、哪些流量推动了您的 AWS Config 使用量，以及工作流程中出现的衡量成功和失败的关键指标。

使用 AWS Config 控制面板

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在左侧导航窗格中，选择控制面板。

目录

- 合规性和资源清单
- AWS Config 使用情况和成功指标

合规性和资源清单

设置完成后， AWS Config 开始记录您的指定资源并根据您的规则对其进行评估。可能需要几分钟 AWS Config 才能显示您的资源、规则、合规包及其合规状态。

按合规性分数列出的合规包

按合规性分数列出的合规包最多显示 10 个合规性分数最低的合规包。合规性分数是合规包中的合规规则资源组合数量与合规包中可能的规则资源组合总数的百分比。

该指标为您提供合规包的合规性状态的简要视图，可用于识别、调查和了解合规包的合规性级别。您可以使用合规性分数来跟踪修正进度，对不同的需求集进行比较，并查看特定更改或部署对合规包的影响。

要在详细视图中查看合规包的部署状态、合规性分数、合规性分数时间线和规则，请选择合规包下的合规包的名称。

Compliance status

合规性状态显示您的合规和不合规规则以及合规和不合规资源的数量。根据对相关规则的评估，确定资源是合规还是不合规。如果资源不符合规则的规范，则该资源和规则将被标记为不合规。

要查看不合规规则和资源的列表，请选择不合规规则或不合规资源。

按不合规资源列出的规则

按不合规资源列出的规则按资源数量的降序显示排名靠前的不合规规则。选择一条规则以查看其详细信息、参数，以及该特定规则范围内的资源。

要查看不合规规则的完整列表，请选择查看所有不合规规则。

资源清单

资源清单按资源数量的降序显示记录的资源总数，以及您的 AWS 账户每种资源类型的数量。 AWS Config 要打开某一资源类型的所有资源，请选择该资源类型以进入其资源清单页面。

您可以使用下拉列表来指明要查看哪些资源总计。默认情况下，它设置为查看所有资源，但您可以将其更改为 AWS 资源、第三方资源或自定义资源。

> **Note**
>
> 由于以下原因，控制面板上可能会出现 “使用 Config 规则评估您的 AWS 资源配置” 消息：
>
> - 您尚未为自己设置 AWS Config 规则 AWS 账户. 您可以选择 Add rule 以转到 Rules 页面。
> - AWS Config 仍在根据您的规则评估您的资源。您可以刷新该页面来查看最新的评估结果。
> - AWS Config 根据您的规则评估了您的资源，但未在范围内发现任何资源。您可以在 “设置” 页面中指定 AWS Config 要记录的资源。有关更多信息，请参阅 录制 AWS 资源。

AWS Config 使用情况和成功指标

您可以在控制台中使用 Amazon AWS Config 控制 CloudWatch 面板来直观显示您的 AWS Config 使用情况和成功指标。

对于每个控制面板，您都可以执行以下操作：

- 调整控制面板的时间范围以显示过去 3 小时、1 天或 1 周的数据。
- 选择 “日历” 图标输入自定义时间范围：过去指定时间段的相对时间或两个日期之间的绝对时间范围。
- 您可以更改时间格式，以 UTC（协调世界时）或本地时区（在设备操作系统中指定为本地时区的时区）显示仪表板数据。
- 使用刷新图标旁边的下拉箭头来指定控制面板中数据的刷新频率，或者关闭自动刷新。选择关闭、10 秒、1 分钟、2 分钟、5 分钟或 15 分钟来更改刷新间隔。
- 选择 “更多选项”（垂直省略号菜单），将您当前在控制 AWS Config 面板中查看的 AWS Config 使用量指标或 AWS Config 成功指标添加到 CloudWatch 控制台。这将在 CloudWatch 控制台中打开一个新选项卡，允许您使用从当前 AWS Config 使用量指标或 AWS Config 成功指标中 CloudWatch 复制的信息创建新的自定义仪表板。

如果要使用对这些指标进行其他分析 CloudWatch，请在 CloudWatch 控制台的左侧导航窗格中选择 M et rics，然后选择 AWS/Config。有关您可以通过 CloudWatch 控制台执行的操作的更多信息，请参阅CloudWatch 用户指南中的使用亚马逊控制 CloudWatch 面板和使用亚马逊 CloudWatch 指标。

AWS Config 使用量指标

指标	描述	单位	
`Configuration Items Recorded`	为每种资源类型或所有资源类型记录的配置项数。配置项目表示所支持 AWS 资源的各种属性的 point-in-time 视图。有关配置项或支持的资源类型的更多信息，请参阅配置项和支持的资源类型。	计数	

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

AWS Config 成功指标

指标	描述	单位	
`Change Notifications Delivery Failed`	向您的配送渠道的 Amazon SNS 主题发送的变更通知失败的数量。更改通知会通知您有关 AWS 资源配置状态的更改。您可以使用 ConfigStreamDeliveryInfoAPI 获取上次尝试交付`lastErrorMessage` 的变更通知的`lastErrorCode` 或。有关更多信息，请参阅管理传输通道。	计数	
`Config History Export Failed`	导出到您的 Amazon S3 存储桶的失败配置历史记录的数量。配置历史记录是给定资源在指定时间段的配置项集合。有关配置历史记录的更多信息，请参阅配置历史记录。	计数	
`Configuration Recorder Insufficient`	由于配置记录器的 IAM 角色策略权限不足而导致的权限访问失败次数。配置记录器可在您的资源配置中检测更改，并将这些更改捕获为配置项。配置记录器需要必要的 IAM 权限，才能	计数	

指标	描述	单位
Permissions Failure	记录您的 AWS 资源配置。有关更多信息，请参阅用于获取配置详细信息的 IAM 角色策略。	
Config Snapshot Export Failed	导出到您的 Amazon S3 存储桶的配置快照失败的次数。配置快照是您账户中受支持资源的配置项集合。有关配置快照的更多信息，请参阅配置	快照。	计数

支持的资源类型

> **Important**
>
> 该页面在每个月初按每月的节奏更新。

AWS Config 支持以下 AWS 资源类型和资源关系。

- 有关资源类型的更多详细信息，请参阅《 AWS CloudFormation 用户指南》中AWS 资源和属性类型参考中的参考信息（例如语法、属性和返回值）。
- 为了进行 AWS Config 录制，某些 AWS 地区支持这些资源类型的子集。有关哪些区域支持哪些资源类型的信息，请参阅按区域可用性列出的资源覆盖范围。
- 的高级查询 AWS Config 支持这些资源类型的子集。有关那些支持的资源类型列表，请参阅支持的高级查询资源类型。
- 的主动评估 AWS Config 支持这些资源类型中的一部分。有关那些支持的资源类型列表，请参阅主动评估支持的资源类型。
- 由于定期规则不依赖于配置项，因此定期规则可在配置记录器未启用的情况下运行。有关变更触发规则和定期规则之间区别的更多信息，请参阅规则的评估模式和触发器 AWS Config 类型。

> **Note**
>
> 在指定 AWS Config 要跟踪的资源类型之前，请检查按区域可用性划分的资源覆盖率，以查看您设置的 AWS 区域是否支持该资源类型 AWS Config。如果至少有一个区域支持某种资源类

型，则即使您设置的区域不支持指定的资源类型 AWS Config，您也可以在支持的所有 AWS 区域中启用该资源类型的记录 AWS Config。 AWS Config

Amazon AppStream

AWS 服务	资源类型值	关系	相关资源
Amazon AppStream	`AWS::AppStream::DirectoryConfig`	NA	NA
	`AWS::AppStream::Application`	NA	NA
	`AWS::AppStream::Stack`	NA	NA
	`AWS::AppStream::Fleet`	NA	NA

Amazon AppFlow

AWS 服务	资源类型值	关系	相关资源
Amazon AppFlow	`AWS::AppFlow::Flow`	NA	NA

AWS 服务	资源类型值	关系	相关资源
Amazon AppIntegrations	`AWS::AppIntegratio`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`ns::Event Integration`		

Amazon API Gateway

AWS 服务	资源类型值	关系	相关资源
API Gateway	`AWS::ApiGateway::Stage`	包含在	ApiGateway 休息 Api
		关联到	WAFRegional WebACL
	`AWS::ApiGateway::RestApi`	contains	ApiGateway 舞台
API Gateway V2	`AWS::ApiGatewayV2::Stage`	包含在	ApiGatewayV2 Api
	`AWS::ApiGatewayV2::Api`	contains	ApiGatewayV2 舞台

要详细了解如何 AWS Config 与 Amazon API Gateway 集成，请参阅使用监控 API 网关 API 配置 AWS Config。

Amazon Athena

AWS 服务	资源类型值	关系	相关资源
Amazon Athena	`AWS::Athena::WorkGroup`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`AWS::Athena::DataCatalog`	NA	NA
	`AWS::Athena::PreparedStatement`	NA	NA

Amazon CloudFront

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

Amazon CloudWatch

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

AWS 服务	资源类型值	关系	相关资源
	`AWS::CloudWatch::MetricStream`	NA	NA
亚马逊 CloudWatch 日志	`AWS::Logs::Destination`	NA	NA
亚马逊 CloudWatch RUM	`AWS::RUM::AppMonitor`	NA	NA
CloudWatch 很明显，亚马逊	`AWS::Evidently::Project`	NA	NA
	`AWS::Evidently::Launch`	NA	NA
	`AWS::Evidently::Segment`	NA	NA

Amazon CodeGuru

AWS 服务	资源类型值	关系	相关资源
Amazon CodeGuru Reviewer	`AWS::CodeGuruReviewer::RepositoryAssociation`	NA	NA
Amazon P CodeGuru rofiler	`AWS::CodeGuruProfiler::ProfilingGroup`	NA	NA

Amazon Cognito

AWS 服务	资源类型值	关系	相关资源
Amazon Cognito	`AWS::Cognito::UserPool`	NA	NA
	`AWS::Cognito::UserPoolClient`	NA	NA
	`AWS::Cognito::UserPoolGroup`	NA	NA

Amazon Connect

AWS 服务	资源类型值	关系	相关资源
Amazon Connect	`AWS::Connect::PhoneNumber`	NA	NA
	`AWS::Connect::QuickConnect`	NA	NA
	`AWS::Connect::Instance`	NA	NA
Amazon Connect Customer Profiles	`AWS::CustomerProfiles::Domain`	NA	NA
	`AWS::CustomerProfi`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`les::Objectype`		

Amazon Detective

AWS 服务	资源类型值	关系	相关资源
Amazon Detective	`AWS::Detective::Graph`	NA	NA

Amazon DynamoDB

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

Amazon Elastic Compute Cloud

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

AWS 服务	资源类型值	关系	相关资源
		包含在	EC2 专用主机
			路由表
			子网
			Virtual Private Cloud (VPC)
	`AWS::EC2::NetworkInterface`	关联到	EC2 安全组
		挂载到	EC2 弹性 IP (EIP)
			EC2 实例
		包含在	路由表
			子网
			Virtual Private Cloud (VPC)
	`AWS::EC2::SecurityGroup` *	关联到	EC2 实例
			EC2 网络接口
			Virtual Private Cloud (VPC)
	`AWS::EC2::NatGateway`	包含在	Virtual Private Cloud (VPC)
		包含在	子网
	`AWS::EC2::EgressOnlyInternetGateway`	挂载到	Virtual Private Cloud (VPC)

AWS 服务	资源类型值	关系	相关资源
	AWS::EC2::EC2Fleet	NA	NA
	AWS::EC2::SpotFleet	NA	NA
	AWS::EC2::PrefixList	NA	NA
	AWS::EC2::FlowLog	NA	NA
	AWS::EC2::TransitGateway	NA	NA
	AWS::EC2::TransitGatewayAttachment	NA	NA
	AWS::EC2::TransitGatewayRouteTable	NA	NA
	AWS::EC2::VPCEndpoint	包含在	Virtual Private Cloud (VPC)
		挂载到	网络接口
		包含在	子网
		包含在	路由表

AWS 服务	资源类型值	关系	相关资源
	AWS::EC2::VPCEndpointService	关联到	ElasticLoadBalancingv2 LoadBalancer
	AWS::EC2::VPCPeeringConnection	关联到	Virtual Private Cloud (VPC)
	AWS::EC2::RegisteredHAInstance	关联到	EC2 实例
	AWS::EC2::SubnetRouteTableAssociation	NA	NA
	AWS::EC2::LaunchTemplate	NA	NA
	AWS::EC2::NetworkInsightsAccessScopeAnalysis	NA	NA
	AWS::EC2::TrafficMirrorTarget	NA	NA
	AWS::EC2::TrafficMirrorSession	NA	NA

AWS 服务	资源类型值	关系	相关资源
	AWS::EC2::DHCPOptions	NA	NA
	AWS::EC2::IPAM	NA	NA
	AWS::EC2::NetworkInsightsPath	NA	NA
	AWS::EC2::TrafficMirrorFilter	NA	NA
	AWS::EC2::CapacityReservation	NA	NA
	AWS::EC2::ClientVpnEndpoint	NA	NA
	AWS::EC2::CustomerGateway	挂载到	VPN 连接
	AWS::EC2::InternetGateway	挂载到	Virtual Private Cloud (VPC)
	AWS::EC2::NetworkAcl	NA	NA
	AWS::EC2::RouteTable	contains	EC2 实例
			EC2 网络接口
			子网

AWS 服务	资源类型值	关系	相关资源
			VPN 网关
		包含在	Virtual Private Cloud (VPC)
	AWS::EC2::Subnet	contains	EC2 实例
			EC2 网络接口
		挂载到	网络 ACL
		包含在	路由表
			Virtual Private Cloud (VPC)
	AWS::EC2::VPC	contains	EC2 实例
			EC2 网络接口
			网络 ACL
			路由表
			子网
		关联到	安全组
		挂载到	互联网网关
			VPN 网关
	AWS::EC2::VPNConnection	挂载到	客户网关
			VPN 网关
	AWS::EC2::VPNGateway	挂载到	Virtual Private Cloud (VPC)
			VPN 连接

AWS 服务	资源类型值	关系	相关资源
		包含在	路由表
	AWS::EC2::IPAMScope	NA	NA
	AWS::EC2::CarrierGateway	NA	NA
	AWS::EC2::TransitGatewayConnect	NA	NA
	AWS::EC2::IPAMPool	NA	NA
	AWS::EC2::TransitGatewayMulticastDomain	NA	NA
	AWS::EC2::NetworkInsightsAccessScope	NA	NA
	AWS::EC2::NetworkInsightsAnalysis	NA	NA
Amazon Elastic Block Store	AWS::EC2::Volume	挂载到	EC2 实例
EC2 Image Builder	AWS::ImageBuilder::ImagePipeline	NA	NA

AWS 服务	资源类型值	关系	相关资源
	AWS::ImageBuilder::DistributionConfiguration	NA	NA
	AWS::ImageBuilder::ContainerRecipe	NA	NA
	AWS::ImageBuilder::InfrastructureConfiguration	NA	NA
	AWS::ImageBuilder::ImageRecipe	NA	NA

*AWS Config 记录专用主机的配置详细信息以及您在这些主机上启动的实例。因此，当您报告服务器绑定软件许可证的合规性时，您可以 AWS Config 将其用作数据源。例如，您可以查看某个实例的配置历史记录并确定其基于哪个 Amazon 系统映像 (AMI)。然后，您可以查找相应主机的配置历史记录（包括套接字和核心数量之类的详细信息），以检查该主机是否符合 AMI 的许可证要求。有关更多信息，请参阅 Amazon EC2 用户指南 AWS Config中的使用跟踪配置更改。

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

Amazon Elastic Container Registry

AWS 服务	资源类型值	关系	相关资源
Amazon Elastic Container Registry	`AWS::ECR::Repository`	NA	NA
	`AWS::ECR::Registry Policy`	NA	NA
	`AWS::ECR::PullThroughCacheRule`	NA	NA
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	NA	NA

Amazon Elastic Container Service

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

AWS 服务	资源类型值	关系	相关资源
	`AWS::ECS::Capacity Provider`	NA	NA

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

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

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

Amazon Elastic File System

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

Amazon Elastic Kubernetes Service

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

AWS 服务	资源类型值	关系	相关资源
	`AWS::EKS::IdentityProviderConfig`	NA	NA
	`AWS::EKS::Addon`	NA	NA

Amazon EMR

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

Amazon EventBridge

AWS 服务	资源类型值	关系	相关资源
Amazon EventBridge	`AWS::Events::EventBus`	NA	NA
	`AWS::Events::ApiDestination`	NA	NA
	`AWS::Events::Archive`	NA	NA
	`AWS::Events::Endpoint`	NA	NA
	`AWS::Events::Connection`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`AWS::Events::Rule`	NA	NA
亚马逊 EventBridge 架构	`AWS::EventSchemas::RegistryPolicy`	NA	NA
	`AWS::EventSchemas::Discoverer`	NA	NA
	`AWS::EventSchemas::Schema`	NA	NA

Amazon Forecast

AWS 服务	资源类型值	关系	相关资源
Amazon Forecast	`AWS::Forecast::Dataset`	NA	NA
	`AWS::Forecast::DatasetGroup`	NA	NA

Amazon Fraud Detector

AWS 服务	资源类型值	关系	相关资源
Amazon Fraud Detector	`AWS::FraudDetector::Label`	NA	NA
	`AWS::FraudDetector::EntityType`	NA	NA
	`AWS::FraudDetector::Variable`	NA	NA
	`AWS::FraudDetector::Outcome`	NA	NA

Amazon GuardDuty

AWS 服务	资源类型值	关系	相关资源
Amazon GuardDuty	`AWS::GuardDuty::Detector`	NA	NA
	`AWS::GuardDuty::ThreatIntelSet`	NA	NA
	`AWS::GuardDuty::IPSet`	NA	NA
	`AWS::GuardDuty::Filter`	NA	NA

Amazon Inspector

AWS 服务	资源类型值	关系	相关资源
Amazon Inspector	`AWS::InspectorV2::Filter`	NA	NA

Amazon Interactive Video Service

AWS 服务	资源类型值	关系	相关资源
Amazon Interactive Video Service	`AWS::IVS::Channel`	NA	NA
	`AWS::IVS::RecordingConfiguration`	NA	NA
	`AWS::IVS::PlaybackKeyPair`	NA	NA

Amazon Keyspaces（Apache Cassandra 兼容）

AWS 服务	资源类型值	关系	相关资源
Amazon Keyspaces（Apache Cassandra 兼容）	`AWS::Cassandra::Keyspace`	NA	NA

亚马逊 OpenSearch 服务

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

> **Note**
>
> 2021 年 9 月 8 日，亚马逊 Elasticsearch 服务更名为亚马逊服务。 OpenSearch OpenSearch 服务支持 OpenSearch 以及传统的 Elasticsearch OSS。有关更多信息，请参阅 Amazon OpenSearch 服务-变更摘要。
> 即使您将一个或多个域名升级到，您也可以在几周内继续在现有`AWS::Elasticsearch::Domain`资源类型`AWS::OpenSearch::Domain`下看到您的数据 OpenSearch。

Amazon Personalize

AWS 服务	资源类型值	关系	相关资源
Amazon Personalize	`AWS::Personalize::Dataset`	NA	NA
	`AWS::Personalize::Schema`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	AWS::Personalize::Solution	NA	NA
	AWS::Personalize::DatasetGroup	NA	NA

Amazon Pinpoint

AWS 服务	资源类型值	关系	相关资源
Amazon Pinpoint	AWS::Pinpoint::ApplicationSettings	NA	NA
	AWS::Pinpoint::Segment	NA	NA
	AWS::Pinpoint::App	NA	NA
	AWS::Pinpoint::Campaign	NA	NA
	AWS::Pinpoint::InAppTemplate	NA	NA
	AWS::Pinpoint::EmailChannel	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`AWS::Pinpoint::EmailTemplate`	NA	NA
	`AWS::Pinpoint::EventStream`	NA	NA

Amazon Quantum Ledger Database (Amazon QLDB)

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

Amazon Kendra

AWS 服务	资源类型值	关系	相关资源
Amazon Kendra	`AWS::Kendra::Index`	NA	NA

Amazon Kinesis

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

AWS 服务	资源类型值	关系	相关资源
Amazon Kinesis Analytics V2	`AWS::KinesisAnalyticsV2::Application`	NA	NA
Amazon Data Firehose	`AWS::KinesisFirehose::DeliveryStream`	NA	NA
Kinesis 视频流	`AWS::KinesisVideo::SignalingChannel`	NA	NA
	`AWS::KinesisVideo::Stream`	NA	NA

Amazon Lex

AWS 服务	资源类型值	关系	相关资源
Amazon Lex	`AWS::Lex::BotAlias`	NA	NA
	`AWS::Lex::Bot`	NA	NA

Amazon Lightsail

AWS 服务	资源类型值	关系	相关资源
Amazon Lightsail	`AWS::Lightsail::Disk`	NA	NA
	`AWS::Lightsail::Certificate`	NA	NA
	`AWS::Lightsail::Bucket`	NA	NA
	`AWS::Lightsail::StaticIp`	NA	NA

Amazon Lookout for Metrics

AWS 服务	资源类型值	关系	相关资源
Amazon Lookout for Metrics	`AWS::LookoutMetrics::Alert`	NA	NA

Amazon Lookout for Vision

AWS 服务	资源类型值	关系	相关资源
Amazon Lookout for Vision	`AWS::LookoutVision::Project`	NA	NA

Amazon Managed Grafana

AWS 服务	资源类型值	关系	相关资源
Amazon Managed Grafana	`AWS::Grafana::Workspace`	NA	NA

Amazon Managed Service for Prometheus

AWS 服务	资源类型值	关系	相关资源
Amazon Managed Service for Prometheus	`AWS::APS::RuleGroupsNamespace`	NA	NA

适用于 Redis 的 Amazon MemoryDB

AWS 服务	资源类型值	关系	相关资源
适用于 Redis 的 Amazon MemoryDB	`AWS::MemoryDB::SubnetGroup`	NA	NA

Amazon MQ

AWS 服务	资源类型值	关系	相关资源
Amazon MQ	`AWS::AmazonMQ::Broker`	NA	NA

Amazon Managed Streaming for Apache Kafka

AWS 服务	资源类型值	关系	相关资源
Amazon Managed Streaming for Apache Kafka	`AWS::MSK::Cluster`	NA	NA
	`AWS::MSK::Configuration`	NA	NA
	`AWS::MSK::BatchScramSecret`	NA	NA
	`AWS::MSK::ClusterPolicy`	NA	NA
	`AWS::MSK::VpcConnection`	NA	NA
Amazon Managed Streaming for Apache Kafka Connect	`AWS::KafkaConnect::Connector`	NA	NA

Amazon Redshift

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

AWS 服务	资源类型值	关系	相关资源
	AWS::Redshift::ClusterParameterGroup	NA	NA
	AWS::Redshift::ClusterSecurityGroup	NA	NA
	AWS::Redshift::ScheduledAction	NA	NA
	AWS::Redshift::ClusterSnapshot	关联到	集群
			Virtual Private Cloud (VPC)
	AWS::Redshift::ClusterSubnetGroup	关联到	子网
			Virtual Private Cloud (VPC)
	AWS::Redshift::EventSubscription	NA	NA
	AWS::Redshift::EndpointAccess	NA	NA
	AWS::Redshift::EndpointAuthorization	NA	NA

Amazon Relational Database Service

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

AWS 服务	资源类型值	关系	相关资源
	AWS::RDS::OptionGroup	NA	NA

Amazon Route 53

AWS 服务	资源类型值	关系	相关资源
Amazon Route 53	AWS::Route53::HostedZone	NA	NA
	AWS::Route53::HealthCheck	NA	NA
Amazon Route 53 Resolver	AWS::Route53Resolver::ResolverEndpoint	NA	NA
	AWS::Route53Resolver::ResolverRule	NA	NA
	AWS::Route53Resolver::ResolverRuleAssociation	NA	NA
	AWS::Route53Resolver::FirewallDomainList	NA	NA
	AWS::Route53Resolver::FirewallRuleGroupAssociation	NA	NA
	AWS::Route53Resolver::ResolverQueryLoggingConfig	NA	NA
	AWS::Route53Resolver::ResolverQueryLoggingConfigAssociation	NA	NA
	AWS::Route53Resolver::FirewallRuleGroup	NA	NA
Amazon Route 53 应用程序恢	AWS::Route53RecoveryReadiness::Cell	NA	NA
	AWS::Route53RecoveryReadiness::ReadinessCheck	NA	NA

AWS 服务	资源类型值	关系	相关资源
复控制器	AWS::Route53RecoveryReadiness::RecoveryGroup	NA	NA
	AWS::Route53RecoveryControl::Cluster	NA	NA
	AWS::Route53RecoveryControl::ControlPanel	NA	NA
	AWS::Route53RecoveryControl::RoutingControl	NA	NA
	AWS::Route53RecoveryControl::SafetyRule	NA	NA
	AWS::Route53RecoveryReadiness::ResourceSet	NA	NA

Amazon SageMaker

AWS 服务	资源类型值	关系	相关资源
Amazon SageMaker	AWS::SageMaker::CodeRepository	NA	NA
	AWS::SageMaker::Domain	NA	NA
	AWS::SageMaker::AppImageConfig	NA	NA
	AWS::SageMaker::Image	NA	NA
	AWS::SageMaker::Model	NA	NA

AWS 服务	资源类型值	关系	相关资源
	AWS::SageMaker::NotebookInstance	NA	NA
	AWS::SageMaker::NotebookInstanceLifecycleConfig	NA	NA
	AWS::SageMaker::EndpointConfig	NA	NA
	AWS::SageMaker::Workteam	NA	NA
	AWS::SageMaker::FeatureGroup	NA	NA

Amazon Simple Email Service

AWS 服务	资源类型值	关系	相关资源
Amazon Simple Email Service	AWS::SES::ConfigurationSet	NA	NA
	AWS::SES::ContactList	NA	NA
	AWS::SES::Template	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`AWS::SES::ReceiptFilter`	NA	NA
	`AWS::SES::ReceiptRuleSet`	NA	NA

Amazon Simple Notification Service

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

Amazon Simple Queue Service

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

Amazon Simple Storage Service

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

AWS 服务	资源类型值	关系	相关资源
	`AWS::S3::MultiRegionAccessPoint`	NA	NA
	`AWS::S3::StorageLens`	NA	NA
	`AWS::S3::AccessPoint`	NA	NA

* 如果您配置 AWS Config 为记录 S3 存储桶，但未收到配置更改通知，请检查您的 S3 存储桶策略是否具有所需的权限。有关更多信息，请参阅 管理 S3 存储桶记录的权限。

Amazon S3 存储桶属性

AWS Config 还记录了 Amazon S3 存储桶资源类型的以下属性。

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

Attributes	描述
WebsiteConfiguration	对存储桶启用静态网站托管。
VersioningConfiguration	对存储桶中的对象启用版本控制。

有关这些属性的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的存储桶配置选项。

Amazon WorkSpaces

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

AWS Amplify

AWS 服务	资源类型值	关系	相关资源
AWS Amplify	`AWS::Amplify::App`	NA	NA
	`AWS::Amplify::Branch`	NA	NA

AWS AppConfig

AWS 服务	资源类型值	关系	相关资源
AWS AppConfig	`AWS::AppConfig::Application`	NA	NA
	`AWS::AppConfig::Environment`	NA	NA
	`AWS::AppConfig::ConfigurationProfile`	NA	NA
	`AWS::AppConfig::DeploymentStrategy`	NA	NA
	`AWS::AppConfig::HostedConfigurationVersion`	NA	NA
	`AWS::AppConfig::ExtensionAssociation`	NA	NA

AWS App Runner

AWS 服务	资源类型值	关系	相关资源
AWS App Runner	`AWS::AppRunner::VpcConnector`	NA	NA
	`AWS::AppRunner::Service`	NA	NA

AWS App Mesh

AWS 服务	资源类型值	关系	相关资源
AWS App Mesh	`AWS::AppMesh::VirtualNode`	NA	NA
	`AWS::AppMesh::VirtualService`	NA	NA
	`AWS::AppMesh::VirtualGateway`	NA	NA
	`AWS::AppMesh::VirtualRouter`	NA	NA
	`AWS::AppMesh::Route`	NA	NA
	`AWS::AppMesh::GatewayRoute`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`AWS::AppMesh::Mesh`	NA	NA

AWS AppSync

AWS 服务	资源类型值	关系	相关资源
AWS AppSync	`AWS::AppSync::GraphQLApi`	NA	NA

AWS Audit Manager

AWS 服务	资源类型值	关系	相关资源
AWS Audit Manager	`AWS::AuditManager::Assessment`	NA	NA

AWS Auto Scaling

AWS 服务	资源类型值	关系	相关资源
AWS Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	contains	Amazon EC2 实例
		关联到	Classic 负载均衡器
			Auto Scaling 启动配置
			子网
	`AWS::AutoScaling::`	关联到	Amazon EC2 安全组

AWS 服务	资源类型值	关系	相关资源
	`LaunchConfiguration`		
	`AWS::AutoScaling::ScalingPolicy`	关联到	自动扩缩组
			警报
	`AWS::AutoScaling::ScheduledAction`	关联到	自动扩缩组
	`AWS::AutoScaling::WarmPool`	NA	NA

AWS Backup

AWS 服务	资源类型值	关系	相关资源
AWS Backup	`AWS::Backup::BackupPlan`	NA	不适用*
	`AWS::Backup::BackupSelection`	NA	NA
	`AWS::Backup::BackupVault`	NA	不适用*
	`AWS::Backup::RecoveryPoint`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`AWS::Backup::ReportPlan`	NA	NA

由于 AWS Backup 工作原理，其中一些资源类型与下表中的其他 AWS Backup 资源类型相关。

`AWS::Backup::BackupPlan`与 Backup Plan 有许多选择的`AWS::Backup::RecoveryPoint`位置有关，`AWS::Backup::BackupVault`也与 AWS Backup Vault 有多个恢复点的位置有关。`AWS::Backup::BackupSelection`

有关更多信息，请参阅使用备份计划管理备份和使用备份保管库。

AWS Batch

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

AWS Budgets

AWS 服务	资源类型值	关系	相关资源
AWS Budgets	`AWS::Budgets::BudgetsAction`	NA	NA

AWS Certificate Manager

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

AWS CloudFormation

AWS 服务	资源类型值	关系	相关资源
AWS CloudFormation	`AWS::CloudFormation::Stack` *	contains	支持的 AWS 资源类型

*AWS Config 记录堆栈的配置更改以及 AWS CloudFormation 堆栈中支持的资源类型。 AWS Config 不记录堆栈中尚不支持的资源类型的配置更改。不受支持的资源类型显示在堆栈的配置项的补充配置部分中。

AWS CloudTrail

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

AWS Cloud9

AWS 服务	资源类型值	关系	相关资源
AWS Cloud9	`AWS::Cloud9::EnvironmentEC2`	NA	NA

AWS Cloud Map

AWS 服务	资源类型值	关系	相关资源
服务发现	`AWS::ServiceDiscovery::Service`	NA	NA
	`AWS::ServiceDiscovery::PublicDnsNamespace`	NA	NA
	`AWS::ServiceDiscovery::HttpNamespace`	NA	NA
`AWS::ServiceDiscovery::Instance`	NA	NA	

AWS CodeArtifact

AWS 服务	资源类型值	关系	相关资源
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	NA	NA

AWS CodeBuild

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

* 要详细了解如何与 AWS Config 集成 AWS CodeBuild，请参阅AWS Config 与 AWS CodeBuild 示例一起使用。

AWS CodeDeploy

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

AWS CodePipeline

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

*AWS Config 记录 CodePipeline 管道的配置更改以及管道中支持的资源类型。 AWS Config 不记录管道中尚不支持的资源类型的配置更改。不受支持的资源类型（如 `CodeCommit repository`, `CodeDeploy application`, `ECS cluster`, 和 `ECS service`）显示在堆栈的配置项的补充配置部分中。

AWS Config

AWS 服务	资源类型值	关系	相关资源
AWS Config	`AWS::Config::ResourceCompliance` *	关联到	所有资源*
	`AWS::Config::ConformancePackCompliance`	NA	NA
	`AWS::Config::Confi`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`gurationRecorder` *		

* `AWS::Config::ResourceCompliance` 与相关资源之间的关系取决于 `AWS::Config::ResourceCompliance` 如何报告该特定资源类型的合规性。

* `AWS::Config::ConfigurationRecorder` 是系统资源类型，默认情况下 AWS Config ，此资源类型的记录处于启用状态。

> **Note**
>
> 记录 `AWS::Config::ConformancePackCompliance` 和 `AWS::Config::ConfigurationRecorder` 资源类型不收取额外费用。

AWS Database Migration Service

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

AWS 服务	资源类型值	关系	相关资源
	`AWS::DMS::Certificate`	NA	NA
	`AWS::DMS::Endpoint`	NA	NA

AWS DataSync

AWS 服务	资源类型值	关系	相关资源
AWS DataSync	`AWS::DataSync::LocationSMB`	NA	NA
	`AWS::DataSync::LocationFSxLustre`	NA	NA
	`AWS::DataSync::LocationFSxWindows`	NA	NA
	`AWS::DataSync::LocationS3`	NA	NA
	`AWS::DataSync::LocationEFS`	NA	NA
	`AWS::DataSync::LocationNFS`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	AWS::DataSync::LocationHDFS	NA	NA
	AWS::DataSync::LocationObjectStorage	NA	NA
	AWS::DataSync::Task	NA	NA

AWS Device Farm

AWS 服务	资源类型值	关系	相关资源
AWS Device Farm	AWS::DeviceFarm::TestGridProject	NA	NA
	AWS::DeviceFarm::InstanceProfile	NA	NA
	AWS::DeviceFarm::Project	NA	NA

AWS Elastic Beanstalk

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

AWS Fault Injection Service

AWS 服务	资源类型值	关系	相关资源
AWS Fault Injection Service	`AWS::FIS::ExperimentTemplate`	NA	NA

AWS Global Accelerator

AWS 服务	资源类型值	关系	相关资源
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	NA	NA
	`AWS::GlobalAccelerator::EndpointGroup`	NA	NA
	`AWS::GlobalAccelerator::Accelerator`	NA	NA

AWS Glue

AWS 服务	资源类型值	关系	相关资源
AWS Glue	`AWS::Glue::Job`	NA	NA
	`AWS::Glue::Classifier`	NA	NA
	`AWS::Glue::MLTransform`	NA	NA

AWS Ground Station

AWS 服务	资源类型值	关系	相关资源
AWS Ground Station	`AWS::GroundStation::Config`	NA	NA
	`AWS::GroundStation::MissionProfile`	NA	NA
	`AWS::GroundStation::DataflowEndpointGroup`	NA	NA

AWS HealthLake

AWS 服务	资源类型值	关系	相关资源
AWS HealthLake	`AWS::HealthLake::FHIRDatastore`	NA	NA

AWS Identity and Access Management (IAM)

AWS 服务	资源类型值	关系	相关资源
AWS Identity and Access Management	`AWS::IAM::User`	挂载到	IAM 组
			IAM 客户托管策略
	`AWS::IAM::Group`	contains	IAM 用户

AWS 服务	资源类型值	关系	相关资源
		挂载到	IAM 客户托管策略
	AWS::IAM::Role	挂载到	IAM 客户托管策略
	AWS::IAM::Policy	挂载到	IAM 用户
			IAM 组
			IAM 角色
	AWS::IAM::SAMLProvider	NA	NA
	AWS::IAM::ServerCertificate	NA	NA
	AWS::IAM::InstanceProfile	NA	NA
	AWS::IAM::OIDCProvider	NA	NA
AWS Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	NA	NA

AWS Config 包括内联策略及其记录的配置详细信息。有关内联策略的更多信息，请参阅《IAM 用户指南》中的托管式策略与内联策略。

AWS IoT

AWS 服务	资源类型值	关系	相关资源
AWS IoT	AWS::IoT::Authorizer	NA	NA
	AWS::IoT::SecurityProfile	NA	NA
	AWS::IoT::RoleAlias	NA	NA
	AWS::IoT::Dimension	NA	NA
	AWS::IoT::Policy	NA	NA
	AWS::IoT::MitigationAction	NA	NA
	AWS::IoT::ScheduledAudit	NA	NA
	AWS::IoT::AccountAuditConfiguration	NA	NA
	AWS::IoTSiteWise::Gateway	NA	NA

AWS 服务	资源类型值	关系	相关资源
	AWS::IoT::CustomMetric	NA	NA
	AWS::IoT::JobTemplate	NA	NA
	AWS::IoT::ProvisioningTemplate	NA	NA
	AWS::IoT::CACertificate	NA	NA
AWS IoT Wireless	AWS::IoTWireless::ServiceProfile	NA	NA
	AWS::IoTWireless::MulticastGroup	NA	NA
	AWS::IoTWireless::FuotaTask	NA	NA
AWS IoT Core	AWS::IoT::FleetMetric	NA	NA
AWS IoT Analytics	AWS::IoTAnalytics::Datastore	NA	NA
	AWS::IoTAnalytics::Dataset	NA	NA

AWS 服务	资源类型值	关系	相关资源
	AWS::IoTAnalytics::Pipeline	NA	NA
	AWS::IoTAnalytics::Channel	NA	NA
AWS IoT Events	AWS::IoTEvents::Input	NA	NA
	AWS::IoTEvents::DetectorModel	NA	NA
	AWS::IoTEvents::AlarmModel	NA	NA
AWS IoT TwinMaker	AWS::IoTTwinMaker::Workspace	NA	NA
	AWS::IoTTwinMaker::Entity	NA	NA
	AWS::IoTTwinMaker::Scene	NA	NA
	AWS::IoTTwinMaker::SyncJob	NA	NA

AWS 服务	资源类型值	关系	相关资源
AWS IoT SiteWise	`AWS::IoTSiteWise::Dashboard`	NA	NA
	`AWS::IoTSiteWise::Project`	NA	NA
	`AWS::IoTSiteWise::Portal`	NA	NA
	`AWS::IoTSiteWise::AssetModel`	NA	NA
AWS IoT Greengrass Version 2	`AWS::GreengrassV2::ComponentVersion`	NA	NA

AWS Key Management Service

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

AWS Lambda

AWS 服务	资源类型值	关系	相关资源
AWS Lambda	`AWS::Lambda::Function`	关联到	IAM 角色
			EC2 安全组
		包含在	EC2 子网
	`AWS::Lambda::Alias`	NA	NA
	`AWS::Lambda::CodeSigningConfig`	NA	NA

AWS Mainframe Modernization

AWS 服务	资源类型值	关系	相关资源
AWS Mainframe Modernization	`AWS::M2::Environment`	NA	NA

AWS Network Firewall

AWS 服务	资源类型值	关系	相关资源
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	挂载到	EC2 子网
		关联到	NetworkFirewall FirewallPolicy
	`AWS::NetworkFirewa`	关联到	NetworkFirewall RuleGroup

AWS 服务	资源类型值	关系	相关资源
	`ll::FirewallPolicy`		
	`AWS::NetworkFirewall::RuleGroup`	NA	NA
	`AWS::NetworkFirewall::TLSInspectionConfiguration`	NA	NA

AWS Network Manager

AWS 服务	资源类型值	关系	相关资源
AWS Network Manager	`AWS::NetworkManager::TransitGatewayRegistration`	NA	NA
	`AWS::NetworkManager::Site`	NA	NA
	`AWS::NetworkManager::Device`	NA	NA
	`AWS::NetworkManager::Link`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`AWS::NetworkManager::GlobalNetwork`	NA	NA
	`AWS::NetworkManager::CustomerGatewayAssociation`	NA	NA
	`AWS::NetworkManager::LinkAssociation`	NA	NA
	`AWS::NetworkManager::ConnectPeer`	NA	NA

AWS Panorama

AWS 服务	资源类型值	关系	相关资源
AWS Panorama	`AWS::Panorama::Package`	NA	NA

AWS Private Certificate Authority

AWS 服务	资源类型值	关系	相关资源
AWS Private Certificate Authority	`AWS::ACMPCA::Certi`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	ficateAuthority		
	AWS::ACMPCA::CertificateAuthorityActivation	NA	NA

AWS Resilience Hub

AWS 服务	资源类型值	关系	相关资源
AWS Resilience Hub	AWS::ResilienceHub::ResiliencyPolicy	NA	NA
	AWS::ResilienceHub::App	NA	NA

AWS 资源探索器

AWS 服务	资源类型值	关系	相关资源
AWS 资源探索器	AWS::ResourceExplorer2::Index	NA	NA

AWS RoboMaker

AWS 服务	资源类型值	关系	相关资源
AWS RoboMaker	`AWS::RoboMaker::RobotApplicationVersion`	NA	NA
	`AWS::RoboMaker::RobotApplication`	NA	NA
	`AWS::RoboMaker::SimulationApplication`	NA	NA

AWS Signer

AWS 服务	资源类型值	关系	相关资源
AWS Signer	`AWS::Signer::SigningProfile`	NA	NA

AWS Secrets Manager

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

AWS Service Catalog

AWS 服务	资源类型值	关系	相关资源
AWS Service Catalog	`AWS::ServiceCatalog::CloudFormationProduct`	包含在	产品组合
		关联到	CloudFormationProvisionedProduct
	`AWS::ServiceCatalog::CloudFormationProvisionedProduct`	关联到	产品组合
			CloudFormation产品
			CloudFormation堆栈
	`AWS::ServiceCatalog::Portfolio`	contains	CloudFormation产品

AWS Shield

AWS 服务	资源类型值	关系	相关资源
AWS Shield	`AWS::Shield::Protection`	关联到	亚马逊 CloudFront 配送
	`AWS::ShieldRegional::Protection`	关联到	EC2 EIP
		关联到	ElasticLoadBalancing 平衡器
		关联到	ElasticLoadBalancingv2 LoadBalancer

AWS Step Functions

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

AWS Systems Manager

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

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

AWS Transfer Family

AWS 服务	资源类型值	关系	相关资源
AWS Transfer Family	`AWS::Transfer::Agreement`	NA	NA
	`AWS::Transfer::Connector`	NA	NA
	`AWS::Transfer::Workflow`	NA	NA
	`AWS::Transfer::Certificate`	NA	NA
	`AWS::Transfer::Profile`	NA	NA

AWS WAF

AWS 服务	资源类型值	关系	相关资源
AWS WAF	`AWS::WAF::RateBasedRule`	NA	NA
	`AWS::WAF::Rule`	NA	NA
	`AWS::WAF::WebACL`	关联到	WAF 规则
			WAF 基于速率的规则

AWS 服务	资源类型值	关系	相关资源
			WAF Rulegroup
	`AWS::WAF::RuleGroup`	关联到	WAF 规则
	`AWS::WAFRegional::RateBasedRule`	NA	NA
	`AWS::WAFRegional::Rule`	NA	NA
	`AWS::WAFRegional::WebACL`	关联到	ElasticLoadBalancingv2 LoadBalancer
			WAFRegional 规则
			WAFRegional 基于速率的规则
			WAFRegional Rulegroup
	`AWS::WAFRegional::RuleGroup`	关联到	WAFRegional 规则
AWS WAF V2	`AWS::WAFv2::WebACL`	关联到	ElasticLoadBalancingv2 LoadBalancer
			ApiGateway 舞台
			WAFv2 IPSet
			Wafv2 RegexPatternSet
			Wafv2 RuleGroup

AWS 服务	资源类型值	关系	相关资源
			Wafv2 ManagedRuleSet
	`AWS::WAFv2::RuleGroup`	关联到	WAFv2 IPSet
			Wafv2 RegexPatternSet
	`AWS::WAFv2::ManagedRuleSet`	关联到	Wafv2 RuleGroup
	`AWS::WAFv2::IPSet`	NA	NA
	`AWS::WAFv2::RegexPatternSet`	NA	NA

AWS X-Ray

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

Elastic Load Balancing

AWS 服务	资源类型值	关系	相关资源
Elastic Load Balancing	应用程序负载均衡器	关联到	EC2 安全组
		挂载到	子网

AWS 服务	资源类型值	关系	相关资源
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	包含在	Virtual Private Cloud (VPC)
	应用程序负载均衡器侦听器 `AWS::ElasticLoadBalancingV2::Listener`	NA	NA
	Classic 负载均衡器 `AWS::ElasticLoadBalancing::LoadBalancer`	关联到	EC2 安全组
		挂载到	子网
		包含在	Virtual Private Cloud (VPC)
	网络负载均衡器 `AWS::ElasticLoadBalancingV2::LoadBalancer`	NA	NA

AWS Elemental MediaConnect

AWS 服务	资源类型值	关系	相关资源
AWS Elemental MediaConnect	`AWS::MediaConnect::FlowEntitlement`	NA	NA

AWS 服务	资源类型值	关系	相关资源
	`AWS::MediaConnect::FlowVpcInterface`	NA	NA
	`AWS::MediaConnect::FlowSource`	NA	NA

AWS Elemental MediaPackage

AWS 服务	资源类型值	关系	相关资源
AWS Elemental MediaPackage	`AWS::MediaPackage::PackagingGroup`	NA	NA
	`AWS::MediaPackage::PackagingConfiguration`	NA	NA

AWS Elemental MediaTailor

AWS 服务	资源类型值	关系	相关资源
AWS Elemental MediaTailor	`AWS::MediaTailor::PlaybackConfiguration`	NA	NA

按区域可用性列出的资源覆盖范围

北美洲和南美洲区域

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::ACM::Certificate	是	是	是	是	是	是	是
AWS::ACMPCA::CertificateAuthority	是	是	是	是	是	是	否
AWS::ACMPCA::CertificateAuthority激活	是	是	是	是	是	是	否
AWS::APS::RuleGroups命名空间	是	是	是	是	否	否	否
AWS::AccessAnalyzer::Analyzer	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::AmazonMQ::Broker	是	是	是	是	是	是	否
AWS::Amplify::App	是	是	是	是	是	是	否
AWS::Amplify::Branch	是	是	是	是	是	是	否
AWS::ApiGateway::RestApi	是	是	是	是	是	是	否
AWS::ApiGateway::Stage	是	是	是	是	是	是	否
AWS::ApiGatewayV2::Api	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::ApiGatewayV2::Stage	是	是	是	是	是	是	否
AWS::AppConfig::Application	是	是	是	是	是	是	否
AWS::AppConfig::ConfigurationProfile	是	是	是	是	是	是	否
AWS::AppConfig::DeploymentStrategy	是	是	是	是	是	是	否
AWS::AppConfig::Environment	是	是	是	是	是	是	否
AWS::AppConfig::ExtensionAssociation	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::AppConfig::HostedConfiguration版本	是	是	是	是	是	是	否
AWS::AppFlow::Flow	是	是	是	是	是	是	否
AWS::AppIntegrations::EventIntegration	否	否	是	是	否	是	否
AWS::AppMesh::GatewayRoute	是	是	是	是	是	是	否
AWS::AppMesh::Mesh	是	是	是	是	是	是	否
AWS::AppMesh::Route	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::AppMesh::VirtualGateway	是	是	是	是	是	是	否
AWS::AppMesh::VirtualNode	是	是	是	是	是	是	否
AWS::AppMesh::VirtualRouter	是	是	是	是	是	是	否
AWS::AppMesh::VirtualService	是	是	是	是	是	是	否
AWS::AppRunner::Service	是	否	是	是	否	否	否
AWS::AppRunner::VpcConnector	是	否	是	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::AppStream::Application	是	是	是	是	否	是	否
AWS::AppStream::DirectoryConfig	是	是	是	是	否	是	否
AWS::AppStream::Fleet	是	否	是	是	否	是	否
AWS::AppStream::Stack	是	否	是	是	否	是	否
AWS::AppSync::GraphqlaPi	是	是	是	是	是	是	否
AWS::Athena::DataCatalog	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Athena::PreparedStatement	是	是	是	是	是	是	否
AWS::Athena::WorkGroup	是	是	是	是	是	是	否
AWS::AuditManager::Assessment	是	否	是	是	是	是	否
AWS::AutoScaling::AutoScaling群组	是	是	是	是	是	是	是
AWS::AutoScaling::LaunchConfiguration	是	是	是	是	是	是	是
AWS::AutoScaling::ScalingPolicy	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::AutoScaling::ScheduledAction	是	是	是	是	是	是	是
AWS::AutoScaling::WarmPool	是	是	是	是	是	是	否
AWS::Backup::BackupPlan	是	是	是	是	是	是	否
AWS::Backup::BackupSelection	是	是	是	是	是	是	否
AWS::Backup::BackupVault	是	是	是	是	是	是	否
AWS::Backup::RecoveryPoint	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Backup::ReportPlan	是	是	是	是	是	是	否
AWS::Batch::ComputeEnvironment	是	是	是	是	是	是	否
AWS::Batch::JobQueue	是	是	是	是	是	是	否
AWS::Batch::SchedulingPolicy	是	是	是	是	是	是	否
AWS::Budgets::BudgetsAction	否	否	是	否	否	否	否
AWS::Cassandra::Keyspace	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Cloud9::EnvironmentEC2	是	是	是	是	是	是	否
AWS::CloudFormation::Stack	是	是	是	是	是	是	否
AWS::CloudFront::Distribution	否	否	是	否	否	否	否
AWS::CloudFront::StreamingDistribution	否	否	是	否	否	否	否
AWS::CloudTrail::Trail	是	是	是	是	是	是	是
AWS::CloudWatch::Alarm	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::CloudWatch::MetricStream	是	是	是	是	是	是	否
AWS::CodeArtifact::Repository	是	否	是	是	否	否	否
AWS::CodeBuild::Project	是	是	是	是	是	是	否
AWS::CodeBuild::ReportGroup	是	是	是	是	是	是	否
AWS::CodeDeploy::Application	是	是	是	是	是	是	否
AWS::CodeDeploy::DeploymentConfig	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::CodeDeploy::DeploymentGroup	是	是	是	是	是	是	否
AWS::CodeGuruProfiler::ProfilingGroup	是	否	是	是	否	否	否
AWS::CodeGuruReviewer::RepositoryAssociation	是	否	是	是	否	否	否
AWS::CodePipeline::Pipeline	是	是	是	是	是	是	否
AWS::Cognito::UserPool	是	是	是	是	是	是	否
AWS::Cognito::UserPool客户端	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Cognito::UserPool群组	是	是	是	是	是	是	否
AWS::Config::ConfigurationRecorder	是	是	是	是	是	是	是
AWS::Config::ConformancePack合规	是	是	是	是	是	是	否
AWS::Config::ResourceCompliance	是	是	是	是	是	是	是
AWS::Connect::Instance	否	否	是	是	否	是	否
AWS::Connect::PhoneNumber	否	否	是	是	否	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Connect::QuickConnect	否	否	是	是	否	是	否
AWS::CustomerProfiles::Domain	否	否	是	是	否	是	否
AWS::CustomerProfiles::ObjectType	否	否	是	是	否	是	否
AWS::DMS::Certificate	是	是	是	是	是	是	否
AWS::DMS::Endpoint	是	是	是	是	是	是	否
AWS::DMS::EventSubscription	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::DMS::ReplicationInstance	是	是	是	是	是	是	否
AWS::DMS::ReplicationSubnet群组	是	是	是	是	是	是	否
AWS::DMS::ReplicationTask	是	是	是	是	是	是	否
AWS::DataSync::LocationEFS	是	是	是	是	是	是	否
AWS::DataSync::LocationF SxLustre	是	是	是	是	是	是	否
AWS::DataSync::LocationF SxWindows	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::DataSync::LocationHDFS	是	是	是	是	是	是	否
AWS::DataSync::LocationNFS	是	是	是	是	是	是	否
AWS::DataSync::LocationObject存储	是	是	是	是	是	是	否
AWS::DataSync::LocationS3	是	是	是	是	是	是	否
AWS::DataSync::Location中小型企业	是	是	是	是	是	是	否
AWS::DataSync::Task	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Detective::Graph	是	是	是	是	是	是	否
AWS::DeviceFarm::InstanceProfile	否	否	否	是	否	否	否
AWS::DeviceFarm::Project	否	否	否	是	否	否	否
AWS::DeviceFarm::TestGrid项目	否	否	否	是	否	否	否
AWS::DynamoDB::Table	是	是	是	是	是	是	是
AWS::EC2::Capacity Reservation	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::EC2::CarrierGateway	是	否	是	是	否	是	否
AWS::EC2::ClientVpn端点	是	是	是	是	是	是	否
AWS::EC2::CustomerGateway	是	是	是	是	是	是	是
AWS::EC2::DHCPOptions	是	是	是	是	是	是	否
AWS::EC2::EC2Fleet	是	是	是	是	是	是	否
AWS::EC2::EIP	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::EC2::EgressOnlyInternetGateway	是	是	是	是	是	是	否
AWS::EC2::FlowLog	是	是	是	是	是	是	否
AWS::EC2::Host	是	是	是	是	是	是	是
AWS::EC2::IPAM	是	是	是	是	是	是	否
AWS::EC2::IPAMPool	是	是	是	是	是	是	否
AWS::EC2::IPAMScope	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::EC2::Instance	是	是	是	是	是	是	是
AWS::EC2::InternetGateway	是	是	是	是	是	是	是
AWS::EC2::LaunchTemplate	是	是	是	是	是	是	否
AWS::EC2::NatGateway	是	是	是	是	是	是	否
AWS::EC2::NetworkAcl	是	是	是	是	是	是	是
AWS::EC2::NetworkInsightsAccessScope	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::EC2::NetworkInsightsAccessScope分析	是	是	是	是	是	是	否
AWS::EC2::NetworkInsights分析	是	是	是	是	是	是	否
AWS::EC2::NetworkInsights路径	是	是	是	是	是	是	否
AWS::EC2::NetworkInterface	是	是	是	是	是	是	是
AWS::EC2::PrefixList	是	是	是	是	是	是	否
AWS::EC2::RegisteredHAInstanc	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::EC2::RouteTable	是	是	是	是	是	是	是
AWS::EC2::SecurityGroup	是	是	是	是	是	是	是
AWS::EC2::SpotFleet	是	是	是	是	是	是	否
AWS::EC2::Subnet	是	是	是	是	是	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是	是	是	是	是	否
AWS::EC2::TrafficMirror过滤器	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::EC2::TrafficMirror会话	是	是	是	是	是	是	否
AWS::EC2::TrafficMirror目标	是	是	是	是	是	是	否
AWS::EC2::TransitGateway	是	是	是	是	是	是	否
AWS::EC2::TransitGateway附件	是	是	是	是	是	是	否
AWS::EC2::TransitGatewayConnect	是	是	是	是	是	是	否
AWS::EC2::TransitGatewayMulticastDomain	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::EC2::TransitGatewayRouteTable	是	是	是	是	是	是	否
AWS::EC2::VPC	是	是	是	是	是	是	是
AWS::EC2::VPCEndpoint	是	是	是	是	是	是	是
AWS:: EC2:: VPC EndpointService	是	是	是	是	是	是	是
AWS:: EC2:: VPC PeeringConnection	是	是	是	是	是	是	是
AWS::EC2::VPNConnection	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::EC2::VPNGateway	是	是	是	是	是	是	是
AWS::EC2::Volume	是	是	是	是	是	是	是
AWS::ECR::PublicRepository	否	否	是	否	否	否	否
AWS::ECR::PullThroughCacheRule	是	是	是	是	是	是	否
AWS::ECR::RegistryPolicy	是	是	是	是	是	是	否
AWS::ECR::Repository	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::ECS::CapacityProvider	是	是	是	是	是	是	否
AWS::ECS::Cluster	是	是	是	是	是	是	是
AWS::ECS::Service	是	是	是	是	是	是	是
AWS::ECS::TaskDefinition	是	是	是	是	是	是	是
AWS::ECS::TaskSet	是	是	是	是	是	是	否
AWS::EFS::AccessPoint	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::EFS::FileSystem	是	是	是	是	是	是	否
AWS::EKS::Addon	是	是	是	是	是	是	否
AWS::EKS::Cluster	是	是	是	是	是	是	否
AWS::EKS::FargateProfile	是	是	是	是	是	是	否
AWS::EKS::IdentityProviderConfig	是	是	是	是	是	是	否
AWS::EMR::SecurityConfiguration	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::ElasticBeanstalk::Application	是	是	是	是	是	是	否
AWS::ElasticBeanstalk::ApplicationVersion	是	是	是	是	是	是	否
AWS::ElasticBeanstalk::Environment	是	是	是	是	是	是	否
AWS::ElasticLoadBalancing::LoadBalancer	是	是	是	是	是	是	是
AWS::ElasticLoadBalancingV2::Listener	是	是	是	是	是	是	否
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Elasticsearch::Domain	是	是	是	是	是	是	是
AWS::EventSchemas::Discoverer	是	是	是	是	是	是	否
AWS::EventSchemas::Registry	是	是	是	是	是	是	否
AWS::EventSchemas::RegistryPolicy	是	是	是	是	是	是	否
AWS::EventSchemas::Schema	是	是	是	是	是	是	否
AWS::Events::ApiDestination	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Events::Archive	是	是	是	是	是	是	否
AWS::Events::Connection	是	是	是	是	是	是	否
AWS::Events::Endpoint	是	是	是	是	是	是	否
AWS::Events::EventBus	是	是	是	是	是	是	否
AWS::Events::Rule	是	是	是	是	是	是	否
AWS::Evidently::Launch	是	否	是	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Evidently::Project	是	否	是	是	否	否	否
AWS::Evidently::Segment	是	否	是	是	否	否	否
AWS::FIS::ExperimentTemplate	是	是	是	是	是	是	否
AWS::Forecast::Dataset	是	否	是	是	否	否	否
AWS::Forecast::DatasetGroup	是	否	是	是	否	否	否
AWS::FraudDetector::EntityType	是	否	是	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::FraudDetector::Label	是	否	是	是	否	否	否
AWS::FraudDetector::Outcome	是	否	是	是	否	否	否
AWS::FraudDetector::Variable	是	否	是	是	否	否	否
AWS::GlobalAccelerator::Accelerator	否	否	否	是	否	否	否
AWS::GlobalAccelerator::EndpointGroup	否	否	否	是	否	否	否
AWS::GlobalAccelerator::Listener	否	否	否	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Glue::Classifier	是	是	是	是	是	是	否
AWS::Glue::Job	是	是	是	是	是	是	否
AWS::Glue:: mlTransf	是	是	是	是	是	是	否
AWS::Grafana::Workspace	是	否	是	是	否	否	否
AWS::GreengrassV2::ComponentVersion	是	否	是	是	否	是	否
AWS::GroundStation::Config	是	是	是	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::GroundStation::DataflowEndpoint群组	是	是	是	是	否	否	否
AWS::GroundStation::MissionProfile	是	是	是	是	否	否	否
AWS::GuardDuty::Detector	是	是	是	是	是	是	否
AWS::GuardDuty::Filter	是	是	是	是	是	是	否
AWS::Guard职责:: IPset	是	是	是	是	是	是	否
AWS::GuardDuty::ThreatIntelSet	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::HealthLake::fhirdataStore	是	否	是	是	否	否	否
AWS::IAM::Group	是	是	是	是	是	是	否
AWS::IAM::InstanceProfile	否	否	是	否	否	否	否
AWS::IAM::OIDCProvider	否	否	是	否	否	否	否
AWS::IAM::Policy	是	是	是	是	是	是	否
AWS::IAM::Role	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::IAM::SAMLProvider	否	否	是	否	否	否	否
AWS::IAM::ServerCertificate	否	否	是	否	否	否	否
AWS::IAM::User	是	是	是	是	是	是	否
AWS::IVS::Channel	否	否	是	是	否	否	否
AWS::IVS::PlaybackKey配对	否	否	是	是	否	否	否
AWS::IVS::RecordingConfiguration	否	否	是	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::ImageBuilder::ContainerRecipe	是	是	是	是	是	是	否
AWS::ImageBuilder::DistributionConfiguration	是	是	是	是	是	是	否
AWS::ImageBuilder::ImagePipeline	是	是	是	是	是	是	否
AWS::ImageBuilder::ImageRecipe	是	是	是	是	是	是	否
AWS::ImageBuilder::InfrastructureConfiguration	是	是	是	是	是	是	否
AWS::InspectorV2::Filter	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::IoT::AccountAudit配置	是	否	是	是	是	是	否
AWS::IoT::Authorizer	是	是	是	是	是	是	否
AWS::IoT:: caCertificate	是	是	是	是	是	是	否
AWS::IoT::CustomMetric	是	否	是	是	是	是	否
AWS::IoT::Dimension	是	否	是	是	是	是	否
AWS::IoT::FleetMetric	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::IoT::JobTemplate	是	是	是	是	是	是	否
AWS::IoT::MitigationAction	是	否	是	是	是	是	否
AWS::IoT::Policy	是	是	是	是	是	是	否
AWS::IoT::ProvisioningTemplate	是	是	是	是	是	是	否
AWS::IoT::RoleAlias	是	是	是	是	是	是	否
AWS::IoT::ScheduledAudit	是	否	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::IoT::SecurityProfile	是	否	是	是	是	是	否
AWS::IoTAnalytics::Channel	是	否	是	是	否	否	否
AWS::IoTAnalytics::Dataset	是	否	是	是	否	否	否
AWS::IoTAnalytics::Datastore	是	否	是	是	否	否	否
AWS::IoTAnalytics::Pipeline	是	否	是	是	否	否	否
AWS::IoTEvents::AlarmModel	是	否	是	是	否	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::IoTEvents::DetectorModel	是	否	是	是	否	是	否
AWS::IoTEvents::Input	是	否	是	是	否	是	否
AWS::IoTSiteWise::AssetModel	是	否	是	是	否	是	否
AWS::IoTSiteWise::Dashboard	是	否	是	是	否	是	否
AWS::IoTSiteWise::Gateway	是	否	是	是	否	是	否
AWS::IoTSiteWise::Portal	是	否	是	是	否	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::IoTSiteWise::Project	是	否	是	是	否	是	否
AWS::IoTTwinMaker::ComponentType	否	否	是	是	否	否	否
AWS::IoTTwinMaker::Entity	否	否	是	是	否	否	否
AWS::IoTTwinMaker::Scene	否	否	是	是	否	否	否
AWS::IoTTwinMaker::SyncJob	否	否	是	是	否	否	否
AWS::IoTTwinMaker::Workspace	否	否	是	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::IoTWireless::FuotaTask	否	是	是	是	否	否	否
AWS::IoTWireless::MulticastGroup	否	是	是	是	否	否	否
AWS::IoTWireless::ServiceProfile	否	是	是	是	否	否	否
AWS::KMS::Alias	是	是	是	是	是	是	否
AWS::KMS::Key	是	是	是	是	是	是	是
AWS::KafkaConnect::Connector	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Kendra::Index	是	否	是	是	否	是	否
AWS::Kinesis::Stream	是	是	是	是	是	是	否
AWS::Kinesis::StreamConsumer	是	是	是	是	是	是	否
AWS::KinesisAnalyticsV2::Application	是	是	是	是	是	是	否
AWS::KinesisFirehose::DeliveryStream	是	是	是	是	是	是	否
AWS::KinesisVideo::SignalingChannel	是	是	是	是	否	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::KinesisVideo::Stream	是	是	是	是	否	是	否
AWS::Lambda::CodeSigningConfig	是	是	是	是	是	是	否
AWS::Lambda::Function	是	是	是	是	是	是	是
AWS::Lex::Bot	否	否	是	是	否	是	否
AWS::Lex::BotAlias	否	否	是	是	否	是	否
AWS::Lightsail::Bucket	是	否	是	是	否	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Lightsail::Certificate	是	否	是	是	否	是	否
AWS::Lightsail::Disk	是	否	是	是	否	是	否
AWS::Lightsail::StaticIp	是	否	是	是	否	是	否
AWS::Logs::Destination	是	是	是	是	是	是	否
AWS::LookoutMetrics::Alert	是	否	是	是	否	否	否
AWS::LookoutVision::Project	是	否	是	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::M2::Environment	是	是	是	是	是	是	否
AWS::MSK::BatchScram秘密	是	是	是	是	是	是	否
AWS::MSK::Cluster	是	是	是	是	是	是	否
AWS::MSK::ClusterPolicy	是	是	是	是	是	是	否
AWS::MSK::Configuration	是	是	是	是	是	是	否
AWS::MSK::VpcConnection	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::MediaConnect::FlowEntitlement	是	是	是	是	是	是	否
AWS::MediaConnect::FlowSource	是	是	是	是	是	是	否
AWS::MediaConnect::FlowVpc接口	是	是	是	是	是	是	否
AWS::MediaPackage::PackagingConfiguration	是	是	是	是	是	否	否
AWS::MediaPackage::PackagingGroup	是	是	是	是	是	否	否
AWS::MediaTailor::PlaybackConfiguration	是	否	是	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::MemoryDB::SubnetGroup	是	是	是	是	是	是	否
AWS::NetworkFirewall::Firewall	是	是	是	是	是	是	否
AWS::NetworkFirewall::FirewallPolicy	是	是	是	是	是	是	否
AWS::NetworkFirewall::RuleGroup	是	是	是	是	是	是	否
AWS::Network防火墙:: TLS InspectionConfiguration	是	是	是	是	是	是	否
AWS::NetworkManager::ConnectPeer	否	否	否	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::NetworkManager::CustomerGateway协会	✗ 否	✗ 否	✗ 否	✓ 是	✗ 否	✗ 否	✗ 否
AWS::NetworkManager::Device	✗ 否	✗ 否	✗ 否	✓ 是	✗ 否	✗ 否	✗ 否
AWS::NetworkManager::GlobalNetwork	✗ 否	✗ 否	✗ 否	✓ 是	✗ 否	✗ 否	✗ 否
AWS::NetworkManager::Link	✗ 否	✗ 否	✗ 否	✓ 是	✗ 否	✗ 否	✗ 否
AWS::NetworkManager::LinkAssociation	✗ 否	✗ 否	✗ 否	✓ 是	✗ 否	✗ 否	✗ 否
AWS::NetworkManager::Site	✗ 否	✗ 否	✗ 否	✓ 是	✗ 否	✗ 否	✗ 否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::NetworkManager::TransitGateway注册	否	否	否	是	否	否	否
AWS::OpenSearch::Domain	是	是	是	是	是	是	否
AWS::Panorama::Package	否	否	是	是	否	是	否
AWS::Personalize::Dataset	是	否	是	是	否	是	否
AWS::Personalize::DatasetGroup	是	否	是	是	否	是	否
AWS::Personalize::Schema	是	否	是	是	否	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Personalize::Solution	是	否	是	是	否	是	否
AWS::Pinpoint::App	否	否	是	是	否	是	否
AWS::Pinpoint::ApplicationSettings	否	否	是	是	否	是	否
AWS::Pinpoint::Campaign	否	否	是	是	否	是	否
AWS::Pinpoint::EmailChannel	否	否	是	是	否	是	否
AWS::Pinpoint::EmailTemplate	否	否	是	是	否	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Pinpoint::EventStream	否	否	是	是	否	是	否
AWS::Pinpoint::InApp模板	是	否	是	是	否	是	否
AWS::Pinpoint::Segment	否	否	是	是	否	是	否
AWS::QLDB::Ledger	是	否	是	是	否	是	否
AWS::QuickSight::DataSource	是	是	是	是	否	是	否
AWS::QuickSight::Template	是	是	是	是	否	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::QuickSight::Theme	是	是	是	是	否	是	否
AWS::RDS::DBCluster	是	是	是	是	是	是	是
AWS:: RDS:: DB ClusterSnapshot	是	是	是	是	是	是	是
AWS::RDS::DBInstance	是	是	是	是	是	是	是
AWS:: RDS:: DB SecurityGroup	是	是	是	是	是	是	是
AWS::RDS::DBSnapshot	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS:: RDS:: DB SubnetGroup	是	是	是	是	是	是	是
AWS::RDS::EventSubscription	是	是	是	是	是	是	是
AWS::RDS::GlobalCluster	是	否	是	是	是	是	否
AWS::RDS::OptionGroup	是	是	是	是	是	是	否
AWS::RUM::AppMonitor	是	否	是	是	否	否	否
AWS::Redshift::Cluster	是	是	是	是	是	是	是

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Redshift::ClusterParameter群组	是	是	是	是	是	是	是
AWS::Redshift::ClusterSecurity群组	是	是	是	是	是	是	是
AWS::Redshift::ClusterSnapshot	是	是	是	是	是	是	是
AWS::Redshift::ClusterSubnet群组	是	是	是	是	是	是	是
AWS::Redshift::EndpointAccess	是	是	是	是	是	是	否
AWS::Redshift::EndpointAuthorization	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Redshift::EventSubscription	是	是	是	是	是	是	是
AWS::Redshift::ScheduledAction	是	是	是	是	是	是	否
AWS::ResilienceHub::App	是	是	是	是	是	是	否
AWS::ResilienceHub::ResiliencyPolicy	是	是	是	是	是	是	否
AWS::ResourceExplorer2::Index	是	是	是	是	是	是	否
AWS::RoboMaker::RobotApplication	是	否	是	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::RoboMaker::RobotApplication版本	是	否	是	是	否	否	否
AWS::RoboMaker::SimulationApplication	是	否	是	是	否	否	否
AWS::Route53::HealthCheck	否	否	是	否	否	否	否
AWS::Route53::HostedZone	否	否	是	否	否	否	否
AWS::Route53RecoveryControl::Cluster	否	否	否	是	否	否	否
AWS::Route53RecoveryControl::ControlPanel	否	否	否	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Route53RecoveryControl::RoutingControl	否	否	否	是	否	否	否
AWS::Route53RecoveryControl::SafetyRule	否	否	否	是	否	否	否
AWS::Route53RecoveryReadiness::Cell	否	否	否	是	否	否	否
AWS::Route53RecoveryReadiness::ReadinessCheck	否	否	否	是	否	否	否
AWS::Route53RecoveryReadiness::RecoveryGroup	否	否	否	是	否	否	否
AWS::Route53RecoveryReadiness::ResourceSet	否	否	否	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Route53Resolver::FirewallDomain名单	是	是	是	是	是	是	否
AWS::Route53Resolver::FirewallRule群组	是	是	是	是	是	是	否
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是	是	是	是	是	否
AWS::Route53Resolver::ResolverEndpoint	是	是	是	是	是	是	否
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是	是	是	是	是	否
AWS::Route53Resolver::ResolverQueryLoggingConfig协会	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Route53Resolver::ResolverRule	是	是	是	是	是	是	否
AWS::Route53Resolver::ResolverRule协会	是	是	是	是	是	是	否
AWS::S3::AccessPoint	是	是	是	是	是	是	否
AWS::S3::AccountPublicAccessBlock	是	是	是	是	是	是	否
AWS::S3::Bucket	是	是	是	是	是	是	是
AWS::S3::MultiRegionAccessPoint	否	否	否	是	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::S3::StorageLens	是	是	是	是	是	是	否
AWS::SES::ConfigurationSet	是	是	是	是	是	是	否
AWS::SES::ContactList	是	是	是	是	是	是	否
AWS::SES::ReceiptFilter	否	否	是	是	否	否	否
AWS::SES::ReceiptRuleSet	否	否	是	是	否	否	否
AWS::SES::Template	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::SNS::Topic	是	是	是	是	是	是	是
AWS::SQS::Queue	是	是	是	是	是	是	否
AWS::SSM::AssociationCompliance	是	是	是	是	是	是	否
AWS::SSM::Document	是	是	是	是	是	是	否
AWS::SSM::FileData	是	是	是	是	是	是	否
AWS::SSM::ManagedInstance库存	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::SSM::PatchCompliance	是	是	是	是	是	是	否
AWS::SageMaker::AppImageConfig	是	是	是	是	是	是	否
AWS::SageMaker::CodeRepository	是	是	是	是	是	是	否
AWS::SageMaker::Domain	是	是	是	是	是	是	否
AWS::SageMaker::EndpointConfig	是	是	是	是	是	是	否
AWS::SageMaker::FeatureGroup	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::SageMaker::Image	是	是	是	是	是	是	否
AWS::SageMaker::Model	是	是	是	是	是	是	否
AWS::SageMaker::NotebookInstance	是	是	是	是	是	是	否
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	是	是	是	是	是	否
AWS::SageMaker::Workteam	是	否	是	是	否	是	否
AWS::SecretsManager::Secret	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::ServiceCatalog::CloudFormation产品	是	是	是	是	是	是	否
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是	是	是	是	是	否
AWS::ServiceCatalog::Portfolio	是	是	是	是	是	是	否
AWS::ServiceDiscovery::HttpNamespace	是	是	是	是	是	是	否
AWS::ServiceDiscovery::Instance	是	是	是	是	是	是	否
AWS::ServiceDiscovery::PublicDns命名空间	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::ServiceDiscovery::Service	是	是	是	是	是	是	否
AWS::Shield::Protection	否	否	是	否	否	否	否
AWS::ShieldRegional::Protection	是	是	是	是	是	是	否
AWS::Signer::SigningProfile	是	是	是	是	是	是	否
AWS::StepFunctions::Activity	是	是	是	是	是	是	否
AWS::StepFunctions::StateMachine	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::Transfer::Agreement	是	是	是	是	是	是	否
AWS::Transfer::Certificate	是	是	是	是	是	是	否
AWS::Transfer::Connector	是	是	是	是	是	是	否
AWS::Transfer::Profile	是	是	是	是	是	是	否
AWS::Transfer::Workflow	是	是	是	是	是	是	否
AWS::WAF::RateBased规则	否	否	是	否	否	否	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::WAF::Rule	否	否	是	否	否	否	否
AWS::WAF::RuleGroup	否	否	是	否	否	否	否
AWS::WAF::WebACL	否	否	是	否	否	否	否
AWS::WAFRegional::RateBased规则	是	是	是	是	是	是	否
AWS::WAFRegional::Rule	是	是	是	是	是	是	否
AWS::WAFRegional::RuleGroup	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::WAFRegional::WebACL	是	是	是	是	是	是	否
AWS::WAFv2::IPSet	是	是	是	是	是	是	否
AWS::WAFv2::ManagedRuleSet	是	是	是	是	是	是	否
AWS::WAFv2::RegexPatternSet	是	是	是	是	是	是	否
AWS::WAFv2::RuleGroup	是	是	是	是	是	是	否
AWS::WAFv2::WebACL	是	是	是	是	是	是	否

资源类型	美国西部（加利福尼亚北部）	美国东部（弗吉尼亚北部）	美国西部（俄勒冈）	美国东部（俄亥俄）	加拿大西部（卡尔加里）	加拿大（中部）	南美洲（圣保罗）
AWS::WorkSpaces::ConnectionAlias	否	是	是	是	否	是	否
AWS::WorkSpaces::Workspace	否	是	是	是	否	是	否
AWS::XRay::EncryptionConfig	是	是	是	是	是	是	否

欧洲区域

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ACM::Certificate	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ACMPCA::CertificateAuthority	是	是	是	是	是	是	是	是
AWS::ACMPCA::CertificateAuthority激活	是	是	是	是	是	是	是	是
AWS::APS::RuleGroups命名空间	是	是	是	是	是	否	否	否
AWS::AccessAnalyzer::Analyzer	是	是	是	是	是	是	是	是
AWS::AmazonMQ::Broker	是	是	是	是	是	是	否	否
AWS::Amplify::App	是	是	是	是	是	是	否	否
AWS::Amplify::Branch	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ApiGateway::RestApi	是	是	是	是	是	是	是	是
AWS::ApiGateway::Stage	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Api	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Stage	是	是	是	是	是	是	是	是
AWS::AppConfig::Application	是	是	是	是	是	是	否	否
AWS::AppConfig::ConfigurationProfile	是	是	是	是	是	是	否	否
AWS::AppConfig::DeploymentStrategy	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::AppConfig::Environment	是	是	是	是	是	是	否	否
AWS::AppConfig::ExtensionAssociation	是	是	是	是	是	是	是	是
AWS::AppConfig::HostedConfiguration版本	是	是	是	是	是	是	否	否
AWS::AppFlow::Flow	否	是	是	是	是	否	否	否
AWS::AppIntegrations::EventIntegration	否	否	否	是	是	否	否	否
AWS::AppMesh::GatewayRoute	是	是	是	是	是	是	否	否
AWS::AppMesh::Mesh	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::AppMesh::Route	是	是	是	是	是	是	否	否
AWS::AppMesh::VirtualGateway	是	是	是	是	是	是	否	否
AWS::AppMesh::VirtualNode	是	是	是	是	是	是	否	否
AWS::AppMesh::VirtualRouter	是	是	是	是	是	是	否	否
AWS::AppMesh::VirtualService	是	是	是	是	是	是	否	否
AWS::AppRunner::Service	否	否	是	是	否	否	否	否
AWS::AppRunner::VpcConnector	否	否	是	否	否	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::AppStream::Application	否	否	是	是	是	否	否	否
AWS::AppStream::DirectoryConfig	否	否	是	是	是	否	否	否
AWS::AppStream::Fleet	否	否	是	是	是	否	否	否
AWS::AppStream::Stack	否	否	是	是	是	否	否	否
AWS::AppSync::GraphqlaPi	是	是	是	是	是	是	是	是
AWS::Athena::DataCatalog	是	是	是	是	是	是	否	否
AWS::Athena::PreparedStatement	是	是	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Athena::WorkGroup	是	是	是	是	是	是	否	否
AWS::AuditManager::Assessment	否	否	是	是	是	否	否	否
AWS::AutoScaling::AutoScaling群组	是	是	是	是	是	是	是	是
AWS::AutoScaling::LaunchConfiguration	是	是	是	是	是	是	是	是
AWS::AutoScaling::ScalingPolicy	是	是	是	是	是	是	是	是
AWS::AutoScaling::ScheduledAction	是	是	是	是	是	是	是	是
AWS::Auto Scaling::WarmPool	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Backup::BackupPlan	是	是	是	是	是	是	否	否
AWS::Backup::BackupSelection	是	是	是	是	是	是	否	否
AWS::Backup::BackupVault	是	是	是	是	是	是	否	否
AWS::Backup::RecoveryPoint	是	是	是	是	是	是	否	否
AWS::Backup::ReportPlan	是	是	是	是	是	是	否	否
AWS::Batch::ComputeEnvironment	是	是	是	是	是	是	是	是
AWS::Batch::JobQueue	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Batch::SchedulingPolicy	是	是	是	是	是	是	是	是
AWS::Cassandra::Keyspace	是	是	是	是	是	否	否	否
AWS::Cloud9::EnvironmentEC2	是	是	是	是	是	是	否	否
AWS::CloudFormation::Stack	是	是	是	是	是	是	否	否
AWS::CloudTrail::Trail	是	是	是	是	是	是	是	是
AWS::CloudWatch::Alarm	是	是	是	是	是	是	是	是
AWS::CloudWatch::MetricStream	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::CodeArtifact::Repository	是	是	是	是	是	是	否	否
AWS::CodeBuild::Project	是	是	是	是	是	是	是	是
AWS::CodeBuild::ReportGroup	是	是	是	是	是	是	否	否
AWS::CodeDeploy::Application	是	是	是	是	是	是	否	否
AWS::CodeDeploy::DeploymentConfig	是	是	是	是	是	是	否	否
AWS::CodeDeploy::DeploymentGroup	是	是	是	是	是	是	否	否
AWS::CodeGuruProfiler::ProfilingGroup	是	否	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::CodeGuruReviewer::RepositoryAssociation	是	否	是	是	是	否	否	否
AWS::CodePipeline::Pipeline	是	是	是	是	是	是	否	否
AWS::Cognito::UserPool	是	是	是	是	是	是	否	否
AWS::Cognito::UserPool客户端	是	是	是	是	是	是	否	否
AWS::Cognito::UserPool群组	是	是	是	是	是	是	否	否
AWS::Config::ConfigurationRecorder	是	是	是	是	是	是	是	是
AWS::Config::ConformancePack合规	是	是	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Config::ResourceCompliance	是	是	是	是	是	是	是	是
AWS::Connect::Instance	否	否	否	是	是	否	否	否
AWS::Connect::PhoneNumber	否	否	否	是	是	否	否	否
AWS::Connect::QuickConnect	否	否	否	是	是	否	否	否
AWS::CustomerProfiles::Domain	否	否	否	是	是	否	否	否
AWS::CustomerProfiles::ObjectType	否	否	否	是	是	否	否	否
AWS::DMS::Certificate	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::DMS::Endpoint	是	是	是	是	是	是	否	否
AWS::DMS::EventSubscription	是	是	是	是	是	是	否	否
AWS::DMS::ReplicationInstance	是	是	是	是	是	是	否	否
AWS::DMS::ReplicationSubnet群组	是	是	是	是	是	是	否	否
AWS::DMS::ReplicationTask	是	是	是	是	是	是	否	否
AWS::DataSync::LocationEFS	是	是	是	是	是	是	是	是
AWS::DataSync::LocationF SxLustre	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::DataSync::LocationF SxWindows	是	是	是	是	是	是	否	否
AWS::Data Sync::LocationHDFS	是	是	是	是	是	是	是	是
AWS::Data Sync::LocationNFS	是	是	是	是	是	是	是	是
AWS::DataSync::LocationObject存储	是	是	是	是	是	是	是	是
AWS::Data Sync::LocationS3	是	是	是	是	是	是	是	是
AWS::DataSync::Location中小型企业	是	是	是	是	是	是	是	是
AWS::DataSync::Task	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Detective::Graph	是	是	是	是	是	是	否	否
AWS::DynamoDB::Table	是	是	是	是	是	是	是	是
AWS::EC2::Capacity Reservation	是	是	是	是	是	是	否	否
AWS::EC2::CarrierGateway	否	是	是	是	是	否	否	否
AWS::EC2::ClientVpn端点	是	是	是	是	是	是	否	否
AWS::EC2::CustomerGateway	是	是	是	是	是	是	是	是
AWS::EC2::DHCPOptions	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EC2::EC2Fleet	是	是	是	是	是	是	是	是
AWS::EC2::EIP	是	是	是	是	是	是	是	是
AWS::EC2::EgressOnlyInternetGateway	是	是	是	是	是	是	否	是
AWS::EC2::FlowLog	是	是	是	是	是	是	否	是
AWS::EC2::Host	是	是	是	是	是	是	是	是
AWS::EC2::IPAM	是	是	是	是	是	是	是	是
AWS::EC2::IPAMPool	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EC2::IPAMScope	是	是	是	是	是	是	是	是
AWS::EC2::Instance	是	是	是	是	是	是	是	是
AWS::EC2::InternetGateway	是	是	是	是	是	是	是	是
AWS::EC2::LaunchTemplate	是	是	是	是	是	是	否	否
AWS::EC2::NatGateway	是	是	是	是	是	是	否	是
AWS::EC2::NetworkAcl	是	是	是	是	是	是	是	是
AWS::EC2::NetworkInsightsAccessScope	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EC2::NetworkInsightsAccessScope分析	是	是	是	是	是	是	否	否
AWS::EC2::NetworkInsights分析	是	是	是	是	是	是	否	否
AWS::EC2::NetworkInsights路径	是	是	是	是	是	是	否	否
AWS::EC2::NetworkInterface	是	是	是	是	是	是	是	是
AWS::EC2::PrefixList	是	是	是	是	是	是	是	是
AWS::EC2::RegisteredHAInstanc	是	是	是	是	是	否	否	否
AWS::EC2::RouteTable	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EC2::SecurityGroup	是	是	是	是	是	是	是	是
AWS::EC2::SpotFleet	是	是	是	是	是	是	是	是
AWS::EC2::Subnet	是	是	是	是	是	是	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是	是	是	是	是	是	是
AWS::EC2::TrafficMirror过滤器	是	是	是	是	是	否	否	否
AWS::EC2::TrafficMirror会话	是	是	是	是	是	否	否	否
AWS::EC2::TrafficMirror目标	是	是	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EC2::TransitGateway	是	是	是	是	是	是	是	是
AWS::EC2::TransitGateway附件	是	是	是	是	是	是	是	是
AWS::EC2::TransitGatewayConnect	是	是	是	是	是	是	否	否
AWS::EC2::TransitGatewayMulticastDomain	是	是	是	是	是	是	是	是
AWS::EC2::TransitGatewayRouteTable	是	是	是	是	是	是	否	是
AWS::EC2::VPC	是	是	是	是	是	是	是	是
AWS::EC2::VPCEndpoint	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS:: EC2:: VPC EndpointService	是	是	是	是	是	是	是	是
AWS:: EC2:: VPC PeeringConnection	是	是	是	是	是	是	是	是
AWS::EC2: :VPNConnection	是	是	是	是	是	是	是	是
AWS::EC2::VPNGateway	是	是	是	是	是	是	是	是
AWS::EC2::Volume	是	是	是	是	是	是	是	是
AWS::ECR::PullThroughCacheRule	是	是	是	是	是	是	是	是
AWS::ECR::RegistryPolicy	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ECR::Repository	是	是	是	是	是	是	是	是
AWS::ECS::CapacityProvider	是	是	是	是	是	是	是	是
AWS::ECS::Cluster	是	是	是	是	是	是	是	是
AWS::ECS::Service	是	是	是	是	是	是	是	是
AWS::ECS::TaskDefinition	是	是	是	是	是	是	是	是
AWS::ECS::TaskSet	是	是	是	是	是	是	是	是
AWS::EFS::AccessPoint	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EFS::FileSystem	是	是	是	是	是	是	是	是
AWS::EKS::Addon	是	是	是	是	是	是	是	是
AWS::EKS::Cluster	是	是	是	是	是	是	是	是
AWS::EKS::FargateProfile	是	是	是	是	是	是	是	是
AWS::EKS::IdentityProviderConfig	是	是	是	是	是	是	是	是
AWS::EMR::SecurityConfiguration	是	是	是	是	是	是	是	是
AWS::ElasticBeanstalk::Application	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ElasticBeanstalk::ApplicationVersion	是	是	是	是	是	是	否	否
AWS::ElasticBeanstalk::Environment	是	是	是	是	是	是	否	否
AWS::ElasticLoadBalancing::LoadBalancer	是	是	是	是	是	是	是	是
AWS::ElasticLoadBalancingV2::Listener	是	是	是	是	是	是	否	否
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是	是	是	是	是	是	是
AWS::Elasticsearch::Domain	是	是	是	是	是	是	是	是
AWS::EventSchemas::Discoverer	是	是	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::EventSchemas::Registry	是	是	是	是	是	否	否	否
AWS::EventSchemas::RegistryPolicy	是	是	是	是	是	否	否	否
AWS::EventSchemas::Schema	是	是	是	是	是	否	否	否
AWS::Events::ApiDestination	是	是	是	是	是	是	否	否
AWS::Events::Archive	是	是	是	是	是	是	是	是
AWS::Events::Connection	是	是	是	是	是	是	否	否
AWS::Events::Endpoint	是	是	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Events::EventBus	是	是	是	是	是	是	否	否
AWS::Events::Rule	是	是	是	是	是	是	是	是
AWS::Evidently::Launch	是	否	是	是	否	否	否	否
AWS::Evidently::Project	是	否	是	是	否	否	否	否
AWS::Evidently::Segment	是	否	是	是	否	否	否	否
AWS::FIS::ExperimentTemplate	是	是	是	是	是	是	否	否
AWS::Forecast::Dataset	否	否	是	是	否	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Forecast::DatasetGroup	否	否	是	是	否	否	否	否
AWS::FraudDetector::EntityType	否	否	是	否	否	否	否	否
AWS::FraudDetector::Label	否	否	是	否	否	否	否	否
AWS::FraudDetector::Outcome	否	否	是	否	否	否	否	否
AWS::FraudDetector::Variable	否	否	是	否	否	否	否	否
AWS::Glue::Classifier	是	是	是	是	是	是	是	是
AWS::Glue::Job	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Glue:: mlTransf	是	是	是	是	是	是	是	是
AWS::Grafana::Workspace	否	否	是	是	是	否	否	否
AWS::GreengrassV2::ComponentVersion	否	否	是	是	是	否	否	否
AWS::GroundStation::Config	是	否	是	是	否	否	否	否
AWS::GroundStation::DataflowEndpoint群组	是	否	是	是	否	否	否	否
AWS::GroundStation::MissionProfile	是	否	是	是	否	否	否	否
AWS::GuardDuty::Detector	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::GuardDuty::Filter	是	是	是	是	是	是	否	否
AWS::Guard职责:: IPset	是	是	是	是	是	是	否	否
AWS::GuardDuty::ThreatIntelSet	是	是	是	是	是	是	否	否
AWS::IAM::Group	是	是	是	是	是	是	否	否
AWS::IAM::Policy	是	是	是	是	是	是	否	否
AWS::IAM::Role	是	是	是	是	是	是	否	否
AWS::IAM::User	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::IVS::Channel	否	否	是	是	否	否	否	否
AWS::IVS::PlaybackKey配对	否	否	是	是	否	否	否	否
AWS::IVS::RecordingConfiguration	否	否	是	是	否	否	否	否
AWS::ImageBuilder::ContainerRecipe	是	是	是	是	是	是	是	是
AWS::ImageBuilder::DistributionConfiguration	是	是	是	是	是	是	否	否
AWS::ImageBuilder::ImagePipeline	是	是	是	是	是	是	是	是
AWS::ImageBuilder::ImageRecipe	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ImageBuilder::InfrastructureConfiguration	是	是	是	是	是	是	是	是
AWS::InspectorV2::Filter	是	是	是	是	是	是	否	否
AWS::IoT::AccountAudit配置	是	是	是	是	是	否	否	否
AWS::IoT::Authorizer	是	是	是	是	是	否	否	否
AWS::IoT:: caCertificate	是	是	是	是	是	否	否	否
AWS::IoT::CustomMetric	是	是	是	是	是	否	否	否
AWS::IoT::Dimension	是	是	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::IoT::FleetMetric	是	是	是	是	是	否	否	否
AWS::IoT::JobTemplate	是	是	是	是	是	否	否	否
AWS::IoT::MitigationAction	是	是	是	是	是	否	否	否
AWS::IoT::Policy	是	是	是	是	是	否	否	否
AWS::IoT::ProvisioningTemplate	是	是	是	是	是	否	否	否
AWS::IoT::RoleAlias	是	是	是	是	是	否	否	否
AWS::IoT::ScheduledAudit	是	是	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::IoT::SecurityProfile	是	是	是	是	是	否	否	否
AWS::IoTAnalytics::Channel	否	否	是	是	否	否	否	否
AWS::IoTAnalytics::Dataset	否	否	是	是	否	否	否	否
AWS::IoTAnalytics::Datastore	否	否	是	是	否	否	否	否
AWS::IoTAnalytics::Pipeline	否	否	是	是	否	否	否	否
AWS::IoTEvents::AlarmModel	否	否	是	是	是	否	否	否
AWS::IoTEvents::DetectorModel	否	否	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::IoTEvents::Input	否	否	是	是	是	否	否	否
AWS::IoTSiteWise::AssetModel	否	否	是	是	否	否	否	否
AWS::IoTSiteWise::Dashboard	否	否	是	是	否	否	否	否
AWS::IoTSiteWise::Gateway	否	否	是	是	否	否	否	否
AWS::IoTSiteWise::Portal	否	否	是	是	否	否	否	否
AWS::IoTSiteWise::Project	否	否	是	是	否	否	否	否
AWS::IoTTwinMaker::ComponentType	否	否	是	是	否	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::IoTTwinMaker::Entity	否	否	是	是	否	否	否	否
AWS::IoTTwinMaker::Scene	否	否	是	是	否	否	否	否
AWS::IoTTwinMaker::SyncJob	否	否	是	是	否	否	否	否
AWS::IoTTwinMaker::Workspace	否	否	是	是	否	否	否	否
AWS::IoTWireless::FuotaTask	否	否	是	是	否	否	否	否
AWS::IoTWireless::MulticastGroup	否	否	是	是	否	否	否	否
AWS::IoTWireless::ServiceProfile	否	否	是	是	否	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::KMS::Alias	是	是	是	是	是	是	否	否
AWS::KMS::Key	是	是	是	是	是	是	是	是
AWS::KafkaConnect::Connector	是	是	是	是	是	否	否	否
AWS::Kendra::Index	否	否	是	否	是	否	否	否
AWS::Kinesis::Stream	是	是	是	是	是	是	是	是
AWS::Kinesis::StreamConsumer	是	是	是	是	是	是	是	是
AWS::KinesisAnalyticsV2::Application	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::KinesisFirehose::DeliveryStream	是	是	是	是	是	是	是	是
AWS::KinesisVideo::SignalingChannel	否	是	是	是	是	否	否	否
AWS::KinesisVideo::Stream	否	是	是	是	是	否	否	否
AWS::Lambda::CodeSigningConfig	是	是	是	是	是	是	否	否
AWS::Lambda::Function	是	是	是	是	是	是	是	是
AWS::Lex::Bot	否	否	是	是	是	否	否	否
AWS::Lex::BotAlias	否	否	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Lightsail::Bucket	是	是	是	是	是	否	否	否
AWS::Lightsail::Certificate	是	是	是	是	是	否	否	否
AWS::Lightsail::Disk	是	是	是	是	是	否	否	否
AWS::Lightsail::StaticIp	是	是	是	是	是	否	否	否
AWS::Logs::Destination	是	是	是	是	是	是	是	是
AWS::LookoutMetrics::Alert	是	否	是	是	否	否	否	否
AWS::LookoutVision::Project	否	否	是	是	否	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::M2::Environment	否	是	是	是	是	否	否	否
AWS::MSK::BatchScram秘密	是	是	是	是	是	是	是	是
AWS::MSK::Cluster	是	是	是	是	是	是	是	是
AWS::MSK::ClusterPolicy	是	是	是	是	是	是	是	是
AWS::MSK::Configuration	是	是	是	是	是	是	是	是
AWS::MSK::VpcConnection	是	是	是	是	是	是	是	是
AWS::MediaConnect::FlowEntitlement	是	是	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::MediaConnect::FlowSource	是	是	是	是	是	否	否	否
AWS::MediaConnect::FlowVpc接口	是	是	是	是	是	否	否	否
AWS::MediaPackage::PackagingConfiguration	是	是	是	是	是	否	否	否
AWS::MediaPackage::PackagingGroup	是	是	是	是	是	否	否	否
AWS::MediaTailor::PlaybackConfiguration	否	否	是	是	否	否	否	否
AWS::MemoryDB::SubnetGroup	是	否	是	是	是	否	否	否
AWS::NetworkFirewall::Firewall	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::NetworkFirewall::FirewallPolicy	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::RuleGroup	是	是	是	是	是	是	是	是
AWS::Network防火墙:: TLS InspectionConfiguration	是	是	是	是	是	是	是	是
AWS::Open Search::Domain	是	是	是	是	是	是	否	否
AWS::Panorama::Package	否	否	是	否	否	否	否	否
AWS::Personalize::Dataset	否	否	是	是	否	否	否	否
AWS::Personalize:: DatasetGroup	否	否	是	是	否	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Personalize::Schema	否	否	是	是	否	否	否	否
AWS::Personalize::Solution	否	否	是	是	否	否	否	否
AWS::Pinpoint::App	否	否	是	是	是	否	否	否
AWS::Pinpoint::ApplicationSettings	否	否	是	是	是	否	否	否
AWS::Pinpoint::Campaign	否	否	是	是	是	否	否	否
AWS::Pinpoint::EmailChannel	否	否	是	是	是	否	否	否
AWS::Pinpoint::EmailTemplate	否	否	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Pinpoint::EventStream	否	否	是	是	是	否	否	否
AWS::Pinpoint::InApp模板	否	否	是	是	是	否	否	否
AWS::Pinpoint::Segment	否	否	是	是	是	否	否	否
AWS::QLDB::Ledger	否	否	是	是	是	否	否	否
AWS::QuickSight::DataSource	是	是	是	是	是	否	否	否
AWS::QuickSight::Template	是	是	是	是	是	否	否	否
AWS::QuickSight::Theme	是	是	是	是	是	否	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::RDS::DBCluster	是	是	是	是	是	是	否	是
AWS:: RDS:: DB ClusterSnapshot	是	是	是	是	是	是	是	是
AWS::RDS::DBInstance	是	是	是	是	是	是	是	是
AWS:: RDS:: DB SecurityGroup	是	是	是	是	是	是	是	是
AWS::RDS::DBSnapshot	是	是	是	是	是	是	是	是
AWS:: RDS:: DB SubnetGroup	是	是	是	是	是	是	是	是
AWS::RDS: :EventSubscription	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::RDS::GlobalCluster	否	是	是	是	是	否	否	否
AWS::RDS::OptionGroup	是	是	是	是	是	是	是	是
AWS::RUM::AppMonitor	是	否	是	是	是	否	否	否
AWS::Redshift::Cluster	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterParameter群组	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSecurity群组	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSnapshot	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Redshift::ClusterSubnet群组	是	是	是	是	是	是	是	是
AWS::Redshift::EndpointAccess	是	是	是	是	是	否	否	否
AWS::Redshift::EndpointAuthorization	是	是	是	是	是	否	否	否
AWS::Redshift::EventSubscription	是	是	是	是	是	是	是	是
AWS::Redshift::ScheduledAction	是	是	是	是	是	是	否	否
AWS::ResilienceHub::App	是	是	是	是	是	是	否	否
AWS::ResilienceHub::ResiliencyPolicy	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ResourceExplorer2::Index	是	是	是	是	是	否	否	否
AWS::RoboMaker::RobotApplication	否	否	是	是	否	否	否	否
AWS::RoboMaker::RobotApplication版本	否	否	是	是	否	否	否	否
AWS::RoboMaker::SimulationApplication	否	否	是	是	否	否	否	否
AWS::Route53Resolver::FirewallDomain名单	是	是	是	是	是	是	否	否
AWS::Route53Resolver::FirewallRule群组	是	是	是	是	是	是	否	否
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::Route53Resolver::ResolverEndpoint	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是	是	是	是	是	否	否
AWS::Route53Resolver::ResolverQueryLoggingConfig协会	是	是	是	是	是	是	否	否
AWS::Route53Resolver::ResolverRule	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverRule协会	是	是	是	是	是	是	是	是
AWS::S3::AccessPoint	是	是	是	是	是	是	是	是
AWS::S3::AccountPublicAccessBlock	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::S3::Bucket	是	是	是	是	是	是	是	是
AWS::S3::StorageLens	是	是	是	是	是	否	否	否
AWS::SES::ConfigurationSet	是	是	是	是	是	是	否	否
AWS::SES::ContactList	是	是	是	是	是	是	否	否
AWS::SES::ReceiptFilter	否	否	是	否	否	否	否	否
AWS::SES::ReceiptRuleSet	否	否	是	否	否	否	否	否
AWS::SES::Template	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::SNS::Topic	是	是	是	是	是	是	否	否
AWS::SQS::Queue	是	是	是	是	是	是	否	否
AWS::SSM::AssociationCompliance	是	是	是	是	是	是	是	是
AWS::SSM::Document	是	是	是	是	是	是	是	是
AWS::SSM::FileData	是	是	是	是	是	是	是	是
AWS::SSM::ManagedInstance库存	是	是	是	是	是	是	是	是
AWS::SSM::PatchCompliance	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::SageMaker::AppImageConfig	是	是	是	是	是	是	否	否
AWS::SageMaker::CodeRepository	是	是	是	是	是	是	否	否
AWS::SageMaker::Domain	是	是	是	是	是	是	否	否
AWS::SageMaker::EndpointConfig	是	是	是	是	是	是	否	否
AWS::SageMaker::FeatureGroup	是	是	是	是	是	是	否	否
AWS::SageMaker::Image	是	是	是	是	是	是	否	否
AWS::SageMaker::Model	是	是	是	是	是	是	否	否

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::SageMaker::NotebookInstance	是	是	是	是	是	是	否	否
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	是	是	是	是	是	否	否
AWS::SageMaker::Workteam	否	否	是	是	是	否	否	否
AWS::SecretsManager::Secret	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::CloudFormation产品	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::Portfolio	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::ServiceDiscovery::HttpNamespace	是	是	是	是	是	是	否	否
AWS::ServiceDiscovery::Instance	是	是	是	是	是	是	否	否
AWS::ServiceDiscovery::PublicDns命名空间	是	是	是	是	是	是	否	否
AWS::ServiceDiscovery::Service	是	是	是	是	是	是	否	否
AWS::ShieldRegional::Protection	是	是	是	是	是	是	否	否
AWS::Signer::SigningProfile	是	是	是	是	是	是	否	否
AWS::StepFunctions::Activity	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::StepFunctions::StateMachine	是	是	是	是	是	是	是	是
AWS::Transfer::Agreement	是	是	是	是	是	是	否	否
AWS::Transfer::Certificate	是	是	是	是	是	是	否	否
AWS::Transfer::Connector	是	是	是	是	是	是	否	否
AWS::Transfer::Profile	是	是	是	是	是	是	是	是
AWS::Transfer::Workflow	是	是	是	是	是	是	否	否
AWS::WAFRegional::RateBased规则	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::WAFRegional::Rule	是	是	是	是	是	是	是	是
AWS::WAFRegional::RuleGroup	是	是	是	是	是	是	是	是
AWS::WAFRegional::WebACL	是	是	是	是	是	是	是	是
AWS::WAFv2::IPSet	是	是	是	是	是	是	是	是
AWS::WAFv2::ManagedRuleSet	是	是	是	是	是	是	是	是
AWS::WAFv2::RegexPatternSet	是	是	是	是	是	是	是	是
AWS::WAFv2::RuleGroup	是	是	是	是	是	是	是	是

资源类型	欧洲地区（爱尔兰）	欧洲地区（法兰克福）	欧洲地区（伦敦）	欧洲（巴黎）	欧洲地区（斯德哥尔摩）	欧洲地区（米兰）	欧洲（西班牙）	欧洲（苏黎世）
AWS::WAFv2::WebACL	是	是	是	是	是	是	是	是
AWS::WorkSpaces::ConnectionAlias	否	否	是	是	是	否	否	否
AWS::WorkSpaces::Workspace	否	否	是	是	是	否	否	否
AWS::XRay::EncryptionConfig	是	是	是	是	是	是	是	是

亚太区域

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::ACM::Certificate	是	是	是	是	是	是	是	是	是	是
AWS::ACMPCA::CertificateAuthority	是	是	是	是	是	是	是	是	是	是
AWS::ACMPCA::CertificateAuthority激活	是	是	是	是	是	是	是	是	是	是
AWS::APS::RuleGroups命名空间	是	否	否	否	是	否	否	是	是	是
AWS::AccessAnalyzer::Analyzer	是	是	是	是	是	是	是	是	是	是
AWS::AmazonMQ::Broker	是	是	是	否	是	是	否	是	是	是
AWS::Amplify::App	是	否	是	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Amplify::Branch	是	否	是	否	是	否	否	是	是	是
AWS::ApiGateway::RestApi	是	是	是	是	是	是	是	是	是	是
AWS::ApiGateway::Stage	是	是	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Api	是	是	是	是	是	是	是	是	是	是
AWS::ApiGatewayV2::Stage	是	是	是	是	是	是	是	是	是	是
AWS::AppConfig::Application	是	是	是	否	是	是	是	是	是	是
AWS::AppConfig::ConfigurationProfile	是	是	是	否	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::AppConfig::DeploymentStrategy	是	是	是	否	是	是	是	是	是	是
AWS::AppConfig::Environment	是	是	是	否	是	是	是	是	是	是
AWS::AppConfig::ExtensionAssociation	是	是	是	是	是	是	是	是	是	是
AWS::AppConfig::HostedConfiguration版本	是	是	是	否	是	是	是	是	是	是
AWS::AppFlow::Flow	是	否	否	否	是	否	否	是	是	是
AWS::AppIntegrations::EventIntegration	否	否	否	否	是	否	否	是	是	是
AWS::AppMesh::GatewayRoute	是	是	是	否	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::AppMesh::Mesh	是	是	是	否	是	是	否	是	是	是
AWS::AppMesh::Route	是	是	是	否	是	是	否	是	是	是
AWS::AppMesh::VirtualGateway	是	是	是	否	是	是	否	是	是	是
AWS::AppMesh::VirtualNode	是	是	是	否	是	是	否	是	是	是
AWS::AppMesh::VirtualRouter	是	是	是	否	是	是	否	是	是	是
AWS::AppMesh::VirtualService	是	是	是	否	是	是	否	是	是	是
AWS::AppRunner::Service	否	否	否	否	否	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::AppRunner::VpcConnector	否	否	否	否	否	否	否	是	否	否
AWS::AppStream::Application	是	否	否	否	是	否	否	是	是	是
AWS::AppStream::DirectoryConfig	是	否	否	否	是	否	否	是	是	是
AWS::AppStream::Fleet	是	否	否	否	是	否	否	是	是	是
AWS::AppStream::Stack	是	否	否	否	是	否	否	是	是	是
AWS::AppSync::GraphqlApi	是	是	是	是	是	是	否	是	是	是
AWS::Athena::DataCatalog	是	是	是	否	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Athena::PreparedStatement	是	是	是	否	是	是	否	是	是	是
AWS::Athena::WorkGroup	是	是	是	否	是	是	否	是	是	是
AWS::AuditManager::Assessment	是	否	否	否	否	否	否	是	是	是
AWS::AutoScaling::AutoScaling群组	是	是	是	是	是	是	是	是	是	是
AWS::AutoScaling::LaunchConfiguration	是	是	是	是	是	是	是	是	是	是
AWS::AutoScaling::ScalingPolicy	是	是	是	是	是	是	是	是	是	是
AWS::AutoScaling::ScheduledAction	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Auto Scaling::WarmPool	是	是	是	否	是	是	否	是	是	是
AWS::Back up::BackupPlan	是	否	是	否	是	是	否	是	是	是
AWS::Back up::BackupSelection	是	是	是	否	是	是	否	是	是	是
AWS::Back up::BackupVault	是	是	是	否	是	是	否	是	是	是
AWS::Back up::RecoveryPoint	是	否	是	否	是	是	否	是	是	是
AWS::Back up::ReportPlan	是	否	是	否	是	否	否	是	是	是
AWS::Batch::Comput eEnvironment	是	是	是	是	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Batch::JobQueue	是	是	是	是	是	是	否	是	是	是
AWS::Batch::SchedulingPolicy	是	是	是	是	是	是	否	是	是	是
AWS::Cassandra::Keyspace	是	否	是	否	是	否	否	是	是	是
AWS::Cloud9::EnvironmentEC2	是	否	是	否	是	是	否	是	是	是
AWS::CloudFormation::Stack	是	否	是	否	是	否	否	是	是	是
AWS::CloudTrail::Trail	是	是	是	是	是	是	是	是	是	是
AWS::CloudWatch::Alarm	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::CloudWatch::MetricStream	是	是	是	是	是	是	是	是	是	是
AWS::CodeArtifact::Repository	是	否	否	否	否	否	否	是	是	是
AWS::CodeBuild::Project	是	否	是	是	是	是	是	是	是	是
AWS::CodeBuild::ReportGroup	是	否	是	否	是	是	否	是	是	是
AWS::CodeDeploy::Application	是	否	是	否	是	是	否	是	是	是
AWS::CodeDeploy::DeploymentConfig	是	否	是	否	是	是	否	是	是	是
AWS::CodeDeploy::DeploymentGroup	是	否	是	否	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::CodeGuruProfiler::ProfilingGroup	否	否	否	否	否	否	否	是	是	是
AWS::CodeGuruReviewer::RepositoryAssociation	否	否	否	否	否	否	否	是	是	是
AWS::CodePipeline::Pipeline	是	否	是	否	是	否	否	是	是	是
AWS::Cognito::UserPool	是	否	否	否	是	是	否	是	是	是
AWS::Cognito::UserPool客户端	是	否	否	否	是	是	否	是	是	是
AWS::Cognito::UserPool群组	是	否	否	否	是	是	否	是	是	是
AWS::Config::ConfigurationRecorder	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Config::ConformancePack合规性	是	否	是	否	是	否	是	是	是	是
AWS::Config::ResourceCompliance	是	是	是	是	是	是	是	是	是	是
AWS::Connect::Instance	否	否	否	否	是	否	否	是	是	是
AWS::Connect::PhoneNumber	否	否	否	否	是	否	否	是	是	是
AWS::Connect::QuickConnect	否	否	否	否	否	否	否	是	是	是
AWS::CustomerProfiles::Domain	否	否	否	否	是	否	否	是	是	是
AWS::CustomerProfiles::ObjectType	否	否	否	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::DMS::Certificate	是	否	是	否	是	是	否	是	是	是
AWS::DMS::Endpoint	是	否	是	否	是	是	否	是	是	是
AWS::DMS::EventSubscription	是	否	是	否	是	是	否	是	是	是
AWS::DMS::ReplicationInstance	是	否	是	否	是	是	否	是	是	是
AWS::DMS::ReplicationSubnet群组	是	否	是	否	是	是	否	是	是	是
AWS::DMS::ReplicationTask	是	否	是	否	是	是	否	是	是	是
AWS::DataSync::LocationEFS	是	是	是	否	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::DataSync::LocationF SxLustre	是	否	是	否	是	是	否	是	是	是
AWS::DataSync::LocationF SxWindows	是	否	是	否	是	是	否	是	是	是
AWS::Data Sync::LocationHDFS	是	是	是	是	是	是	是	是	是	是
AWS::Data Sync::LocationNFS	是	是	是	是	是	是	是	是	是	是
AWS::DataSync::LocationObject存储	是	是	是	是	是	是	否	是	是	是
AWS::Data Sync::LocationS3	是	是	是	是	是	是	否	是	是	是
AWS::DataSync::Location中小型企业	是	是	是	是	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::DataSync::Task	是	是	是	是	是	是	是	是	是	是
AWS::Detective::Graph	是	否	是	否	是	否	否	是	是	是
AWS::DynamoDB::Table	是	是	是	是	是	是	是	是	是	是
AWS::EC2::Capacity Reservation	是	是	是	否	是	是	否	是	是	是
AWS::EC2::CarrierGateway	否	否	否	否	是	否	否	是	否	是
AWS::EC2::ClientVpn端点	是	否	是	否	是	否	否	是	是	是
AWS::EC2::CustomerGateway	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::EC2::DHCPOptions	是	是	是	是	是	是	否	是	是	是
AWS::EC2::EC2Fleet	是	是	是	是	是	是	是	是	是	是
AWS::EC2::EIP	是	是	是	是	是	是	是	是	是	是
AWS::EC2::EgressOnlyInternetGateway	是	是	是	否	是	是	否	是	是	是
AWS::EC2::FlowLog	是	是	是	否	是	是	否	是	是	是
AWS::EC2::Host	是	是	是	是	是	是	是	是	是	是
AWS::EC2::IPAM	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::EC2::IPAMPool	是	是	是	是	是	是	是	是	是	是
AWS::EC2::IPAMScope	是	是	是	是	是	是	是	是	是	是
AWS::EC2::Instance	是	是	是	是	是	是	是	是	是	是
AWS::EC2::InternetGateway	是	是	是	是	是	是	是	是	是	是
AWS::EC2::LaunchTemplate	是	是	是	否	是	是	否	是	是	是
AWS::EC2::NatGateway	是	是	是	否	是	是	否	是	是	是
AWS::EC2::NetworkAcl	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::EC2::NetworkInsightsAccessScope	是	否	是	否	是	否	否	是	是	是
AWS::EC2::NetworkInsightsAccessScope分析	是	否	是	否	是	否	否	是	是	是
AWS::EC2::NetworkInsights分析	是	否	是	否	是	否	否	是	是	是
AWS::EC2::NetworkInsights路径	是	否	是	否	是	否	否	是	是	是
AWS::EC2::NetworkInterface	是	是	是	是	是	是	是	是	是	是
AWS::EC2::PrefixList	是	是	是	是	是	是	是	是	是	是
AWS::EC2::RegisteredHAInstanc	是	否	否	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::EC2::RouteTable	是	是	是	是	是	是	是	是	是	是
AWS::EC2::SecurityGroup	是	是	是	是	是	是	是	是	是	是
AWS::EC2::SpotFleet	是	是	是	是	是	是	是	是	是	是
AWS::EC2::Subnet	是	是	是	是	是	是	是	是	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是	是	是	是	是	是	是	是	是
AWS::EC2::TrafficMirror过滤器	是	否	是	否	是	否	否	是	是	是
AWS::EC2::TrafficMirror会话	是	否	是	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::EC2::TrafficMirror目标	是	否	是	否	是	否	否	是	是	是
AWS::EC2::TransitGateway	是	是	是	是	是	否	否	是	是	是
AWS::EC2::TransitGateway附件	是	是	是	是	是	是	否	是	是	是
AWS::EC2::TransitGatewayConnect	是	是	是	否	是	是	否	是	是	是
AWS::EC2::TransitGatewayMulticastDomain	是	是	是	是	是	是	是	是	是	是
AWS::EC2::TransitGatewayRouteTable	是	是	是	否	是	是	否	是	是	是
AWS::EC2::VPC	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::EC2::VPCEndpoint	是	是	是	是	是	是	是	是	是	是
AWS:: EC2:: VPC EndpointService	是	是	是	是	是	是	是	是	是	是
AWS:: EC2:: VPC PeeringConnection	是	是	是	是	是	是	是	是	是	是
AWS::EC2::VPNConnection	是	是	是	是	是	是	是	是	是	是
AWS::EC2::VPNGateway	是	是	是	是	是	是	是	是	是	是
AWS::EC2::Volume	是	是	是	是	是	是	是	是	是	是
AWS::ECR::PullThroughCacheRule	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::ECR::RegistryPolicy	是	是	是	是	是	是	是	是	是	是
AWS::ECR::Repository	是	是	是	是	是	是	是	是	是	是
AWS::ECS::CapacityProvider	是	是	是	是	是	是	是	是	是	是
AWS::ECS::Cluster	是	是	是	是	是	是	是	是	是	是
AWS::ECS::Service	是	是	是	是	是	是	是	是	是	是
AWS::ECS::TaskDefinition	是	是	是	是	是	是	是	是	是	是
AWS::ECS::TaskSet	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::EFS::AccessPoint	是	是	是	是	是	是	是	是	是	是
AWS::EFS::FileSystem	是	是	是	是	是	是	是	是	是	是
AWS::EKS::Addon	是	是	是	是	是	是	是	是	是	是
AWS::EKS::Cluster	是	是	是	是	是	是	是	是	是	是
AWS::EKS::FargateProfile	是	是	是	是	是	是	是	是	是	是
AWS::EKS::IdentityProviderConfig	是	是	是	是	是	是	是	是	是	是
AWS::EMR::SecurityConfiguration	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::ElasticBeanstalk::Application	是	是	是	否	是	否	否	是	是	是
AWS::ElasticBeanstalk::ApplicationVersion	是	是	是	否	是	否	否	是	是	是
AWS::ElasticBeanstalk::Environment	是	是	是	否	是	否	否	是	是	是
AWS::ElasticLoadBalancing::LoadBalancer	是	是	是	是	是	是	是	是	是	是
AWS::ElasticLoadBalancingV2::Listener	是	否	是	否	是	是	否	是	是	是
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是	是	是	是	是	是	是	是	是
AWS::Elasticsearch::Domain	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::EventSchemas::Discoverer	是	否	是	否	是	否	否	是	是	是
AWS::EventSchemas::Registry	是	否	是	否	是	否	否	是	是	是
AWS::EventSchemas::RegistryPolicy	是	否	是	否	是	否	否	是	是	是
AWS::EventSchemas::Schema	是	否	是	否	是	否	否	是	是	是
AWS::Events::ApiDestination	是	否	是	否	是	否	否	是	是	是
AWS::Events::Archive	是	是	是	是	是	是	否	是	是	是
AWS::Events::Connection	是	否	是	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Events::Endpoint	是	否	否	否	是	是	否	是	是	是
AWS::Events::EventBus	是	是	是	否	是	是	否	是	是	是
AWS::Events::Rule	是	否	是	是	是	是	是	是	是	是
AWS::Evidently::Launch	否	否	否	否	否	否	否	是	是	是
AWS::Evidently::Project	否	否	否	否	否	否	否	是	是	是
AWS::Evidently::Segment	否	否	否	否	否	否	否	是	是	是
AWS::FIS::ExperimentTemplate	是	否	是	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Forecast::Dataset	是	否	否	否	是	否	否	是	是	是
AWS::Forecast::DatasetGroup	是	否	否	否	是	否	否	是	是	是
AWS::FraudDetector::EntityType	否	否	否	否	否	否	否	否	是	是
AWS::FraudDetector::Label	否	否	否	否	否	否	否	否	是	是
AWS::FraudDetector::Outcome	否	否	否	否	否	否	否	否	是	是
AWS::FraudDetector::Variable	否	否	否	否	否	否	否	否	是	是
AWS::Glue::Classifier	是	否	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Glue::Job	是	否	是	是	是	是	是	是	是	是
AWS::Glue:: mlTransf	是	否	是	是	是	是	是	是	是	是
AWS::Grafana::Workspace	否	否	否	否	是	否	否	是	是	是
AWS::GreengrassV2::ComponentVersion	是	否	否	否	是	否	否	是	是	是
AWS::GroundStation::Config	否	否	否	否	是	否	否	否	是	是
AWS::GroundStation::DataflowEndpoint群组	否	否	否	否	是	否	否	否	是	是
AWS::GroundStation::MissionProfile	否	否	否	否	是	否	否	否	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::GuardDuty::Detector	是	否	是	否	是	是	否	是	是	是
AWS::GuardDuty::Filter	是	否	是	否	是	是	否	是	是	是
AWS::Guard 职责:: IPset	是	否	是	否	是	是	否	是	是	是
AWS::GuardDuty::ThreatIntelSet	是	否	是	否	是	是	否	是	是	是
AWS::HealthLake::fhirdataStore	是	否	否	否	否	否	否	否	否	否
AWS::IAM::Group	是	是	是	否	是	是	否	是	是	是
AWS::IAM::Policy	是	是	是	否	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::IAM::Role	是	是	是	否	是	是	否	是	是	是
AWS::IAM::User	是	是	是	否	是	是	否	是	是	是
AWS::IVS::Channel	是	否	否	否	是	否	否	是	否	否
AWS::IVS::PlaybackKey配对	是	否	否	否	是	否	否	是	否	否
AWS::IVS::RecordingConfiguration	是	否	否	否	是	否	否	否	否	否
AWS::ImageBuilder::ContainerRecipe	是	是	是	是	是	是	是	是	是	是
AWS::ImageBuilder::DistributionConfiguration	是	是	是	否	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::ImageBuilder::ImagePipeline	是	是	是	是	是	是	是	是	是	是
AWS::ImageBuilder::ImageRecipe	是	是	是	否	是	是	否	是	是	是
AWS::ImageBuilder::InfrastructureConfiguration	是	是	是	是	是	是	是	是	是	是
AWS::InspectorV2::Filter	是	否	是	否	是	否	否	是	是	是
AWS::IoT::AccountAudit配置	是	否	是	否	是	否	否	是	是	是
AWS::IoT::Authorizer	是	否	是	否	是	否	否	是	是	是
AWS::IoT::caCertificate	是	否	是	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::IoT::CustomMetric	是	否	是	否	是	否	否	是	是	是
AWS::IoT::Dimension	是	否	是	否	是	否	否	是	是	是
AWS::IoT::FleetMetric	是	否	是	否	是	否	否	是	是	是
AWS::IoT::JobTemplate	是	否	是	否	是	否	否	是	是	是
AWS::IoT::MitigationAction	是	否	是	否	是	否	否	是	是	是
AWS::IoT::Policy	是	否	是	否	是	否	否	是	是	是
AWS::IoT::ProvisioningTemplate	是	否	是	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::IoT::RoleAlias	是	否	是	否	是	否	否	是	是	是
AWS::IoT::ScheduledAudit	是	否	是	否	是	否	否	是	是	是
AWS::IoT::SecurityProfile	是	否	是	否	是	否	否	是	是	是
AWS::IoTAnalytics::Channel	是	否	否	否	否	否	否	是	否	是
AWS::IoTAnalytics::Dataset	是	否	否	否	否	否	否	是	否	是
AWS::IoTAnalytics::Datastore	是	否	否	否	否	否	否	是	否	是
AWS::IoTAnalytics::Pipeline	是	否	否	否	否	否	否	是	否	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::IoTEvents::AlarmModel	是	否	否	否	是	否	否	是	是	是
AWS::IoTEvents::DetectorModel	是	否	否	否	是	否	否	是	是	是
AWS::IoTEvents::Input	是	否	否	否	是	否	否	是	是	是
AWS::IoTSiteWise::AssetModel	是	否	否	否	是	否	否	是	是	是
AWS::IoTSiteWise::Dashboard	是	否	否	否	是	否	否	是	是	是
AWS::IoTSiteWise::Gateway	是	否	否	否	是	否	否	是	是	是
AWS::IoTSiteWise::Portal	是	否	否	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::IoTSiteWise::Project	是	否	否	否	是	否	否	是	是	是
AWS::IoTTwinMaker::ComponentType	否	否	否	否	否	否	否	否	是	是
AWS::IoTTwinMaker::Entity	否	否	否	否	否	否	否	否	是	是
AWS::IoTTwinMaker::Scene	否	否	否	否	否	否	否	否	是	是
AWS::IoTTwinMaker::SyncJob	否	否	否	否	否	否	否	否	是	是
AWS::IoTTwinMaker::Workspace	否	否	否	否	否	否	否	否	是	是
AWS::IoTWireless::FuotaTask	否	否	否	否	否	否	否	是	否	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::IoTWireless::MulticastGroup	否	否	否	否	否	否	否	是	否	是
AWS::IoTWireless::ServiceProfile	否	否	否	否	否	否	否	是	否	是
AWS::KMS::Alias	是	是	是	否	是	是	否	是	是	是
AWS::KMS::Key	是	是	是	是	是	是	是	是	是	是
AWS::KafkaConnect::Connector	是	否	否	否	是	否	否	是	是	是
AWS::Kendra::Index	是	否	否	否	否	否	否	是	是	是
AWS::Kinesis::Stream	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Kinesis::StreamConsumer	是	否	是	是	是	是	是	是	是	是
AWS::KinesisAnalyticsV2::Application	是	是	是	否	是	是	否	是	是	是
AWS::KinesisFirehose::DeliveryStream	是	是	是	是	是	是	是	是	是	是
AWS::KinesisVideo::SignalingChannel	是	否	是	否	是	否	否	是	是	是
AWS::KinesisVideo::Stream	是	否	是	否	是	否	否	是	是	是
AWS::Lambda::CodeSigningConfig	是	否	是	否	是	否	否	是	是	是
AWS::Lambda::Function	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Lex::Bot	否	否	否	否	是	否	否	是	是	是
AWS::Lex::BotAlias	否	否	否	否	是	否	否	是	是	是
AWS::Lightsail::Bucket	是	否	否	否	是	否	否	是	是	是
AWS::Lightsail::Certificate	是	否	否	否	是	否	否	是	是	是
AWS::Lightsail::Disk	是	否	否	否	是	否	否	是	是	是
AWS::Lightsail::StaticIp	是	否	否	否	是	否	否	是	是	是
AWS::Logs::Destination	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::LookoutMetrics::Alert	否	否	否	否	否	否	否	是	是	是
AWS::LookoutVision::Project	否	否	否	否	是	否	否	是	否	否
AWS::M2::Environment	是	否	否	否	是	否	否	是	是	是
AWS::MSK::BatchScram秘密	是	是	是	是	是	是	是	是	是	是
AWS::MSK::Cluster	是	是	是	是	是	是	是	是	是	是
AWS::MSK::ClusterPolicy	是	是	是	是	是	是	是	是	是	是
AWS::MSK::Configuration	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::MSK::VpcConnection	是	是	是	是	是	是	是	是	是	是
AWS::MediaConnect::FlowEntitlement	是	否	是	否	是	是	否	是	是	是
AWS::MediaConnect::FlowSource	是	否	是	否	是	是	否	是	是	是
AWS::MediaConnect::FlowVpc接口	是	否	是	否	是	是	否	是	是	是
AWS::MediaPackage::PackagingConfiguration	是	否	否	否	是	否	否	是	是	是
AWS::MediaPackage::PackagingGroup	是	否	否	否	是	否	否	是	是	是
AWS::MediaTailor::PlaybackConfiguration	是	否	否	否	否	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::MemoryDB::SubnetGroup	是	否	是	否	是	否	否	是	是	是
AWS::NetworkFirewall::Firewall	是	是	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是	是	是	是	是	是	是	是	是
AWS::NetworkFirewall::RuleGroup	是	是	是	是	是	是	是	是	是	是
AWS::Network防火墙:: TLS InspectionConfiguration	是	否	是	是	是	是	是	是	是	是
AWS::OpenSearch::Domain	是	是	是	否	是	是	否	是	是	是
AWS::Panorama::Package	否	否	否	否	否	否	否	否	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Personalize::Dataset	是	否	否	否	是	否	否	是	是	是
AWS::Personalize::DatasetGroup	是	否	否	否	是	否	否	是	是	是
AWS::Personalize::Schema	是	否	否	否	是	否	否	是	是	是
AWS::Personalize::Solution	是	否	否	否	是	否	否	是	是	是
AWS::Pinpoint::App	是	否	否	否	是	否	否	是	是	是
AWS::Pinpoint::ApplicationSettings	是	否	否	否	是	否	否	是	是	是
AWS::Pinpoint::Campaign	是	否	否	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Pinpoint::EmailChannel	是	否	否	否	是	否	否	是	是	是
AWS::Pinpoint::EmailTemplate	是	否	否	否	是	否	否	是	是	是
AWS::Pinpoint::EventStream	是	否	否	否	是	否	否	是	是	是
AWS::Pinpoint::InApp模板	是	否	否	否	是	否	否	是	是	是
AWS::Pinpoint::Segment	是	否	否	否	是	否	否	是	是	是
AWS::QLDB::Ledger	否	否	否	否	是	否	否	是	是	是
AWS::QuickSight::DataSource	是	否	否	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::QuickSight::Template	是	否	否	否	是	否	否	是	是	是
AWS::QuickSight::Theme	是	否	否	否	是	否	否	是	是	是
AWS::RDS::DBCluster	是	是	是	否	是	是	否	是	是	是
AWS:: RDS:: DB ClusterSnapshot	是	是	是	是	是	是	是	是	是	是
AWS::RDS::DBInstance	是	是	是	是	是	是	是	是	是	是
AWS:: RDS:: DB SecurityGroup	是	是	是	是	是	是	是	是	是	是
AWS::RDS::DBSnapshot	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS:: RDS:: DB SubnetGroup	是	是	是	是	是	是	是	是	是	是
AWS::RDS: :EventSubscription	是	是	是	是	是	是	是	是	是	是
AWS::RDS: :GlobalCluster	是	否	否	否	是	否	否	是	是	是
AWS::RDS: :OptionGroup	是	是	是	是	是	是	是	是	是	是
AWS::RUM: :AppMonitor	否	否	否	否	否	否	否	是	是	是
AWS::Redshift::Cluster	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::Cluster Parameter群组	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Redshift::ClusterSecurity群组	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSnapshot	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::ClusterSubnet群组	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::EndpointAccess	是	否	否	否	是	否	否	是	是	是
AWS::Redshift::EndpointAuthorization	是	否	否	否	是	否	否	是	是	是
AWS::Redshift::EventSubscription	是	是	是	是	是	是	是	是	是	是
AWS::Redshift::ScheduledAction	是	否	是	否	是	否	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::ResilienceHub::App	是	否	是	否	是	否	否	是	是	是
AWS::ResilienceHub::ResiliencyPolicy	是	否	是	否	是	否	否	是	是	是
AWS::ResourceExplorer2::Index	是	否	否	否	是	是	否	是	是	是
AWS::RoboMaker::RobotApplication	否	否	否	否	否	否	否	是	是	否
AWS::RoboMaker::RobotApplication版本	否	否	否	否	否	否	否	是	是	否
AWS::RoboMaker::SimulationApplication	否	否	否	否	否	否	否	是	是	否
AWS::Route53Resolver::FirewallDomain名单	是	是	是	否	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::Route53Resolver::FirewallRule群组	是	是	是	否	是	是	否	是	是	是
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是	是	否	是	是	否	是	是	是
AWS::Route53Resolver::ResolverEndpoint	是	否	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	否	是	否	是	是	否	是	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig协会	是	否	是	否	是	是	否	是	是	是
AWS::Route53Resolver::ResolverRule	是	否	是	是	是	是	是	是	是	是
AWS::Route53Resolver::ResolverRule协会	是	否	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::S3::AccessPoint	是	是	是	是	是	是	是	是	是	是
AWS::S3::AccountPublicAccessBlock	是	否	是	否	是	是	否	是	是	是
AWS::S3::Bucket	是	是	是	是	是	是	是	是	是	是
AWS::S3::StorageLens	是	否	否	否	是	否	否	是	是	是
AWS::SES::ConfigurationSet	是	是	否	否	是	是	否	是	是	是
AWS::SES::ContactList	是	是	否	否	是	是	否	是	是	是
AWS::SES::Template	是	是	否	否	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::SNS::Topic	是	否	是	否	是	是	否	是	是	是
AWS::SQS::Queue	是	否	是	否	是	是	否	是	是	是
AWS::SSM::AssociationCompliance	是	是	是	是	是	否	是	是	是	是
AWS::SSM::Document	是	是	是	是	是	是	是	是	是	是
AWS::SSM::FileData	是	是	是	是	是	否	是	是	是	是
AWS::SSM::ManagedInstance库存	是	是	是	是	是	是	是	是	是	是
AWS::SSM::PatchCompliance	是	是	是	是	是	否	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::SageMaker::AppImageConfig	是	是	是	否	是	是	否	是	是	是
AWS::SageMaker::CodeRepository	是	否	是	否	是	是	否	是	是	是
AWS::SageMaker::Domain	是	是	是	否	是	是	否	是	是	是
AWS::SageMaker::EndpointConfig	是	是	是	否	是	是	否	是	是	是
AWS::SageMaker::FeatureGroup	是	否	是	否	是	是	否	是	是	是
AWS::SageMaker::Image	是	否	是	否	是	否	否	是	是	是
AWS::SageMaker::Model	是	是	是	否	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::SageMaker::NotebookInstance	是	是	是	否	是	是	否	是	是	是
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	否	是	否	是	是	否	是	是	是
AWS::SageMaker::Workteam	是	否	否	否	是	否	否	是	是	是
AWS::SecretsManager::Secret	是	是	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::CloudFormation产品	是	否	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	否	是	是	是	是	是	是	是	是
AWS::ServiceCatalog::Portfolio	是	否	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::ServiceDiscovery::HttpNamespace	是	否	是	否	是	否	是	是	是	是
AWS::ServiceDiscovery::Instance	是	否	是	否	是	否	否	是	是	是
AWS::ServiceDiscovery::PublicDns命名空间	是	否	是	否	是	否	否	是	是	是
AWS::ServiceDiscovery::Service	是	否	是	否	是	否	否	是	是	是
AWS::ShieldRegional::Protection	是	是	是	否	是	是	否	是	是	是
AWS::Signer::SigningProfile	是	否	是	否	是	否	否	是	是	是
AWS::StepFunctions::Activity	是	是	是	是	是	是	否	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::StepFunctions::StateMachine	是	是	是	是	是	是	否	是	是	是
AWS::Transfer::Agreement	是	是	是	否	是	是	否	是	是	是
AWS::Transfer::Certificate	是	是	是	否	是	是	否	是	是	是
AWS::Transfer::Connector	是	是	是	否	是	是	否	是	是	是
AWS::Transfer::Profile	是	是	是	是	是	是	是	是	是	是
AWS::Transfer::Workflow	是	是	是	否	是	是	否	是	是	是
AWS::WAFRegional::RateBased规则	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::WAFRegional::Rule	是	是	是	是	是	是	是	是	是	是
AWS::WAFRegional::RuleGroup	是	是	是	是	是	是	是	是	是	是
AWS::WAFRegional::WebACL	是	是	是	是	是	是	是	是	是	是
AWS::WAFv2::IPSet	是	是	是	是	是	是	是	是	是	是
AWS::WAFv2::ManagedRuleSet	是	是	是	是	是	是	是	是	是	是
AWS::WAFv2::RegexPatternSet	是	是	是	是	是	是	是	是	是	是
AWS::WAFv2::RuleGroup	是	是	是	是	是	是	是	是	是	是

资源类型	亚太地区（新加坡）	亚太地区（东京）	亚太地区（悉尼）	亚太地区（首尔）	亚太地区（孟买）	亚太地区（大阪）	亚太地区（香港）	亚太地区（雅加达）	亚太地区（海得拉巴）	亚太地区（墨尔本）
AWS::WAFv2::WebACL	是	是	是	是	是	是	是	是	是	是
AWS::WorkSpaces::ConnectionAlias	否	否	否	否	是	否	否	是	是	是
AWS::WorkSpaces::Workspace	是	否	否	否	是	否	否	是	是	是
AWS::XRay::EncryptionConfig	是	是	是	是	是	是	是	是	是	是

中国区域

资源类型	中国（北京）	中国（宁夏）
AWS::ACM::Certificate	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::AmazonMQ::Broker	是	是
AWS::ApiGateway::RestApi	是	是
AWS::ApiGateway::Stage	是	是
AWS::ApiGatewayV2::Api	是	是
AWS::ApiGatewayV2::Stage	是	是
AWS::AppConfig::Application	是	是
AWS::AppConfig::ConfigurationProfile	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::AppConfig::DeploymentStrategy	是	是
AWS::AppConfig::Environment	是	是
AWS::AppConfig::ExtensionAssociation	是	是
AWS::AppConfig::HostedConfiguration版本	是	是
AWS::AppSync::GraphqlaPi	是	是
AWS::Athena::DataCatalog	是	是
AWS::Athena::PreparedStatement	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Athena::WorkGroup	是	是
AWS::AutoScaling::AutoScaling群组	是	是
AWS::AutoScaling::LaunchConfiguration	是	是
AWS::AutoScaling::ScalingPolicy	是	是
AWS::AutoScaling::ScheduledAction	是	是
AWS::AutoScaling::WarmPool	是	是
AWS::Backup::BackupPlan	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Backup::BackupSelection	是	是
AWS::Backup::BackupVault	是	是
AWS::Backup::RecoveryPoint	是	是
AWS::Batch::ComputeEnvironment	是	是
AWS::Batch::JobQueue	是	是
AWS::Batch::SchedulingPolicy	是	是
AWS::Cassandra::Keyspace	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::CloudFormation::Stack	是	是
AWS::CloudTrail::Trail	是	是
AWS::CloudWatch::Alarm	是	是
AWS::CloudWatch::MetricStream	是	是
AWS::CodeBuild::Project	是	是
AWS::CodeBuild::ReportGroup	是	是
AWS::Config::ConfigurationRecorder	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Config::ResourceCompliance	是	是
AWS::DMS::Certificate	是	是
AWS::DMS::Endpoint	是	是
AWS::DMS::EventSubscription	是	是
AWS::DMS::ReplicationInstance	是	是
AWS::DMS::ReplicationSubnet群组	是	是
AWS::DMS::ReplicationTask	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::DataSync::LocationEFS	是	是
AWS::DataSync::LocationHDFS	是	是
AWS::DataSync::LocationNFS	是	是
AWS::DataSync::LocationObject存储	是	是
AWS::DataSync::LocationS3	是	是
AWS::DataSync::Location中小型企业	是	是
AWS::DataSync::Task	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::DynamoDB::Table	是	是
AWS::EC2::CapacityReservation	是	是
AWS::EC2::DHCPOptions	是	是
AWS::EC2::EC2Fleet	是	是
AWS::EC2::EIP	是	是
AWS::EC2::FlowLog	是	是
AWS::EC2::Host	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::EC2::Instance	是	是
AWS::EC2::InternetGateway	是	是
AWS::EC2::LaunchTemplate	是	是
AWS::EC2::NatGateway	是	是
AWS::EC2::NetworkAcl	是	是
AWS::EC2::NetworkInterface	是	是
AWS::EC2::PrefixList	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::EC2::RouteTable	是	是
AWS::EC2::SecurityGroup	是	是
AWS::EC2::SpotFleet	是	是
AWS::EC2::Subnet	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是
AWS::EC2::TrafficMirror过滤器	是	是
AWS::EC2::TrafficMirror会话	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::EC2::TrafficMirror目标	是	是
AWS::EC2::TransitGateway	是	是
AWS::EC2::TransitGateway附件	是	是
AWS::EC2::TransitGatewayConnect	是	是
AWS::EC2::TransitGatewayMulticastDomain	是	是
AWS::EC2::TransitGatewayRouteTable	是	是
AWS::EC2::VPC	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::EC2::VPCEndpoint	是	是
AWS:: EC2:: VPC EndpointService	是	是
AWS:: EC2:: VPC PeeringConnection	是	是
AWS::EC2::VPNGateway	是	否
AWS::EC2::Volume	是	是
AWS::ECR::Repository	是	是
AWS::ECS::CapacityProvider	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::ECS::Cluster	是	是
AWS::ECS::Service	是	是
AWS::ECS::TaskDefinition	是	是
AWS::ECS::TaskSet	是	是
AWS::EFS::AccessPoint	是	是
AWS::EFS::FileSystem	是	是
AWS::EKS::Addon	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::EKS::Cluster	是	是
AWS::EKS::FargateProfile	是	是
AWS::EKS::IdentityProviderConfig	是	是
AWS::EMR::SecurityConfiguration	是	是
AWS::ElasticBeanstalk::Application	是	是
AWS::ElasticBeanstalk::ApplicationVersion	是	是
AWS::ElasticBeanstalk::Environment	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::ElasticLoadBalancing::LoadBalancer	是	是
AWS::ElasticLoadBalancingV2::Listener	是	是
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是
AWS::Elasticsearch::Domain	是	是
AWS::Events::Archive	是	是
AWS::Events::EventBus	是	是
AWS::Events::Rule	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Glue::Classifier	是	是
AWS::Glue::Job	是	是
AWS::Glue:: mlTransf	是	否
AWS::GreengrassV2::ComponentVersion	是	否
AWS::GuardDuty::Filter	是	是
AWS::GuardDuty::ThreatIntelSet	是	是
AWS::IAM::Group	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::IAM::InstanceProfile	是	否
AWS::IAM::OIDCProvider	是	否
AWS::IAM::Policy	是	是
AWS::IAM::Role	是	是
AWS::IAM::SAMLProvider	是	否
AWS::IAM::ServerCertificate	是	否
AWS::IAM::User	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::ImageBuilder::ContainerRecipe	是	是
AWS::ImageBuilder::DistributionConfiguration	是	是
AWS::ImageBuilder::ImagePipeline	是	是
AWS::ImageBuilder::ImageRecipe	是	是
AWS::ImageBuilder::InfrastructureConfiguration	是	是
AWS::IoT::AccountAudit配置	是	是
AWS::IoT::Authorizer	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::IoT:: caCertificate	是	是
AWS::IoT::CustomMetric	是	是
AWS::IoT::Dimension	是	是
AWS::IoT::FleetMetric	是	是
AWS::IoT::JobTemplate	是	是
AWS::IoT::MitigationAction	是	是
AWS::IoT::Policy	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::IoT::ProvisioningTemplate	是	是
AWS::IoT::RoleAlias	是	是
AWS::IoT::ScheduledAudit	是	是
AWS::IoT::SecurityProfile	是	是
AWS::IoTAnalytics::Channel	是	否
AWS::IoTAnalytics::Dataset	是	否
AWS::IoTAnalytics::Datastore	是	否

资源类型	中国（北京）	中国（宁夏）
AWS::IoTAnalytics::Pipeline	是	否
AWS::IoTEvents::AlarmModel	是	否
AWS::IoTEvents::DetectorModel	是	否
AWS::IoTEvents::Input	是	否
AWS::IoTSiteWise::AssetModel	是	否
AWS::IoTSiteWise::Dashboard	是	否
AWS::IoTSiteWise::Gateway	是	否

资源类型	中国（北京）	中国（宁夏）
AWS::IoTSiteWise::Portal	是	否
AWS::IoTSiteWise::Project	是	否
AWS::KMS::Alias	是	是
AWS::KMS::Key	是	是
AWS::Kinesis::Stream	是	是
AWS::Kinesis::StreamConsumer	是	是
AWS::KinesisAnalyticsV2::Application	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::KinesisFirehose::DeliveryStream	是	是
AWS::Lambda::Function	是	否
AWS::Logs::Destination	是	是
AWS::MSK::BatchScram秘密	是	是
AWS::MSK::Cluster	是	是
AWS::MSK::ClusterPolicy	是	是
AWS::MSK::Configuration	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::MSK::VpcConnection	是	是
AWS::NetworkFirewall::Firewall	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是
AWS::NetworkFirewall::RuleGroup	是	是
AWS::Network防火墙:: TLS InspectionConfiguration	是	是
AWS::OpenSearch::Domain	是	是
AWS::Personalize::Dataset	是	否

资源类型	中国（北京）	中国（宁夏）
AWS::Personalize::DatasetGroup	是	否
AWS::Personalize::Schema	是	否
AWS::Personalize::Solution	是	否
AWS::RDS::DBCluster	否	是
AWS:: RDS:: DB ClusterSnapshot	是	是
AWS::RDS::DBInstance	是	是
AWS:: RDS:: DB SecurityGroup	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::RDS::DBSnapshot	是	是
AWS:: RDS:: DB SubnetGroup	是	是
AWS::RDS::EventSubscription	是	是
AWS::RDS::OptionGroup	是	是
AWS::Redshift::Cluster	是	是
AWS::Redshift::ClusterParameter群组	是	是
AWS::Redshift::ClusterSecurity群组	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Redshift::ClusterSnapshot	是	是
AWS::Redshift::ClusterSubnet群组	是	是
AWS::Redshift::EventSubscription	是	是
AWS::Route53Resolver::FirewallDomain名单	是	是
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是
AWS::Route53Resolver::ResolverEndpoint	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Route53Resolver::ResolverQueryLoggingConfig协会	是	是
AWS::Route53Resolver::ResolverRule	是	是
AWS::Route53Resolver::ResolverRule协会	是	是
AWS::S3::AccessPoint	是	是
AWS::S3::AccountPublicAccessBlock	是	是
AWS::S3::Bucket	是	是
AWS::SES::ConfigurationSet	否	是

资源类型	中国（北京）	中国（宁夏）
AWS::SES::ContactList	否	是
AWS::SES::Template	否	是
AWS::SNS::Topic	是	是
AWS::SQS::Queue	是	是
AWS::SSM::AssociationCompliance	是	是
AWS::SSM::Document	是	是
AWS::SSM::FileData	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::SSM::ManagedInstance库存	是	是
AWS::SSM::PatchCompliance	是	是
AWS::SageMaker::AppImageConfig	是	是
AWS::SageMaker::CodeRepository	是	是
AWS::SageMaker::Domain	是	是
AWS::SageMaker::EndpointConfig	是	是
AWS::SageMaker::FeatureGroup	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::SageMaker::Image	是	是
AWS::SageMaker::Model	是	是
AWS::SageMaker::NotebookInstance	是	是
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	是
AWS::SecretsManager::Secret	是	是
AWS::ServiceCatalog::CloudFormation产品	是	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::ServiceCatalog::Portfolio	是	是
AWS::ServiceDiscovery::HttpNamespace	是	是
AWS::ServiceDiscovery::Instance	是	是
AWS::ServiceDiscovery::PublicDns命名空间	是	是
AWS::ServiceDiscovery::Service	是	是
AWS::StepFunctions::Activity	是	否
AWS::StepFunctions::StateMachine	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::Transfer::Agreement	是	是
AWS::Transfer::Certificate	是	是
AWS::Transfer::Connector	是	是
AWS::Transfer::Profile	是	是
AWS::Transfer::Workflow	是	是
AWS::WAFRegional::RateBased规则	是	是
AWS::WAFRegional::Rule	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::WAFRegional::RuleGroup	是	是
AWS::WAFRegional::WebACL	是	是
AWS::WAFv2::IPSet	是	是
AWS::WAFv2::ManagedRuleSet	是	是
AWS::WAFv2::RegexPatternSet	是	是
AWS::WAFv2::RuleGroup	是	是
AWS::WAFv2::WebACL	是	是

资源类型	中国（北京）	中国（宁夏）
AWS::WorkSpaces::Workspace	否	是

非洲和中东区域

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::ACM::Certificate	是	是	是	是
AWS::ACMPCA::CertificateAuthority	是	是	是	否
AWS::ACMPCA::CertificateAuthority激活	是	是	是	否
AWS::AccessAnalyzer::Analyzer	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::AmazonMQ::Broker	是	是	是	否
AWS::Amplify::App	是	否	否	否
AWS::Amplify::Branch	是	否	否	否
AWS::ApiGateway::RestApi	是	是	是	是
AWS::ApiGateway::Stage	是	是	是	是
AWS::ApiGatewayV2::Api	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::ApiGatewayV2::Stage	是	是	是	是
AWS::AppConfig::Application	是	是	否	是
AWS::AppConfig::ConfigurationProfile	是	是	否	是
AWS::AppConfig::DeploymentStrategy	是	是	否	是
AWS::AppConfig::Environment	是	是	否	是
AWS::AppConfig::ExtensionAssociation	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::AppConfig::HostedConfiguration版本	是	是	否	是
AWS::AppIntegrations::EventIntegration	否	是	否	否
AWS::AppMesh::GatewayRoute	是	是	否	否
AWS::AppMesh::Mesh	是	是	否	否
AWS::AppMesh::Route	是	是	否	否
AWS::AppMesh::VirtualGateway	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::AppMesh::VirtualNode	是	是	否	否
AWS::AppMesh::VirtualRouter	是	是	否	否
AWS::AppMesh::VirtualService	是	是	否	否
AWS::AppSync::GraphqlaPi	是	是	是	否
AWS::Athena::DataCatalog	是	是	是	否
AWS::Athena::PreparedStatement	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Athena::WorkGroup	是	是	是	否
AWS::AutoScaling::AutoScaling群组	是	是	是	是
AWS::AutoScaling::LaunchConfiguration	是	是	是	是
AWS::AutoScaling::ScalingPolicy	是	是	是	是
AWS::AutoScaling::ScheduledAction	是	是	是	是
AWS::AutoScaling::WarmPool	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Backup::BackupPlan	是	是	否	否
AWS::Backup::BackupSelection	是	是	是	否
AWS::Backup::BackupVault	是	是	是	否
AWS::Backup::RecoveryPoint	是	是	否	否
AWS::Backup::ReportPlan	是	是	否	否
AWS::Batch::ComputeEnvironment	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Batch::JobQueue	是	是	是	否
AWS::Batch::SchedulingPolicy	是	是	是	否
AWS::Cassandra::Keyspace	是	否	否	否
AWS::Cloud9::EnvironmentEC2	是	是	否	否
AWS::CloudFormation::Stack	是	是	否	否
AWS::CloudTrail::Trail	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::CloudWatch::Alarm	是	是	是	是
AWS::CloudWatch::MetricStream	是	是	是	是
AWS::CodeBuild::Project	是	是	是	是
AWS::CodeBuild::ReportGroup	是	是	否	否
AWS::CodeDeploy::Application	是	是	否	否
AWS::CodeDeploy::DeploymentConfig	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::CodeDeploy::DeploymentGroup	是	是	否	否
AWS::Cognito::UserPool	是	否	否	是
AWS::Cognito::UserPool客户端	是	否	否	是
AWS::Cognito::UserPool群组	是	否	否	是
AWS::Config::ConfigurationRecorder	是	是	是	是
AWS::Config::ConformancePack合规性	是	否	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Config::ResourceCompliance	是	是	是	是
AWS::Connect::Instance	否	是	否	否
AWS::CustomerProfiles::Domain	否	是	否	否
AWS::CustomerProfiles::ObjectType	否	是	否	否
AWS::DMS::Certificate	是	是	否	否
AWS::DMS::Endpoint	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::DMS::EventSubscription	是	是	否	否
AWS::DMS::ReplicationInstance	是	是	否	否
AWS::DMS::ReplicationSubnet群组	是	是	否	否
AWS::DMS::ReplicationTask	是	是	否	否
AWS::DataSync::LocationEFS	是	是	是	否
AWS::DataSync::LocationF SxLustre	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::DataSync::LocationF SxWindows	是	是	否	否
AWS::DataSync::LocationHDFS	是	是	是	否
AWS::DataSync::LocationNFS	是	是	是	否
AWS::DataSync::LocationObject存储	是	是	是	否
AWS::DataSync::LocationS3	是	是	是	否
AWS::DataSync::Location中小型企业	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::DataSync::Task	是	是	是	否
AWS::Detective::Graph	是	是	否	否
AWS::DynamoDB::Table	是	是	是	是
AWS::EC2::CapacityReservation	是	是	否	否
AWS::EC2::ClientVpn端点	是	是	否	否
AWS::EC2::CustomerGateway	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::EC2::DHCPOptions	是	是	是	是
AWS::EC2::EC2Fleet	是	是	是	否
AWS::EC2::EIP	是	是	是	是
AWS::EC2::EgressOnlyInternetGateway	是	是	是	否
AWS::EC2::FlowLog	是	是	是	否
AWS::EC2::Host	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::EC2::IPAM	是	是	是	否
AWS::EC2::IPAMPool	是	是	是	否
AWS::EC2::IPAMScope	是	是	是	否
AWS::EC2::Instance	是	是	是	是
AWS::EC2::InternetGateway	是	是	是	是
AWS::EC2::LaunchTemplate	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::EC2::NatGateway	是	是	是	否
AWS::EC2::NetworkAcl	是	是	是	是
AWS::EC2::NetworkInsightsAccessScope	是	是	否	否
AWS::EC2::NetworkInsightsAccessScope分析	是	是	否	否
AWS::EC2::NetworkInsights分析	是	是	否	否
AWS::EC2::NetworkInsights路径	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::EC2::NetworkInterface	是	是	是	是
AWS::EC2::PrefixList	是	是	是	是
AWS::EC2::RouteTable	是	是	是	是
AWS::EC2::SecurityGroup	是	是	是	是
AWS::EC2::SpotFleet	是	是	是	是
AWS::EC2::Subnet	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::EC2::SubnetRouteTableAssociation	是	是	是	是
AWS::EC2::TrafficMirror过滤器	是	否	否	否
AWS::EC2::TrafficMirror会话	是	否	否	否
AWS::EC2::TrafficMirror目标	是	否	否	否
AWS::EC2::TransitGateway	是	是	是	否
AWS::EC2::TransitGateway附件	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::EC2::TransitGatewayConnect	是	是	是	否
AWS::EC2::TransitGatewayMulticastDomain	是	是	是	是
AWS::EC2::TransitGatewayRouteTable	是	是	是	否
AWS::EC2::VPC	是	是	是	是
AWS::EC2::VPCEndpoint	是	是	是	是
AWS:: EC2:: VPC EndpointService	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS:: EC2:: VPC PeeringConnection	是	是	是	是
AWS::EC2::VPNConnection	是	是	是	是
AWS::EC2::VPNGateway	是	是	是	是
AWS::EC2::Volume	是	是	是	是
AWS::ECR::PullThroughCacheRule	是	是	是	是
AWS::ECR::RegistryPolicy	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::ECR::Repository	是	是	是	否
AWS::ECS::CapacityProvider	是	是	是	是
AWS::ECS::Cluster	是	是	是	是
AWS::ECS::Service	是	是	是	是
AWS::ECS::TaskDefinition	是	是	是	是
AWS::ECS::TaskSet	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::EFS::AccessPoint	是	是	是	否
AWS::EFS::FileSystem	是	是	是	否
AWS::EKS::Addon	是	是	是	否
AWS::EKS::Cluster	是	是	是	否
AWS::EKS::FargateProfile	是	是	是	是
AWS::EKS::IdentityProviderConfig	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::EMR::SecurityConfiguration	是	是	是	否
AWS::ElasticBeanstalk::Application	否	是	否	否
AWS::ElasticBeanstalk::ApplicationVersion	否	是	否	否
AWS::ElasticBeanstalk::Environment	否	是	否	否
AWS::ElasticLoadBalancing::LoadBalancer	是	是	是	是
AWS::ElasticLoadBalancingV2::Listener	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是	是	是
AWS::Elasticsearch::Domain	是	是	是	是
AWS::Events::ApiDestination	是	是	否	否
AWS::Events::Archive	是	是	是	否
AWS::Events::Connection	是	是	否	否
AWS::Events::EventBus	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Events::Rule	是	是	否	否
AWS::FIS::ExperimentTemplate	是	是	否	否
AWS::Glue::Classifier	是	是	是	是
AWS::Glue::Job	是	是	是	是
AWS::Glue:: mlTransf	是	是	是	是
AWS::GroundStation::Config	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::GroundStation::DataflowEndpoint群组	是	是	否	否
AWS::GroundStation::MissionProfile	是	是	否	否
AWS::GuardDuty::Detector	是	是	否	否
AWS::GuardDuty::Filter	是	是	否	否
AWS::Guard职责:: IPset	是	是	否	否
AWS::GuardDuty::ThreatIntelSet	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::IAM::Group	是	是	否	否
AWS::IAM::Policy	是	是	否	否
AWS::IAM::Role	是	是	否	否
AWS::IAM::User	是	是	否	否
AWS::ImageBuilder::ContainerRecipe	是	是	是	是
AWS::ImageBuilder::DistributionConfiguration	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::ImageBuilder::ImagePipeline	是	是	是	是
AWS::ImageBuilder::ImageRecipe	是	是	否	否
AWS::ImageBuilder::InfrastructureConfiguration	是	是	是	是
AWS::InspectorV2::Filter	是	否	否	否
AWS::IoT::AccountAudit配置	是	否	是	否
AWS::IoT::Authorizer	是	否	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::IoT:: caCertificate	是	否	是	否
AWS::IoT::CustomMetric	是	否	是	否
AWS::IoT::Dimension	是	否	是	否
AWS::IoT::FleetMetric	是	否	是	否
AWS::IoT::JobTemplate	是	否	是	否
AWS::IoT::MitigationAction	是	否	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::IoT::Policy	是	否	是	否
AWS::IoT::ProvisioningTemplate	是	否	是	否
AWS::IoT::RoleAlias	是	否	是	否
AWS::IoT::ScheduledAudit	是	否	是	否
AWS::IoT::SecurityProfile	是	否	是	否
AWS::KMS::Alias	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::KMS::Key	是	是	是	是
AWS::Kinesis::Stream	是	是	是	否
AWS::Kinesis::StreamConsumer	是	是	是	否
AWS::KinesisAnalyticsV2::Application	是	是	是	否
AWS::KinesisFirehose::DeliveryStream	是	是	是	是
AWS::Lambda::CodeSigningConfig	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Lambda::Function	是	是	是	是
AWS::Lex::Bot	否	是	否	否
AWS::Lex::BotAlias	否	是	否	否
AWS::Logs::Destination	是	是	是	是
AWS::MSK::BatchScram秘密	是	是	是	否
AWS::MSK::Cluster	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::MSK::ClusterPolicy	是	是	是	是
AWS::MSK::Configuration	是	是	是	否
AWS::MSK::VpcConnection	是	是	是	是
AWS::MediaConnect::FlowEntitlement	否	是	否	否
AWS::MediaConnect::FlowSource	否	是	否	否
AWS::MediaConnect::FlowVpc接口	否	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::MediaTailor::PlaybackConfiguration	否	是	否	否
AWS::NetworkFirewall::Firewall	是	是	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是	是	是
AWS::NetworkFirewall::RuleGroup	是	是	是	是
AWS::Network防火墙:: TLS InspectionConfiguration	是	是	是	是
AWS::OpenSearch::Domain	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::RDS::DBCluster	是	是	是	否
AWS:: RDS:: DB ClusterSnapshot	是	是	是	否
AWS::RDS::DBInstance	是	是	是	是
AWS:: RDS:: DB SecurityGroup	是	是	是	是
AWS::RDS::DBSnapshot	是	是	是	是
AWS:: RDS:: DB SubnetGroup	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::RDS::EventSubscription	是	是	是	是
AWS::RDS::OptionGroup	是	是	是	否
AWS::Redshift::Cluster	是	是	是	是
AWS::Redshift::ClusterParameter群组	是	是	是	是
AWS::Redshift::ClusterSecurity群组	是	是	是	是
AWS::Redshift::ClusterSnapshot	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Redshift::ClusterSubnet群组	是	是	是	是
AWS::Redshift::EventSubscription	是	是	是	是
AWS::Redshift::ScheduledAction	是	否	否	否
AWS::ResilienceHub::App	是	是	否	否
AWS::ResilienceHub::ResiliencyPolicy	是	是	否	否
AWS::Route53Resolver::FirewallDomain名单	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Route53Resolver::FirewallRule群组	是	是	否	否
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是	否	否
AWS::Route53Resolver::ResolverEndpoint	是	是	是	否
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是	否	否
AWS::Route53Resolver::ResolverQueryLoggingConfig协会	是	是	否	否
AWS::Route53Resolver::ResolverRule	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Route53Resolver::ResolverRule协会	是	是	是	否
AWS::S3::AccessPoint	是	是	是	是
AWS::S3::AccountPublicAccessBlock	是	是	否	否
AWS::S3::Bucket	是	是	是	是
AWS::SES::ConfigurationSet	是	是	否	否
AWS::SES::ContactList	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::SES::Template	是	是	否	否
AWS::SNS::Topic	是	是	否	否
AWS::SQS::Queue	是	是	否	否
AWS::SSM::AssociationCompliance	是	是	是	是
AWS::SSM::Document	是	是	是	是
AWS::SSM::FileData	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::SSM::ManagedInstance库存	是	是	是	是
AWS::SSM::PatchCompliance	是	是	是	是
AWS::SageMaker::AppImageConfig	是	是	否	否
AWS::SageMaker::CodeRepository	是	是	否	否
AWS::SageMaker::Domain	是	是	否	否
AWS::SageMaker::EndpointConfig	是	是	否	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::SageMaker::FeatureGroup	是	是	否	否
AWS::SageMaker::Image	是	是	否	否
AWS::SageMaker::Model	是	是	否	否
AWS::SageMaker::NotebookInstance	是	是	否	否
AWS::SageMaker::NotebookInstanceLifecycleConfig	是	是	否	否
AWS::SecretsManager::Secret	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::ServiceCatalog::CloudFormation产品	是	是	是	否
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是	是	否
AWS::ServiceCatalog::Portfolio	是	是	是	否
AWS::ServiceDiscovery::HttpNamespace	是	是	是	是
AWS::ServiceDiscovery::Instance	是	是	是	否
AWS::ServiceDiscovery::PublicDns命名空间	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::ServiceDiscovery::Service	是	是	是	否
AWS::ShieldRegional::Protection	是	是	是	否
AWS::Signer::SigningProfile	是	是	否	否
AWS::StepFunctions::Activity	是	是	是	否
AWS::StepFunctions::StateMachine	是	是	是	否
AWS::Transfer::Agreement	是	是	是	否

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::Transfer::Certificate	是	是	是	否
AWS::Transfer::Connector	是	是	是	否
AWS::Transfer::Profile	是	是	是	是
AWS::Transfer::Workflow	是	是	否	否
AWS::WAFRegional::RateBased规则	是	是	是	是
AWS::WAFRegional::Rule	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::WAFRegional::RuleGroup	是	是	是	是
AWS::WAFRegional::WebACL	是	是	是	是
AWS::WAFv2::IPSet	是	是	是	是
AWS::WAFv2::ManagedRuleSet	是	是	是	是
AWS::WAFv2::RegexPatternSet	是	是	是	是
AWS::WAFv2::RuleGroup	是	是	是	是

资源类型	非洲（开普敦）	中东（巴林）	中东（阿联酋）	以色列（特拉维夫）
AWS::WAFv2::WebACL	是	是	是	是
AWS::WorkSpaces::Workspace	否	是	否	否
AWS::XRay::EncryptionConfig	否	是	是	是

GovCloud 区域

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::ACM::Certificate	是	是
AWS::ACMPCA::CertificateAuthority	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::ACMPCA::CertificateAuthority激活	是	是
AWS::AccessAnalyzer::Analyzer	是	是
AWS::AmazonMQ::Broker	是	是
AWS::ApiGateway::RestApi	是	是
AWS::ApiGateway::Stage	是	是
AWS::ApiGatewayV2::Api	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::ApiGatewayV2::Stage	是	是
AWS::AppConfig::Application	是	是
AWS::AppConfig::ConfigurationProfile	是	是
AWS::AppConfig::DeploymentStrategy	是	是
AWS::AppConfig::Environment	是	是
AWS::AppConfig::ExtensionAssociation	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::AppConfig::HostedConfiguration版本	是	是
AWS::AppStream::Application	是	是
AWS::AppStream::DirectoryConfig	否	是
AWS::AppStream::Fleet	否	是
AWS::AppStream::Stack	否	是
AWS::Athena::DataCatalog	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::Athena::WorkGroup	是	是
AWS::AutoScaling::AutoScaling群组	是	是
AWS::AutoScaling::LaunchConfiguration	是	是
AWS::AutoScaling::ScalingPolicy	是	是
AWS::AutoScaling::ScheduledAction	是	是
AWS::AutoScaling::WarmPool	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::Backup::BackupPlan	是	是
AWS::Backup::BackupSelection	是	是
AWS::Backup::BackupVault	是	是
AWS::Backup::RecoveryPoint	是	是
AWS::Batch::ComputeEnvironment	是	是
AWS::Batch::JobQueue	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::Batch::SchedulingPolicy	是	是
AWS::Cassandra::Keyspace	是	是
AWS::CloudFormation::Stack	是	是
AWS::CloudTrail::Trail	是	是
AWS::CloudWatch::Alarm	是	是
AWS::CodeBuild::Project	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::CodeBuild::ReportGroup	是	是
AWS::Cognito::UserPool群组	否	是
AWS::Config::ConfigurationRecorder	是	是
AWS::Config::ConformancePack合规性	是	是
AWS::Config::ResourceCompliance	是	是
AWS::Connect::Instance	否	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::Connect::QuickConnect	否	是
AWS::DMS::Certificate	是	是
AWS::DMS::Endpoint	是	是
AWS::DMS::EventSubscription	是	是
AWS::DMS::ReplicationInstance	是	是
AWS::DMS::ReplicationSubnet群组	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::DMS::ReplicationTask	是	是
AWS::DataSync::LocationEFS	是	是
AWS::DataSync::LocationF SxLustre	是	是
AWS::DataSync::LocationF SxWindows	是	是
AWS::DataSync::LocationHDFS	是	是
AWS::DataSync::LocationNFS	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::DataSync::LocationObject存储	是	是
AWS::DataSync::LocationS3	是	是
AWS::DataSync::Location中小型企业	是	是
AWS::DataSync::Task	是	是
AWS::Detective::Graph	是	是
AWS::DynamoDB::Table	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::EC2::CapacityReservation	是	是
AWS::EC2::ClientVpn端点	是	是
AWS::EC2::CustomerGateway	是	是
AWS::EC2::DHCPOptions	是	是
AWS::EC2::EC2Fleet	是	是
AWS::EC2::EIP	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::EC2::EgressOnlyInternetGateway	是	是
AWS::EC2::FlowLog	是	是
AWS::EC2::Host	是	是
AWS::EC2::IPAM	是	是
AWS::EC2::IPAMPool	是	是
AWS::EC2::IPAMScope	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::EC2::Instance	是	是
AWS::EC2::InternetGateway	是	是
AWS::EC2::LaunchTemplate	是	是
AWS::EC2::NatGateway	是	是
AWS::EC2::NetworkAcl	是	是
AWS::EC2::NetworkInterface	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::EC2::PrefixList	是	是
AWS::EC2::RouteTable	是	是
AWS::EC2::SecurityGroup	是	是
AWS::EC2::SpotFleet	是	是
AWS::EC2::Subnet	是	是
AWS::EC2::SubnetRouteTableAssociation	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::EC2::TrafficMirror过滤器	是	是
AWS::EC2::TrafficMirror会话	是	是
AWS::EC2::TrafficMirror目标	是	是
AWS::EC2::TransitGateway	否	是
AWS::EC2::TransitGateway附件	是	是
AWS::EC2::TransitGatewayConnect	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::EC2::TransitGatewayMulticastDomain	是	是
AWS::EC2::TransitGatewayRouteTable	是	是
AWS::EC2::VPC	是	是
AWS::EC2::VPCEndpoint	是	是
AWS:: EC2:: VPC EndpointService	否	是
AWS:: EC2:: VPC PeeringConnection	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::EC2::VPNConnection	是	是
AWS::EC2::VPNGateway	是	是
AWS::EC2::Volume	是	是
AWS::ECR::Repository	是	是
AWS::ECS::CapacityProvider	是	是
AWS::ECS::Cluster	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::ECS::Service	是	是
AWS::ECS::TaskDefinition	是	是
AWS::ECS::TaskSet	是	是
AWS::EFS::AccessPoint	是	是
AWS::EFS::FileSystem	是	是
AWS::EKS::Addon	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::EKS::Cluster	是	是
AWS::EKS::IdentityProviderConfig	是	是
AWS::EMR::SecurityConfiguration	是	是
AWS::ElasticBeanstalk::Application	是	是
AWS::ElasticBeanstalk::ApplicationVersion	是	是
AWS::ElasticBeanstalk::Environment	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::ElasticLoadBalancing::LoadBalancer	是	是
AWS::ElasticLoadBalancingV2::Listener	是	是
AWS::ElasticLoadBalancingV2::LoadBalancer	是	是
AWS::Elasticsearch::Domain	是	是
AWS::Events::EventBus	是	是
AWS::Events::Rule	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::FIS::ExperimentTemplate	是	是
AWS::Glue::Classifier	是	是
AWS::Glue::Job	是	是
AWS::Glue:: mlTransf	否	是
AWS::GreengrassV2::ComponentVersion	是	是
AWS::GuardDuty::Detector	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::GuardDuty::Filter	是	是
AWS::Guard职责:: IPset	是	是
AWS::GuardDuty::ThreatIntelSet	是	是
AWS::IAM::Group	是	是
AWS::IAM::InstanceProfile	是	否
AWS::IAM::OIDCProvider	是	否

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::IAM::Policy	是	是
AWS::IAM::Role	是	是
AWS::IAM::SAMLProvider	是	否
AWS::IAM::ServerCertificate	是	否
AWS::IAM::User	是	是
AWS::ImageBuilder::ContainerRecipe	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::ImageBuilder::DistributionConfiguration	是	是
AWS::ImageBuilder::ImagePipeline	是	是
AWS::ImageBuilder::ImageRecipe	是	是
AWS::ImageBuilder::InfrastructureConfiguration	是	是
AWS::IoT::AccountAudit配置	是	是
AWS::IoT::Authorizer	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::IoT:: caCertificate	是	是
AWS::IoT::CustomMetric	是	是
AWS::IoT::Dimension	是	是
AWS::IoT::FleetMetric	是	是
AWS::IoT::JobTemplate	是	是
AWS::IoT::MitigationAction	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::IoT::Policy	是	是
AWS::IoT::ProvisioningTemplate	是	是
AWS::IoT::RoleAlias	是	是
AWS::IoT::ScheduledAudit	是	是
AWS::IoT::SecurityProfile	是	是
AWS::IoTEvents::AlarmModel	否	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::IoTEvents::DetectorModel	否	是
AWS::IoTEvents::Input	否	是
AWS::IoTSiteWise::AssetModel	否	是
AWS::IoTSiteWise::Gateway	否	是
AWS::IoTSiteWise::Portal	否	是
AWS::IoTTwinMaker::ComponentType	否	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::IoTTwinMaker::Entity	否	是
AWS::IoTTwinMaker::Workspace	否	是
AWS::KMS::Alias	是	是
AWS::KMS::Key	是	是
AWS::Kinesis::Stream	是	是
AWS::Kinesis::StreamConsumer	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::KinesisAnalyticsV2::Application	是	是
AWS::KinesisFirehose::DeliveryStream	是	是
AWS::Lambda::Function	是	是
AWS::Logs::Destination	是	是
AWS::MSK::BatchScram秘密	是	是
AWS::MSK::Cluster	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::MSK::ClusterPolicy	是	是
AWS::MSK::Configuration	是	是
AWS::MSK::VpcConnection	是	是
AWS::NetworkFirewall::Firewall	是	是
AWS::NetworkFirewall::FirewallPolicy	是	是
AWS::NetworkFirewall::RuleGroup	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::NetworkManager::CustomerGateway协会	否	是
AWS::NetworkManager::Device	否	是
AWS::NetworkManager::GlobalNetwork	否	是
AWS::NetworkManager::Link	否	是
AWS::NetworkManager::LinkAssociation	否	是
AWS::NetworkManager::Site	否	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::NetworkManager::TransitGateway注册	否	是
AWS::OpenSearch::Domain	是	是
AWS::Pinpoint::App	否	是
AWS::Pinpoint::ApplicationSettings	否	是
AWS::Pinpoint::Campaign	否	是
AWS::Pinpoint::EmailChannel	否	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::Pinpoint::EmailTemplate	否	是
AWS::Pinpoint::EventStream	否	是
AWS::Pinpoint::InApp模板	否	是
AWS::Pinpoint::Segment	否	是
AWS::QuickSight::Template	否	是
AWS::RDS::DBCluster	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS:: RDS:: DB ClusterSnapshot	是	是
AWS::RDS::DBInstance	是	是
AWS:: RDS:: DB SecurityGroup	是	是
AWS::RDS::DBSnapshot	是	是
AWS:: RDS:: DB SubnetGroup	是	是
AWS::RDS::EventSubscription	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::RDS::OptionGroup	是	是
AWS::Redshift::Cluster	是	是
AWS::Redshift::ClusterParameter群组	是	是
AWS::Redshift::ClusterSecurity群组	是	是
AWS::Redshift::ClusterSnapshot	是	是
AWS::Redshift::ClusterSubnet群组	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::Redshift::EventSubscription	是	是
AWS::Redshift::ScheduledAction	是	是
AWS::RoboMaker::RobotApplication	否	是
AWS::RoboMaker::RobotApplication版本	否	是
AWS::RoboMaker::SimulationApplication	否	是
AWS::Route53Resolver::FirewallDomain名单	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::Route53Resolver::FirewallRule群组	是	是
AWS::Route53Resolver::FirewallRuleGroupAssociation	是	是
AWS::Route53Resolver::ResolverEndpoint	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig	是	是
AWS::Route53Resolver::ResolverQueryLoggingConfig协会	是	是
AWS::Route53Resolver::ResolverRule	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::Route53Resolver::ResolverRule协会	是	是
AWS::S3::AccessPoint	是	是
AWS::S3::AccountPublicAccessBlock	是	是
AWS::S3::Bucket	是	是
AWS::SES::ConfigurationSet	否	是
AWS::SES::ContactList	否	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::SES::Template	否	是
AWS::SNS::Topic	是	是
AWS::SQS::Queue	是	是
AWS::SSM::AssociationCompliance	是	是
AWS::SSM::Document	是	是
AWS::SSM::FileData	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::SSM::ManagedInstance库存	是	是
AWS::SSM::PatchCompliance	是	是
AWS::SageMaker::Model	否	是
AWS::SageMaker::NotebookInstance	否	是
AWS::SageMaker::NotebookInstanceLifecycleConfig	否	是
AWS::SecretsManager::Secret	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::ServiceCatalog::CloudFormation产品	是	是
AWS::ServiceCatalog::CloudFormationProvisionedProduct	是	是
AWS::ServiceCatalog::Portfolio	是	是
AWS::ServiceDiscovery::HttpNamespace	是	是
AWS::ServiceDiscovery::Instance	是	是
AWS::ServiceDiscovery::Service	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::StepFunctions::StateMachine	是	是
AWS::Transfer::Agreement	是	是
AWS::Transfer::Certificate	是	是
AWS::Transfer::Connector	是	是
AWS::Transfer::Profile	是	是
AWS::Transfer::Workflow	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::WAFRegional::RateBased规则	是	是
AWS::WAFRegional::Rule	是	是
AWS::WAFRegional::RuleGroup	是	是
AWS::WAFRegional::WebACL	是	是
AWS::WAFv2::IPSet	是	是
AWS::WAFv2::ManagedRuleSet	是	是

资源类型	AWS GovCloud（美国西部）	AWS GovCloud（美国东部）
AWS::WAFv2::RegexPatternSet	是	是
AWS::WAFv2::RuleGroup	是	是
AWS::WAFv2::WebACL	是	是
AWS::WorkSpaces::Workspace	否	是

录制 AWS 资源

AWS Config 持续检测何时创建、更改或删除支持的资源类型。 AWS Config 将这些事件记录为配置项目 (CI)。您可以自定义 AWS Config ，以使其记录所有受支持类型的资源的配置更改，或仅记录与您相关的资源类型的配置更改。有关 AWS Config 可以记录的支持资源类型的列表，请参阅支持的资源类型。

注意事项

AWS Config 评估次数多

与随后的几个月相比，您可能会注意到，在使用 AWS Config 记录的最初一个月中，您的账户活动有所增加。在初始引导过程中， AWS Config 会对您账户中您选择 AWS Config 要记录的所有资源进行评估。

如果您运行的是临时工作负载，则可能会看到活动增加， AWS Config 因为它记录了与创建和删除这些临时资源相关的配置更改。临时工作负载 是临时使用在需要时加载和运行的计算资源。示例包括 Amazon Elastic Compute Cloud (Amazon EC2) 竞价型实例、Amazon EMR 任务和 AWS Auto Scaling。如果要避免因运行临时工作负载而增加的活动，则可以设置配置记录器以将这些资源类型排除在记录之外，或者在 AWS Config 关闭的情况下在单独的帐户中运行这些类型的工作负载，以避免增加配置记录和规则评估。

区域可用性

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

区域性资源和全局资源有什么区别？

区域性资源

区域性资源与某个区域相关联，且仅可在该区域中使用。你在指定的区域中创建它们 AWS 区域，然后它们就存在于该区域中。要查看这些资源或与之交互，您必须将操作定向到该区域。例如，要使用创建 Amazon EC2 实例 AWS 区域，请选择要在中创建实例的。 AWS Management Console 如果您使用 AWS Command Line Interface (AWS CLI) 创建实例，则需要包含`--region`参数。每个 AWS SDK 都有自己的等效机制来指定操作使用的区域。

使用区域性资源有几个原因。原因之一是要确保资源以及您用来访问资源的服务终端节点尽可能靠近客户。这通过最大限度减少延迟来提高性能。另一个原因是为了提供隔离边界。这样，您可以在多个区域中创建独立的资源副本，以分配负载并提高可扩展性。同时，它可以将资源相互隔离，以提高可用性。

如果您在控制台或 AWS CLI 命令 AWS 区域 中指定其他内容，则无法再查看在前一个区域中可以看到的资源或与之交互。

当您查看区域资源的 Amazon 资源名称（ARN）时，包含该资源的区域被指定为 ARN 中的第四个字段。例如，Amazon EC2 实例是一种区域性资源。以下是面向 `us-east-1` 区域中 Amazon EC2 实例的 ARN 示例。

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

全局资源

有些 AWS 服务资源是全球资源，这意味着您可以从任何地方使用该资源。您无需在全局服务的控制台中指定 AWS 区域 。要访问全局资源，在使用服务 AWS CLI 和 AWS SDK 操作时无需指定`--region`参数。

全局资源支持在关键时刻某一特定资源只能存在一个实例的情况。在这些情况下，在不同区域的副本之间进行复制或同步是不够的。为了确保资源使用者能即时看到任何变化，访问单一全局终端节点被认为是可以接受的，虽然可能会增加延迟。

例如，Amazon Aurora 全局集群 (`AWS::RDS::GlobalCluster`) 是全局资源，因此与区域无关。这意味着您无需依赖区域终端节点即可创建全局集群。好处是，虽然 Amazon Relational Database Service (Amazon RDS) 本身是按区域组织的，但全局集群所源自的特定区域不会影响全局集群。它以单个连续的全局集群形式出现在所有区域。

全局资源的 Amazon 资源名称 (ARN) 不包括区域。第四个字段为空，例如以下全局集群的 ARN 示例。

```
arn:aws:rds::123456789012:global-cluster:test-global-cluster
```

> **Important**
>
> 2022 年 2 月 AWS Config 之后加入的全球资源类型将仅记录在服务主区域（商业分区）和分区 AWS GovCloud （美国西部）中。 GovCloud 您只能在其所在地区和（美国西部）查看这些新的全球资源类型的配置项目 AWS GovCloud (CI)。
> 2022 年 2 月之前载入的全局资源类型（`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role` 和 `AWS::IAM::User`）保持不变。您可以在 2022 年 2 月之前支持的所有区域启用这些全球 IAM 资源的记录。 AWS Config 2022 年 2 月 AWS Config 之后，这些全球 IAM 资源无法记录在支持的区域中。

全局资源类型 | IAM 资源

以下 IAM 资源类型是全局资源：IAM 用户、组、角色和客户管理型策略。这些资源类型可以在 2022 AWS Config 年 2 月之前可用的区域 AWS Config 中进行记录。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

为防止重复的配置项目 (CI)，您应考虑仅在其中一个支持的区域中记录一次全球 IAM 资源类型。这还可以帮助您避免不必要的评估和 API 节流。

全局资源类型 | 仅限主区域

以下服务的全球资源仅按 AWS Config 全球资源类型的主区域记录：亚马逊弹性容器注册表公共区域、 AWS Global Accelerator Amazon Route 53 CloudFront、Amazon 和 AWS WAF。对于这些全球资源，可以在多个 AWS 区域中使用同一资源类型的实例，但是配置项目 (CI) 仅记录在商业分区的本地区域或分区的 AWS GovCloud （美国西部）中 AWS GovCloud (US) 。

全局资源类型的主区域

AWS 服务	资源类型值	主区域
Amazon Elastic Container Registry Public	`AWS::ECR::PublicRepository`	美国东部（弗吉尼亚州北部）区域
AWS Global Accelerator	`AWS::GlobalAccelerator::Listener`	美国西部（俄勒冈州）区域
	`AWS::GlobalAccelerator::EndpointGroup`	美国西部（俄勒冈州）区域
	`AWS::GlobalAccelerator::Accelerator`	美国西部（俄勒冈州）区域
Amazon Route 53	`AWS::Route53::HostedZone`	美国东部（弗吉尼亚州北部）区域
	`AWS::Route53::HealthCheck`	美国东部（弗吉尼亚州北部）区域
Amazon CloudFront	`AWS::CloudFront::Distribution`	美国东部（弗吉尼亚州北部）区域
AWS WAF	`AWS::WAFv2::WebACL`	美国东部（弗吉尼亚州北部）区域

全局资源类型 | Aurora 全局集群

`AWS::RDS::GlobalCluster`是一种全球资源，记录在启用配置记录器的所有支持 AWS Config 区域中。这种全局资源类型的独特之处在于，如果您在一个区域启用此资源的记录，则 AWS Config 将在所有已启用的区域中记录该资源类型的配置项目 (CI)。

如果您不想`AWS::RDS::GlobalCluster`在所有已启用的区域进行录制，请在 AWS Config 控制台使用以下录制策略之一：

- 使用可自定义的替代项录制所有资源类型，选择 GlobalCluster “AWS RDS”，然后选择替代 “从录制中排除”
- 记录特定的资源类型。

如果您不想在所有已启用的区域中记录 `AWS::RDS::GlobalCluster`，请使用以下适用于 API/CLI 的记录策略之一：

- 记录所有当前和未来的资源类型，排除项除外 (`EXCLUSION_BY_RESOURCE_TYPES`)
- 记录特定的资源类型 (`INCLUSION_BY_RESOURCE_TYPES`)。

在 AWS Config 控制台中录制资源

记录资源（控制台）

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

选择资源

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在左侧导航窗格上，选择设置，然后选择编辑。有关支持的区域列表，请参见 Amazon Web Services 一般参考 中的 AWS Config 端点和配额。
3. 在记录方法部分，选择记录策略。您可以指定 AWS Config 要记录的 AWS 资源。

   All resource types with customizable overrides

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

   - 默认设置

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

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

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

- 覆盖设置

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

> **Note**
>
> 全局资源类型 | Aurora 全局集群最初包含在记录范围内
> `AWS::RDS::GlobalCluster`资源类型将在启用配置记录器的所有支持 AWS Config 区域中进行记录。
> 如果您不想在所有已启用的区域中记录 `AWS::RDS::GlobalCluster`，请选择“AWS RDS GlobalCluster”，然后选择“从记录中排除”覆盖方法。

> **Note**
>
> 全局资源类型 | IAM 资源类型最初不包含在记录范围内
> 为了帮您降低成本，“所有全局记录的 IAM 资源类型”最初都不包含在记录范围内。此捆绑包包括 IAM 用户、组、角色和客户管理型策略。选择移除以删除覆盖，并将这些资源包含在您的记录范围内。
> 美国东部（弗吉尼亚州北部）除外。全局 IAM 资源类型最初包含在美国东部（弗吉尼亚州北部）区域内，因为该区域是全局 IAM 资源类型的主区域。
> 此外，全球 IAM 资源类型
> （`AWS::IAM::User``AWS::IAM::Group`、`AWS::IAM::Role`、
> 和`AWS::IAM::Policy`）不能记录在 2022 年 2 月 AWS Config 之后支持的区域中。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

> **Note**
>
> 限制
>
> 您可以添加最多 100 项频率覆盖和 600 项排除覆盖。
>
> 以下资源类型不支持每日记录：
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

Specific resource types

设置 AWS Config 为仅记录您指定的资源类型的配置更改。

- 特定的资源类型

  选择要记录的资源类型及其频率。有关更多信息，请参阅记录频率。

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

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

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

> **Note**
>
> 区域可用性
>
> 在指定 AWS Config 要跟踪的资源类型之前，请检查按区域划分的资源覆盖率，以查看您设置的 AWS 区域是否支持该资源类型 AWS Config。如果至少有一个区域支持某种

资源类型，则即使您设置的区域不支持指定的资源类型 AWS Config，您也可以在支持的所有 AWS 区域中启用该资源类型的记录 AWS Config。 AWS Config

> **Note**
>
> 限制
>
> 如果所有资源类型的频率都相同，则没有限制。如果至少将一种资源类型设置为“持续”，则最多可以添加 100 种频率为“每日”的资源类型。
>
> 以下资源类型不支持“每日”频率：
>
> - `AWS::Config::ResourceCompliance`
> - `AWS::Config::ConformancePackCompliance`
> - `AWS::Config::ConfigurationRecorder`

4. 选择 保存 以保存您的更改。

使用 AWS CLI 录制资源

录制资源 (AWS CLI)

您可以使用 C AWS LI 来选择 AWS Config 要记录的资源类型。为此，您可以创建一个配置记录器，以记录您在记录组中指定的资源类型。在记录组中，您可以指定是要记录所有受支持的资源类型，还是包括或排除特定类型的资源。

Record all current and future supported resource types

设置 AWS Config 为记录该区域所有当前和 future 支持的资源类型的配置更改。有关更多信息，请参阅支持的资源类型。

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

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

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

> **Note**
>
> 录制组和配置记录器
> `--recording-group` 字段指定要记录哪些资源类型。
> 该`--configuration-recorder`字段指定`name`和`roleArn`以及配置记录器的默认录制频率 (`recordingMode`)。您也可以使用此字段来覆盖特定资源类型的记录频率。

i. `put-configuration-recorder` 使用 `--recording-group` 参数的以下字段：

- `allSupported=true`— AWS Config 记录所有支持的资源类型的配置更改，不包括全球 IAM 资源类型。 AWS Config 添加对新资源类型的支持后，会自动 AWS Config 开始记录该类型的资源。
- `includeGlobalResourceTypes=true` – 此选项是一个捆绑包，仅适用于全局 IAM 资源类型：IAM 用户、组、角色和客户管理型策略。这些全球 IAM 资源类型只能在 2022 年 2 月之前可用的 AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后，您无法在支持的区域中记录全球 IAM 资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

> **Important**
>
> Aurora 全局集群记录在所有已启用的区域中
> `AWS::RDS::GlobalCluster`资源类型将记录在启用配置记录器的所有支持 AWS Config 区域，即使`includeGlobalResourceTypes`未设置为`true`。`includeGlobalResourceTypes` 选项是一个捆绑包，仅适用于 IAM 用户、组、角色和客户管理型策略。
> 如果您不想在所有已启用的区域中记录 `AWS::RDS::GlobalCluster`，请使用以下记录策略之一：
>
> 1. 记录所有当前和未来的资源类型，您指定的类型除外 (`EXCLUSION_BY_RESOURCE_TYPES`)，或者
> 2. 记录特定的资源类型 (`INCLUSION_BY_RESOURCE_TYPES`)。
>
> 有关更多信息，请参阅选择所记录的资源 | 区域性资源和全局资源。

> **Important**
>
> 包含GlobalResourceTypes 和排除记录策略
> 该includeGlobalResourceTypes字段
> 对EXCLUSION_BY_RESOURCE_TYPES录制策略没有影响。这意味着，当设置为exclusionByResourceTypes时includeGlobalResourceTypes，全球 IAM 资源类型（IAM 用户、群组、角色和客户托管策略）不会自动添加为排除项。false
> 该includeGlobalResourceTypes字段只能用于修改该AllSupported字段，因为该字段的默认设置是记录除全球 IAM 资源类型之AllSupported外的所有受支持资源类型的配置更改。要在设置为时AllSupported包括全局 IAM 资源类型true，请确保将设置includeGlobalResourceTypes为true。
> 要排除EXCLUSION_BY_RESOURCE_TYPES录制策略的全球 IAM 资源类型，您需要手动将其添加到的resourceTypes字段中exclusionByResourceTypes。

> **Note**
>
> 必填字段和可选字段
> 将 includeGlobalResourceTypes 设置为 true 之前，请先将 allSupported 字段设置为 true。
> 也可以将 RecordingStrategy 的 useOnly 字段设置为 ALL_SUPPORTED_RESOURCE_TYPES。

> **Note**
>
> 覆盖字段
> 如果您在的字段中设置includeGlobalResourceTypes为false但列出了全局 IAM 资源类型 RecordingGroup，则无论您是否 AWS Config 将该resourceTypes字段设置为 false，仍会记录这些指定资源类型的配置更改。includeGlobalResourceTypes

> 如果您不想记录对全局 IAM 资源类型（IAM 用户、组、角色和客户管理型策略）的配置更改，那么除了将 `includeGlobalResourceTypes` 字段设置为 false 之外，切勿在 `resourceTypes` 字段中列出这些内容。

`recordingGroup.json` 文件指定 AWS Config 将记录的资源类型。

```
{
    "allSupported": true,
    "recordingStrategy": {
        "useOnly": "ALL_SUPPORTED_RESOURCE_TYPES"
    },
    "includeGlobalResourceTypes": true
}
```

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

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

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

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

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

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

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

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

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

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

以下为响应示例。

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

Record all current and future supported resources types excluding the types you specify

设置 AWS Config 为记录所有当前和 future 支持的资源类型的配置更改，包括全局资源类型，但您指定要从记录中排除的资源类型除外。如果您选择停止记录某一资源类型，则已记录的配置项将保持不变。有关更多信息，请参阅支持的资源类型。

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

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

> **Note**
>
> 录制组和配置记录器
> `--recording-group` 字段指定要记录哪些资源类型。
> 该`--configuration-recorder`字段指定name和roleArn以及配置记录器的默认录制频率 (recordingMode)。您也可以使用此字段来覆盖特定资源类型的记录频率。

1. 使用 `put-configuration-recorder` 命令，并传递 `exclusionByResourceTypes` 的 `resourceTypes` 字段中指定的一个或多个要排除的资源类型，如以下示例所示。
   i. `recordingGroup.json` 文件指定 AWS Config 将记录的资源类型。

```
{
    "allSupported": false,
    "exclusionByResourceTypes": {
        "resourceTypes": [
            "AWS::Redshift::ClusterSnapshot",
            "AWS::RDS::DBClusterSnapshot",
            "AWS::CloudFront::StreamingDistribution"
        ]
    },
   "includeGlobalResourceTypes": false,
   "recordingStrategy": {
       "useOnly": "EXCLUSION_BY_RESOURCE_TYPES"
    },

}
```

在指定要从记录中排除的资源类型之前，请执行以下操作：

- 必须将 `--recording-group` 参数的 `allSupported` 和 `includeGlobalResourceTypes` 字段设置为 `false`，或省略它们。
- 必须将 `RecordingStrategy` 的 `useOnly` 字段设置为 `EXCLUSION_BY_RESOURCE_TYPES`。

> **Note**
>
> 覆盖字段
>
> 如果您对记录策略选择 `EXCLUSION_BY_RESOURCE_TYPES`，则 `exclusionByResourceTypes` 字段将覆盖请求中的其他属性。
>
> 例如，即使您将 `includeGlobalResourceTypes` 设置为 false，全局 IAM 资源类型仍将自动记录在此选项中，除非这些资源类型在 `exclusionByResourceTypes` 的 `resourceTypes` 字段中被明确列为排除项。

> **Note**
>
> 全局资源类型和资源排除记录策略
>
> 默认情况下，如果您选择`EXCLUSION_BY_RESOURCE_TYPES`录制策略，则在设置配置记录器的区域中 AWS Config 添加对新资源类型（包括全局资源类型）的支持时，会自动 AWS Config 开始记录该类型的资源。
>
> 除非特别列为排除项，否则`AWS::RDS::GlobalCluster`将在启用配置记录器的所有受支持 AWS Config 区域中自动记录。
>
> IAM 用户、群组、角色和客户托管策略将记录在您设置配置记录器的区域（如果该区域在 2022 年 2 月之前可用）。 AWS Config 2022 年 2 月 AWS Config 之后，您无法在支持的区域中记录全球 IAM 资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

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

- `name`— 配置记录器的名称。 AWS Config 创建配置记录器时会自动分配 “默认” 的名称。
- `roleARN`— 由配置记录器担任 AWS Config 和使用的 IAM 角色的 Amazon 资源名称 (ARN)。
- `recordingMode`— 指定用于记录配置更改的 AWS Config 默认录制频率。 AWS Config 支持连续录制和每日录制。连续记录可让您在每次发生配置更改时连续记录更改。使用每日记

录，您将收到代表过去 24 小时内资源的最新状态的配置项 (CI)，前提是它与之前记录的 CI 不同。

- `recordingFrequency`— AWS Config 用于记录配置更改的默认录制频率。

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

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

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

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

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

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

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

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

以下为响应示例。

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
                "exclusionByResourceTypes": {
                    "resourceTypes": [
                        "AWS::Redshift::ClusterSnapshot",
                        "AWS::RDS::DBClusterSnapshot",
                        "AWS::CloudFront::StreamingDistribution"
                    ]
                },
                "includeGlobalResourceTypes": false,
```

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

Record specific resource types

设置 AWS Config 为仅记录您指定的资源类型的配置更改。如果您选择停止记录某一资源类型，则已记录的配置项将保持不变。

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

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

> **Note**
>
> 录制组和配置记录器
> `--recording-group` 字段指定要记录哪些资源类型。
> 该`--configuration-recorder`字段指定name和roleArn以及配置记录器的默认录制频率 (`recordingMode`)。您也可以使用此字段来覆盖特定资源类型的记录频率。

1. 使用 put-configuration-recorder 命令，并传递 recordingGroup 的 resourceTypes 字段中指定的一个或多个资源类型，如以下示例所示。

   i. recordingGroup.json 文件指定 AWS Config 将记录的资源类型。

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

> **Note**
>
> 必填字段和可选字段
>
> 在指定要包含在录制中的资源类型之前，必须将 allSupported 和 includeGlobalResourceTypes 字段设置为 false，或省略它们。当您在 --recording-group 的 resourceTypes 字段中列出资源类型时，recordingStrategy 字段是可选的。

> **Note**
>
> 区域可用性
>
> 在指定 AWS Config 要跟踪的资源类型之前，请检查按区域划分的资源覆盖率，以查看您设置的 AWS 区域是否支持该资源类型 AWS Config。如果至少有一个区域支持某

种资源类型，则即使您设置的区域不支持指定的资源类型 AWS Config，您也可以在支持的所有 AWS 区域中启用该资源类型的记录 AWS Config。 AWS Config

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

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

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

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

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

> **Note**
>
> 限制

以下资源类型不支持每日记录：

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

对于记录所有当前和未来支持的资源类型 (ALL_SUPPORTED_RESOURCE_TYPES) 记录策略，这些资源类型将设置为“连续记录”。

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

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

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

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

以下为响应示例。

```
{
    "ConfigurationRecorders": [
        {
            "name": "default",
            "recordingGroup": {
                "allSupported": false,
```

```
                "exclusionByResourceTypes": {
                    "resourceTypes": []
                },
                "includeGlobalResourceTypes": false
                "recordingStrategy": {
                    "useOnly": "INCLUSION_BY_RESOURCE_TYPES"
                },
                "resourceTypes": [
                    "AWS::EC2::EIP",
                    "AWS::EC2::Instance",
                    "AWS::EC2::NetworkAcl",
                    "AWS::EC2::SecurityGroup",
                    "AWS::CloudTrail::Trail",
                    "AWS::EC2::Volume",
                    "AWS::EC2::VPC",
                    "AWS::IAM::User",
                    "AWS::IAM::Policy"
                ]
            },
            "recordingMode": {
                "recordingFrequency": CONTINUOUS or DAILY,
                "recordingModeOverrides": [
                 {
                     "description": "Description you provide for the override,
                     "recordingFrequency": CONTINUOUS or DAILY,
                     "resourceTypes": [ Comma-separated list of resource types to
 include in the override]
                }
              ]
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-role"
        }
    ]
}
```

记录频率

AWS Config 支持连续录制和每日录制。连续记录可让您在每次发生配置更改时连续记录更改。使用每日记录，您将收到代表过去 24 小时内资源的最新状态的配置项 (CI)，前提是它与之前记录的 CI 不同。

连续记录

连续记录的部分优势包括：

- 实时监控：连续记录可以立即检测未经授权的更改或意外改动，从而提升您的安全性和合规性。
- 详细分析：连续记录可以让您在资源配置更改发生时对其进行深入分析，确定当下的模式和趋势。

每日记录

每日记录的部分优势包括：

- 最大限度减少干扰：每日记录可以为您提供更易于管理的信息流，从而减少通知频率和警报疲劳。
- 成本效益：每日记录可以让您灵活地以较低的频率记录资源更改，从而降低与记录的配置更改数量相关的成本。

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

停止记录资源

您可以随时停止 AWS Config 记录某类资源。 AWS Config 停止记录资源后，它会保留先前捕获的配置信息，您可以继续访问这些信息。

未记录的资源

如果未记录资源，则仅 AWS Config 捕获该资源的创建和删除情况，不记录其他详细信息，而不会向您收取任何费用。创建或删除未录制的资源时， AWS Config 会发送通知，并在资源详细信息页面上显示该事件。在未记录资源的详细信息页面上，大多数配置详细信息的值为 null，且不会显示关于关系和配置更改的信息。

> **Note**
>
> 仅当资源被选为或以前被选为要在配置记录器中记录的资源时，`AWS::IAM::User`、`AWS::IAM::Policy`、 `AWS::IAM::Group`、`AWS::IAM::Role` 资源类型才会捕获创建 (`ResourceNotRecorded`) 和删除 (`ResourceDeletedNotRecorded`) 状态。

> **Note**
>
> `ResourceNotRecorded`和的配置项目 (CI) `ResourceDeletedNotRecorded` 不遵循资源类型的典型录制时间。这些资源类型仅在配置记录器的定期基准化过程中进行记录，与其他资源类型相比，该过程的频率较低。

由于缺少未记录资源的数据， AWS Config 提供已记录资源的关系信息不受限制。如果某个已记录资源与未记录资源相关联，则已记录资源的详细信息页面会提供相应的关系信息。

AWS Config 规则和全局资源类型

2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后，这些全球 IAM 资源类型无法记录在支持的区域中。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。

2022 年 2 月前上线的全球资源合规报告最佳实践

为避免不必要的评估，您只应将包含这些全球资源的 AWS Config 规则和一致性包部署到支持的区域之一。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。这适用于 AWS Config 规则、组织 AWS Config 规则以及由其他 AWS 服务（例如 AWS Security Hub 和）创建的规则 AWS Control Tower。

如果您没有记录 2022 年 2 月之前载入的全局资源类型，建议您不要启用以下定期规则，以避免不必要的评估：

- access-keys-rotated
- account-part-of-organizations
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam-user-mfa-enabled

- iam-user-unused-credentials-check
- mfa-enabled-for-iam-console-access
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled

2022 年 2 月后上线的全球资源合规报告最佳实践

2022 年 2 月之后加入 AWS Config 录制的全球资源类型将仅记录在服务主区域（商业分区）和分区 AWS GovCloud （美国西部）中。 AWS GovCloud (US) 您应该将这些全球资源范围内的 AWS Config 规则和一致性包部署到资源类型的起始区域。有关更多信息，请参阅全球资源类型的主区域。

记录第三方资源的配置

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

> **Note**
>
> 如果您已配置 AWS Config 为记录所有资源类型，则通过 AWS CloudFormation 其管理（创建、更新或删除）的第三方资源将自动 AWS Config 作为配置项目进行跟踪。

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

主题

- 步骤 1：设置开发环境
- 步骤 2：资源建模
- 步骤 3：生成构件
- 步骤 4：注册资源
- 步骤 5：发布资源配置
- 使用记录和删除第三方资源的配置状态 AWS CLI
- 使用 API 管理第三方资源类型的配置状态

步骤 1：设置开发环境

安装和配置 AWS CloudFormation AWS CLI。 AWS CLI 允许您对自定义资源进行建模和注册。有关更多信息，请参阅自定义资源和什么是 CloudFormation 命令行界面？ 。

步骤 2：资源建模

创建符合资源类型配置的资源提供程序架构，并验证该架构。

1. 使用 `init` 命令创建资源提供程序项目并生成所需的文件。

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

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

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

3. 输入资源的包名称。

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

> **Note**
>
> 为了确保正确解析任何项目依赖关系，您可以将生成的项目导入支持 Maven 的 IDE 中。例如，如果您使用的是 IntelliJ IDEA，则需要执行以下操作：
>
> - 从文件菜单中，选择新建，然后选择现有源中的项目。
> - 导航到项目目录。
> - 在导入项目对话框中，选择从外部模型导入项目，然后选择 Maven。
> - 选择下一步，并接受所有默认设置以完成项目导入。

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

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

5. 验证架构。

```
$ cfn validate
```

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

```
$ cfn generate
```

> **Note**
>
> 使用 Maven 时，作为编译过程的一部分，`generate` 命令会在编译代码之前自动运行。因此，您的更改永远不会与生成的代码不同步。
> 请注意， CloudFormation CLI 必须位于 Maven/系统可以找到的位置。有关更多信息，请参阅设置用于开发扩展的环境。

有关整个过程的更多信息，请参阅对资源提供程序进行建模以在 AWS CloudFormation中使用。

步骤 3：生成构件

运行以下命令以生成 `cfn submit` 的构件。

```
$ mvn package
```

步骤 4：注册资源

AWS Config 不需要资源提供者处理程序对您的资源执行配置跟踪。运行以下命令来注册您的资源。

```
$ cfn submit
```

有关更多信息，请参阅注册资源提供者以在 AWS CloudFormation 模板中使用。

步骤 5：发布资源配置

确定:: 测试 MyCustomNamespace:: 的配置。WordPress

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

从中确定架构版本 ID AWS CloudFormation `DescribeType`。

AWS Config 看看这个资源配置是否被接受。要评估合规性，您可以使用此资源编写 AWS Config 规则。有关更多信息，请参阅使用 AWS CLI 记录和删除第三方资源的配置状态。

可选：要自动记录配置，请实施定期配置收集器或基于更改的配置收集器。

使用记录和删除第三方资源的配置状态 AWS CLI

AWS CLI 是一款用于管理您的 AWS 服务的统一工具。只需下载和配置一个工具，您就可以从命令行控制多项 AWS 服务，并使用脚本自动执行这些服务。有关 AWS CLI 和 AWS CLI 工具安装说明的更多信息，请参阅《AWS Command Line Interface 用户指南》中的以下内容。

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

如有必要，`aws configure`请输入配置 AWS CLI 为使用有 AWS Config 聚合器的 AWS 区域。

主题

- 记录配置项
- 使用 AWS Config API 读取配置项
- 删除第三方资源

记录配置项

使用以下过程记录第三方资源或自定义资源类型的配置项：

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

1. 打开命令提示符或终端窗口。
2. 输入以下 命令：

```
aws configservice put-resource-config --resource-type
 MyCustomNamespace::Testing::WordPress --resource-id resource-001 --schema-version-
id 00000001 --configuration  '{
  "Id": "resource-001",
  "Name": "My example custom resource.",
  "PublicAccess": false
}'
```

> **Note**
>
> 按照类型架构中的定义，`writeOnlyProperties`将在记录之前从配置中删除 AWS Config。这意味着，当通过读取 API 获取配置时，这些值将不存在。有关 `writeOnlyProperties` 的更多信息，请参阅资源类型架构。

使用 AWS Config API 读取配置项

1. 打开命令提示符或终端窗口。
2. 输入以下 命令：

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

3. 按 Enter。

   您应该可以看到类似于如下所示的输出内容：

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

4. 输入以下 命令：

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

5. 按 Enter。

   您应该可以看到类似于如下所示的输出内容：

```
{
    "unprocessedResourceKeys": [],
    "baseConfigurationItems": [
```

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

删除第三方资源

您可以记录要删除的第三方资源或自定义资源类型的配置状态。

- 输入以下 命令：

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

  如果成功，则命令会执行，而没有附加输出。

使用 API 管理第三方资源类型的配置状态

您可以使用 C PutResourceon fig 和 Config API 管理第三方资源或自定义资源类型的DeleteResource 配置状态。有关更多信息，请参阅 API 参考。

- PutResourceConfig
- DeleteResourceConfig

记录托管实例的软件配置

您可以使用 AWS Config 记录 Amazon EC2 实例和本地服务器上的软件库存变化。这样您就可以了解到软件配置的变更历史。例如，在托管 Windows 实例上安装新的 Windows 更新时，会 AWS Config 记录更改，然后将更改发送到您的交付渠道，以便您收到有关更改的通知。借 AWS Config助，您可以查看托管实例何时安装 Windows 更新的历史记录以及它们如何随着时间的推移而发生变化。

您必须完成以下步骤来记录软件配置变更：

- 在 AWS Config中打开对托管实例清单资源类型的记录。
- 将 EC2 和本地服务器配置为 AWS Systems Manager中的托管实例。托管实例是一台已配置为与 Systems Manager 一起使用的计算机。
- 使用 Systems Manager 清单功能启动收集托管实例的软件清单。

> **Note**
>
> Systems Manager 现在支持为非托管实例创建配置项
> 非托管实例的配置项将拥有具有 `Key: “InstanceStatus”` 和 `Value: “Unmanaged”` 的补充配置。
> 非托管实例的配置项不会接收其他更新
> 要接收其他更新，配置项必须是托管实例。

您还可以使用 AWS Config 规则来监控软件配置更改，并通知更改是否符合您的规则。例如，如果您创建了一条规则来检查您的托管实例是否有指定的应用程序，而某个实例没有安装该应用程序，则会将该实例 AWS Config 标记为不符合您的规则。有关 AWS Config 托管规则的列表，请参阅AWS Config 托管规则列表。

在 AWS Config中启用软件配置变更的记录：

1. 在 AWS Config中记录所有支持的资源类型，或选择性地记录托管实例清单资源类型。有关更多信息，请参阅 录制 AWS 资源。
2. 使用包含 Amaz onSSM ManagedInstanceCore 托管策略的 Systems Manager 实例配置文件启动一个 Amaz on EC2 实例。此 AWS 托管策略使实例能够使用 Systems Manager 服务核心功能。

   有关可以添加到 Systems Manager 的实例配置文件中的其他策略的信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

> **Important**
>
> SSM 代理是必须安装在托管实例上的 Amazon 软件，以便在云中与 Systems Manager 进行通信。如果您的 EC2 实例是从 AMI 为以下一种操作系统创建的，则会预装代理：
>
> - 2016 年 11 月或之后发布的 Windows Server 2003-2012 R2 AMI
> - Windows Server 2016 和 2019
> - Amazon Linux
> - Amazon Linux 2
> - Ubuntu Server 16.04
> - Ubuntu Server 18.04
>
> 在不是从预装代理的 AMI 上创建的 EC2 实例上，必须手动安装代理。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的以下主题：
>
> - 在适用于 Windows Server 的 EC2 实例上安装和配置 SSM 代理
> - 在适用于 Linux 的 EC2 实例上安装和配置 SSM 代理

3. 按照《AWS Systems Manager 用户指南》中的配置清单收集中所述启动清单收集。Linux 和 Windows 实例的步骤相同。

   AWS Config 可以记录以下清单类型的配置更改：

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

   > **Note**
   >
   > AWS Config 目前不支持记录自定义库存类型。

清单收集是众多 Systems Manager 功能之一，这些功能分为运营管理、操作和更改、实例和节点以及共享资源等类别。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的什么是 Systems Manager？和 Systems Manager 功能。

查看 资源配置和历史记录

您可以查看账户中记录的所有 AWS Config 资源、资源在指定时间段内发生的配置更改以及所选资源与所有相关资源的关系。您还可以查看时间轴中 AWS Config 规则 显示的资源的合规性状态变化。

主题

- 查找由以下人员发现的资源 AWS Config
- 查看合规信息和评估结果
- 查看配置和合规性历史记录

查找由以下人员发现的资源 AWS Config

您可以使用 AWS Config 控制台 AWS CLI、和 AWS Config API 来查找 AWS Config 已清点或发现的资源，包括已删除的资源和当前 AWS Config 未记录的资源。 AWS Config 仅发现支持的资源类型。有关更多信息，请参阅 支持的资源类型。

查找资源（控制台）

您可以使用资源类型或标签信息在 AWS Config 控制台中查找资源。

查找资源（控制台）

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在资源清单页面上，为您要查找的资源指定搜索选项：
   - 资源类别-选择所有资源类别或将结果范围缩小到仅 AWS 资源。
   - 资源类型 – 选择所有资源类型或选择要筛选的资源。
   - 合规性 – 选择按任何合规性状态、合规或不合规进行筛选。
3. AWS Config 列出了与您的搜索选项相匹配的资源。您可以查看有关资源的以下信息：
   - 资源标识符 – 资源标识符可以是资源 ID，也可以是资源名称（如果适用）。选择资源标识符链接以查看资源详细信息页面。

- 资源类型 – 列出资源的类型。
- 合规性-根据您的规则进行 AWS Config 评估的资源的状态。

  有关更多信息，请参阅 查看配置和合规性历史记录。

查找资源 (AWS CLI)

您可以使用列 AWS CLI 出 AWS Config 已发现的资源。

查找资源 (AWS CLI)

使用 AWS Config service **`list-discovered-resources`** 命令：

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

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

查找资源 (API)

您可以指定资源类型，然后 AWS Config 返回该类型资源的资源标识符列表。有关更多信息，请参阅 AWS Config API 参考ResourceIdentifier中的。

要查找资源 (API)

使用 ListDiscoveredResources 操作。

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

查看合规信息和评估结果

> **Important**
>
> 要准确报告合规性状态，必须记录 `AWS::Config::ResourceCompliance` 资源类型。有关更多信息，请参阅重新编码 AWS 资源。

您可以使用 AWS Config 控制台或 AWS 软件开发工具包查看您的规则和资源的合规性信息以及评估结果。

目录

- 查看合规性（控制台）
- 查看合规性 (AWS SDK)

查看合规性（控制台）

查看合规性（控制台）

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 在导航窗格中，选择资源。在“资源”清单页面上，您可以按资源类别、资源类型和合规性状态进行筛选。根据需要选择包括已删除的资源。该表显示了资源类型的资源标识符和该资源的资源合规性状态。资源标识符可以是资源 ID，也可以是资源名称。
4. 从资源标识符列中选择资源。
5. 选择资源时间表按钮。您可以按配置事件、合规性事件或 CloudTrail 事件进行筛选。

> **Note**
>
> 或者，在“资源”清单页面上，您可以直接选择资源名称。要从资源详细信息页面访问资源时间表，请选择资源时间表按钮。

此外，您还可以在 Resource inventory 页面查找您的资源，以查看其合规性。有关更多信息，请参阅查找由以下人员发现的资源 AWS Config。

查看合规性 (AWS SDK)

获取 AWS Config 规则的合规性信息

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

CLI

AWS CLI

获取您的 AWS Config 规则的合规性信息

以下命令返回一个或多个 AWS 资源违反的每个 AWS Config 规则的合规性信息：

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

在输出中，每个`CappedCount`属性的值都表示有多少资源不符合相关规则。例如，以下输出表明 3 个资源不符合名为的规则`InstanceTypesAreT2micro`。

输出：

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
```

```
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

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

PowerShell

用于 PowerShell

示例 1：此示例检索规则的合规性详细信息，该规则当前没有评估结果 ebs-optimized-instance，因此它返回 INSUFKIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

输出：

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

示例 2：此示例返回规则 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK 的不合规资源数量。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       2
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考DescribeComplianceByConfigRule中的。

获取 AWS 资源的合规性信息

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

CLI

AWS CLI

获取 AWS 资源的合规性信息

以下命令返回由 AWS Config 记录且违反一条或多条规则的每个 EC2 实例的合规性信息：

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

在输出中，每个`CappedCount`属性的值都表示该资源违反了多少规则。例如，以下输出表明该实例`i-1a2b3c4d`违反了 2 条规则。

输出：

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
```

```
            }
        }
    ]
}
```

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

PowerShell

用于 PowerShell

示例 1：此示例检查**AWS::SSM::ManagedInstanceInventory**资源类型的 “合规” 合规性类型。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

输出：

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考DescribeComplianceByResource中的。

获取 AWS Config 规则的合规性摘要

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

CLI

AWS CLI

获取您的 AWS Config 规则的合规性摘要

以下命令返回合规规则的数量和不合规的规则数量：

```
aws configservice get-compliance-summary-by-config-rule
```

在输出中，每个CappedCount属性的值表示有多少规则合规或不合规。

输出：

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

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

PowerShell

用于 PowerShell

示例 1：此示例返回不合规的 Config 规则的数量。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       9
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考GetComplianceSummaryByConfigRule中的。

获取 AWS 资源的合规性摘要

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

CLI

AWS CLI

获取所有资源类型的合规性摘要

以下命令返回不合规的 AWS 资源数量和合规资源的数量：

```
aws configservice get-compliance-summary-by-resource-type
```

在输出中，每个`CappedCount`属性的值表示有多少资源合规或不合规。

输出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

获取特定资源类型的合规性摘要

以下命令返回不合规的 EC2 实例的数量和合规的数量：

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

在输出中，每个CappedCount属性的值表示有多少资源合规或不合规。

输出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

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

PowerShell

用于 PowerShell

示例 1：此示例返回合规或不合规资源的数量，并将输出转换为 json。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
```

```
    "CappedCount": 100
  }
}
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考GetComplianceSummaryByResourceType中的。

获取 AWS Config 规则的评估结果

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

CLI

AWS CLI

获取 AWS Config 规则的评估结果

以下命令返回所有不符合名为的 AWS Config 规则的资源的评估结果`InstanceTypesAreT2micro`：

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

输出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
```

```
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

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

PowerShell

用于 PowerShell

示例 1：此示例获取规则的评估结果 access-keys-rotated 并返回按合规类型分组的输出

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

输出：

```
Count Name                      Group
----- ----                      -----
```

```
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

示例 2：此示例查询合规资源的规则 access-keys-rotated 的合规性详细信息。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

输出：

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考GetComplianceDetailsByConfigRule中的。

获取 AWS 资源的评估结果

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

CLI

AWS CLI

获取 AWS 资源的评估结果

以下命令返回 EC2 实例`i-1a2b3c4d`不符合的每条规则的评估结果：

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

输出：

```
{
    "EvaluationResults": [
        {
```

```
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

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

PowerShell

用于 PowerShell

示例 1：此示例评估结果针对给定资源。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

输出：

```
Annotation                  :
```

```
ComplianceType              : COMPLIANT
ConfigRuleInvokedTime       : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime          : 8/25/2019 11:34:56 PM
ResultToken                 :
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考GetComplianceDetailsByResource中的。

查看配置和合规性历史记录

> **Important**
>
> 要准确报告合规性状态，必须记录 `AWS::Config::ResourceCompliance` 资源类型。有关更多信息，请参阅重新编码 AWS 资源。

您可以在 AWS Config 控制台中查看资源的配置、关系和更改次数。您可以使用查看资源的配置历史记录 AWS CLI。

查看配置详细信息（控制台）

使用控制台查看配置详细信息

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

要从资源详细信息页面访问资源时间表，请选择资源时间表按钮。资源时间线将特定资源在一段时间内的更改捕获为 `ConfigurationItems`。您可以按配置事件、合规性事件或 CloudTrail事件进行筛选。

查看配置详细信息 (AWS CLI)

使用查看配置详细信息 AWS CLI

AWS Config 记录的配置项目以配置快照和配置流的形式按需传送到指定的交付渠道。您可以使用 AWS CLI 来查看每种资源的配置项目历史记录。

查看配置历史记录

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

```
$ aws configservice get-resource-config-history --resource-type AWS::EC2::SecurityGroup
 --resource-id sg-6fbb3807
{
    "configurationItems": [
        {
            "configurationItemCaptureTime": 1414708529.9219999,
            "relationships": [
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-7a3b232a",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-8b6eb2ab",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-c478efe5",
                    "relationshipName": "Is associated with Instance"
                },
                {
                    "resourceType": "AWS::EC2::Instance",
                    "resourceId": "i-e4cbe38d",
                    "relationshipName": "Is associated with Instance"
                }
            ],
            "availabilityZone": "Not Applicable",
            "tags": {},
            "resourceType": "AWS::EC2::SecurityGroup",
            "resourceId": "sg-6fbb3807",
            "configurationStateId": "1",
            "relatedEvents": [],
            "arn": "arn:aws:ec2:us-east-2:012345678912:security-group/default",
            "version": "1.0",
            "configurationItemMD5Hash": "860aa81fc3869e186b2ee00bc638a01a",
            "configuration": "{\"ownerId\":\"605053316265\",\"groupName\":\"default
\",\"groupId\":\"sg-6fbb3807\",\"description\":\"default group\",\"ipPermissions
\":[{\"ipProtocol\":\"tcp\",\"fromPort\":80,\"toPort\":80,\"userIdGroupPairs\":
[{\"userId\":\"amazon-elb\",\"groupName\":\"amazon-elb-sg\",\"groupId\":\"sg-843f59ed
\"}],\"ipRanges\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":0,\"toPort
\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName\":\"default
```

```
\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"udp\",\"fromPort
\":0,\"toPort\":65535,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",\"groupName
\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol\":\"icmp
\",\"fromPort\":-1,\"toPort\":-1,\"userIdGroupPairs\":[{\"userId\":\"605053316265\",
\"groupName\":\"default\",\"groupId\":\"sg-6fbb3807\"}],\"ipRanges\":[]},{\"ipProtocol
\":\"tcp\",\"fromPort\":1433,\"toPort\":1433,\"userIdGroupPairs\":[],\"ipRanges
\":[\"0.0.0.0/0\"]},{\"ipProtocol\":\"tcp\",\"fromPort\":3389,\"toPort\":3389,
\"userIdGroupPairs\":[],\"ipRanges\":[\"207.171.160.0/19\"]}],\"ipPermissionsEgress\":
[],\"vpcId\":null,\"tags\":[]}",
            "configurationItemStatus": "ResourceDiscovered",
            "accountId": "605053316265"
        }
    ],
    "nextToken":
     ..........
```

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

来自 AWS Config的 Amazon EBS 配置历史记录示例

AWS Config 生成一组文件，每个文件代表一种资源类型，并列出 AWS Config 正在记录的该类型资源的所有配置更改。 AWS Config 将此以资源为中心的配置历史记录作为对象导出到您在启用时指定的 Amazon S3 存储桶中。 AWS Config每个资源类型的配置历史记录文件中包含自上一个历史记录文件传送完毕后检测到的该类型资源出现的更改。历史记录文件通常每六小时传送一次。

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

```
{
    "fileVersion": "1.0",
    "requestId": "asudf8ow-4e34-4f32-afeb-0ace5bf3trye",
    "configurationItems": [
        {
            "snapshotVersion": "1.0",
            "resourceId": "vol-ce676ccc",
            "arn": "arn:aws:us-west-2b:123456789012:volume/vol-ce676ccc",
            "accountId": "12345678910",
            "configurationItemCaptureTime": "2014-03-07T23:47:08.918Z",
            "configurationStateID": "3e660fdf-4e34-4f32-afeb-0ace5bf3d63a",
            "configurationItemStatus": "OK",
            "relatedEvents": [
                "06c12a39-eb35-11de-ae07-adb69edbb1e4",
```

```
                "c376e30d-71a2-4694-89b7-a5a04ad92281"
            ],
            "availibilityZone": "us-west-2b",
            "resourceType": "AWS::EC2::Volume",
            "resourceCreationTime": "2014-02-27T21:43:53.885Z",
            "tags": {},
            "relationships": [
                {
                    "resourceId": "i-344c463d",
                    "resourceType": "AWS::EC2::Instance",
                    "name": "Attached to Instance"
                }
            ],
            "configuration": {
                "volumeId": "vol-ce676ccc",
                "size": 1,
                "snapshotId": "",
                "availabilityZone": "us-west-2b",
                "state": "in-use",
                "createTime": "2014-02-27T21:43:53.0885+0000",
                "attachments": [
                    {
                        "volumeId": "vol-ce676ccc",
                        "instanceId": "i-344c463d",
                        "device": "/dev/sdf",
                        "state": "attached",
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume1"
                    }
                ],
                "volumeType": "standard"
            }
        },
        {
```

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

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

```
                        "attachTime": "2014-03-07T23:46:28.0000+0000",
                        "deleteOnTermination": false
                    }
                ],
                "tags": [
                    {
                        "tagName": "environment",
                        "tagValue": "PROD"
                    },
                    {
                        "tagName": "name",
                        "tagValue": "DataVolume2"
                    }
                ],
                "volumeType": "standard"
            }
        }
    ]
}
```

查看资源的合规性历史记录时间线

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

您可以选择加入或选择退出记录 AWS Config中的所有资源类型。如果您选择记录所有资源类型，则 AWS Config 会自动开始记录由评估的资源合规性历史记录 AWS Config 规则。默认情况下，AWS Config 记录所有受支持资源的配置更改。您也可以仅选择特定的资源合规性历史记录资源类型：`AWS::Config::ResourceCompliance`。有关更多信息，请参阅选择 AWS Config 记录哪些资源。

使用资源查看资源时间线

通过从资源清单页面中选择特定资源来访问资源时间线。

1. 从左侧导航中选择资源。
2. 在“资源”清单页面上，您可以按资源类别、资源类型和合规性状态进行筛选。根据需要选择包括已删除的资源。

   该表显示了资源类型的资源标识符和该资源的资源合规性状态。资源标识符可以是资源 ID，也可以是资源名称。

3. 从资源标识符列中选择资源。
4. 选择资源时间表按钮。您可以按配置事件、合规性事件或 CloudTrail 事件进行筛选。

> **Note**
>
> 或者，在“资源”清单页面上，您可以直接选择资源名称。要从资源详细信息页面访问资源时间表，请选择资源时间表按钮。

使用规则查看资源时间线

通过从规则页面中选择特定规则来访问资源时间线。

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

查询合规性历史记录

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

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

您应该可以看到类似于如下所示的输出内容：

```
{
 "configurationItems": [
  {
   "configurationItemCaptureTime": 1539799966.921,
   "relationships": [
    {
     "resourceType": "AWS::S3::Bucket",
     "resourceId": "configrules-bucket",
     "relationshipName": "Is associated with "
```

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

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

标记您的 AWS Config 资源

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

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

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

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

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

与标记相关的限制

下面是适用于标签的基本限制。

限制	描述
每个资源的最大标签数	50
最大密钥长度	128 个 Unicode 字符（采用 UTF-8 格式）
最大值长度	256 个 Unicode 字符（采用 UTF-8 格式）
前缀限制	请勿在标签名称或值中使用 `aws:` 前缀，因为它专为 AWS 使用预留。您无法编辑或删除带此前缀的标签名称或值。具有此前缀的标签不计入每个资源的标签数限制。
字符限制	标签只能包含 Unicode 字母、数字、空格或以下符号：`_ . : / = + - @`

使用 AWS Config API 操作管理标签

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

- ListTagsForResource
- TagResource
- UntagResource

> **Note**
>
> `TagResource` 和 `UntagResource` 需要某些 AWS Identity and Access Management (IAM) 权限才能控制访问权限。有关更多信息，请参阅《IAM 用户指南》中的根据标签键控制访问权限。

使用 AWS Config 规则评估资源

AWS Config 用于评估 AWS 资源的配置设置。为此，您可以创建 AWS Config 规则，这些规则代表您的理想配置设置。 AWS Config 提供名为托管规则的可自定义预定义规则，以帮助您入门。

AWS Config 规则如何运作

在 AWS Config 持续跟踪您的资源中出现的配置更改时，它会检查这些更改是否不符合规则中的任何条件。如果资源不符合规则，则会将该资源和规则 AWS Config 标记为不合规。以下是 AWS Config 规则可能的评估结果：

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

例如，创建 EC2 卷时， AWS Config 可以根据要求加密卷的规则评估该卷。如果卷未加密，则会将该卷和规则 AWS Config 标记为不合规。 AWS Config 还可以检查您的所有资源以了解整个账户的需求。例如， AWS Config 可以检查账户中的 EC2 卷数量是否保持在所需的总数之内，或者账户是否 AWS CloudTrail 用于日志记录。

服务关联规则

服务相关规则是一种独特的托管规则，它支持其他 AWS 服务在您的账户中创建 AWS Config 规则。这些规则是预定义的，包括代表您调用其他 AWS 服务所需的所有权限。这些规则与 AWS 服务在您的合规性验证中推荐 AWS 账户 的标准类似。有关更多信息，请参阅 服务相关规则 AWS Config。

自定义规则

您还可以创建自定义规则来评估尚未 AWS Config 记录的其他资源。有关更多信息，请参阅 AWS Config 自定义规则 和 评估其他资源类型。

查看合规性

AWS Config 控制台显示您的规则和资源的合规性状态。您可以查看您的 AWS 资源总体上如何符合所需的配置，并了解哪些特定资源不合规。您还可以使用 AWS CLI、 AWS Config API 和 AWS 软件开发工具包向 AWS Config 服务请求合规性信息。

通过使用 AWS Config 来评估您的资源配置，您可以评估您的资源配置在多大程度上符合内部实践、行业准则和法规。

限制

有关每个地区每个账户的最大 AWS Config 规则数和其他服务限制，请参阅AWS Config 服务限制。

与成本相关的注意事项

有关资源记录相关费用的详细信息，请参阅AWS Config 定价。

建议：删除规则之前停止记录资源合规性

强烈建议您在删除账户中的规则之前，停止记录该`AWS::Config::ResourceCompliance`资源类型。删除规则会为配置记录器创建配置项目 (CI)，`AWS::Config::ResourceCompliance`并可能影响您的 AWS Config 配置记录器成本。如果您要删除评估大量资源类型的规则，则可能会导致记录的 CI 数量激增。

最佳实践：

1. 停止录制 `AWS::Config::ResourceCompliance`
2. 删除规则
3. 开启录制 `AWS::Config::ResourceCompliance`

建议：添加逻辑以处理自定义 lambda 规则对已删除资源的评估

在创建 AWS Config 自定义 lambda 规则时，强烈建议您添加逻辑来处理已删除资源的评估。

当评估结果被标记为 `NOT_APPLICABLE` 时，这些资源将被标记为已删除并被清理。如果未将其标记为`NOT_APPLICABLE`，则在删除规则之前，评估结果将保持不变，这可能会导致规则删除`AWS::Config::ResourceCompliance`后创建的 CI 出现意外激增。

有关如何设置 AWS Config 自定义 lambda 规则以返回`NOT_APPLICABLE`已删除资源的信息，请参阅使用 AWS Config 自定义 lambda 规则管理已删除的资源。

建议：为自定义 lambda 规则提供范围内的资源

AWS Config 如果自定义 Lambda 规则的范围不限于一种或多种资源类型，则该规则可能会导致大量的 Lambda 函数调用。为避免与您的账户相关的活动增加，强烈建议您在自定义 Lambda 规则的范围内提供资源。如果未选择任何资源类型，该规则将为账户中的所有资源调用 Lambda 函数。

区域支持

目前，以下 AWS 区域支持 AWS Config 规则功能。有关哪些区域支持哪些单独 AWS Config 规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com config-fips.us-east-2.amazonaws.com	HTTPS HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com config-fips.us-east-1.amazonaws.com	HTTPS HTTPS
美国西部（加利福尼亚北部）	us-west-1	config.us-west-1.amazonaws.com config-fips.us-west-1.amazonaws.com	HTTPS HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com config-fips.us-west-2.amazonaws.com	HTTPS HTTPS
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

以下区域支持跨 AWS 组织成员账户部署 AWS Config 规则。

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS
美国西部（加利福尼亚北部）	us-west-1	config.us-west-1.amazonaws.com	HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

区域名称	区域	端点	协议
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config 规则的组成部分

AWS Config 规则会评估您的 AWS 资源的配置设置。有两种类型的规则：AWS Config 托管规则和 AWS Config 自定义规则。

AWS Config 托管规则是由创建的预定义的、可自定义的规则 AWS Config。有关托管规则的列表，请参阅 AWS Config 托管规则列表。

AWS Config 自定义规则是您从头开始创建的规则。有两种方法可以创建 AWS Config 自定义规则：使用 Lambda 函数（AWS Lambda 开发者指南）和使用 Guard（Guard GitHub存储库）（一种 policy-as-code 语言）。 AWS Config 使用创建的 AWS Lambda 自定义规则称为AWS Config 自定义 Lambda 规则，使用 Guard 创建的 AWS Config 自定义规则称为AWS Config 自定义策略规则。

本页讨论 AWS Config 托管规则的元数据以及如何使用规则开发套件 (RDK) 和 AWS Config 规则开发工具包库 (RDKLib) 使用 Python 编写 AWS Config 自定义 AWS Config 规则的最佳实践。

有关如何创建 AWS Config 自定义策略规则的演练，请参阅创建 AWS Config 自定义策略规则。有关如何创建自定义 Lambda 规则的演练，请参阅 AWS Config 创建 AWS Config 自定义 Lamb da 规则。

目录

- AWS Config 托管规则元数据
- AWS Config 自定义规则结构
  - 写入规则
  - 规则逻辑

AWS Config 托管规则元数据

AWS Config 托管规则可以包含以下可变元数据：

默认名称

defaultName 是规则实例在默认情况下将获得的名称。

描述

规则描述提供了规则评估内容的上下文。 AWS Config 控制台具有 256 个字符的限制。作为最佳实践，规则描述应以“检查是否”开头，并包括对 NON_COMPLIANT 场景的描述。在规则描述中首次提及时，服务名称应以 AWS 或 Amazon 开头。例如， AWS CloudTrail 或者用 Amazon CloudWatch 代替 CloudTrail 或 CloudWatch 首次使用。服务名称可以在后续引用后使用缩写。

范围

范围决定了规则所针对的资源类型。有关支持的资源类型列表，请参阅支持的资源类型。

必填InputParameter详情

compulsoryInputParameter详细信息用于规则进行评估所需的参数。例如，`access-keys-rotated` 托管规则包含 `maxAccessKeyAge` 作为必要参数。如果为必要参数，则不会被标记为（可选）。必须指定每个参数的类型。类型可以是 “字符串”、“整数”、“双精度”、“CSV”、“布尔值” 和 “StringMap” 之一。

可选InputParameter详情

optionalInputParameter详细信息用于规则评估时可选的参数。例如，`elasticsearch-logs-to-cloudwatch` 托管规则包含 `logTypes` 作为可选参数。必须指定每个参数的类型。类型可以是 “字符串”、“整数”、“双精度”、“CSV”、“布尔值” 和 “StringMap” 之一。

支持的 EvaluationModes

supportedEvaluationModes 决定何时对资源进行评估，无论是在部署资源之前，还是在部署资源之后。

DETECTIVE 用于评估已经部署的资源。这允许您评估现有资源的配置设置。PROACTIVE 用于在资源部署之前对其进行评估。

这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。

您可以指定 to supportedEvaluationModes DETECTIVE PROACTIVE、或两者兼DETECTIVE而有之PROACTIVE。必须指定评估模式，且此字段不能为空。

有关更多信息，请参阅评估模式。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。

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

AWS Config 自定义规则结构

本节包含有关使用 AWS Config 规则开发套件 (RDK) 和 AWS Config 规则开发套件库 (rdkLib) 的信息。有关 RDK 或 RDKLib 的更多信息，请参阅和 aws-config-rdklib 存储库。aws-config-rdk GitHub

写入规则

先决条件

1. 按照安装 AWS CLI 中的步骤进行操作。
2. 按照 “使用控制台AWS Config 进行设置” 或 “使用控制台 AWS Config进行设置” 中的步骤进行操作 AWS CLI。有关支持 AWS 区域的信息，请从AWS 区域服务列表中选择您的区域。 AWS Config
3. 使用推荐的 pip 方法安装 RDK：

```
pip install rdk
```

> **Note**
>
> 在使用之前，请确保 pip 已安装在您的计算机上。

4. 使用推荐的 pip 方法安装 RDKLib：

```
pip install rdklib
```

> **Note**
>
> 在使用之前，请确保 pip 已安装在您的计算机上。

变更触发的规则

1. 要创建通过更改指定资源类型触发的规则，请运行以下命令：

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

以下示例将创建一个通过更改 `AWS::IAM::User` 资源类型触发的规则：

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

您可将以下标记与 `rdk create` 命令一起用于变更触发的规则：

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

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

运行 `rdk create` 后，您应该会看到一个带有规则名称的新目录，里面有 3 个文件：

- *RULE_NAME*`.py` - 存储规则逻辑的 Python 文件
- *RULE_NAME*`_test.py` - 存储规则的单元测试的 Python 文件

- `parameters.json` - RDK 部署设置的 JSON 文件

2. 下一步是编写规则逻辑。您只需编辑 *RULE_NAME*.py 文件即可。如果打开 *RULE_NAME*.py 文件，会看到一个模板，可以在其中添加规则逻辑。以下是为 MFA_ENABLED_RULE 生成的模板：

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

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

class MFA_ENABLED_RULE(ConfigRule):

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

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

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

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

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

以下示例是具有规则逻辑的 MFA_ENABLED_RULE 模板的编辑后版本。此规则检查 IAM 用户是否已启用多重身份验证 (MFA)。如果 IAM 用户未启用 MFA，则该规则 NON_COMPLIANT。有关模板中提供的规则逻辑和方法的更多信息，请参阅规则逻辑。

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

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

```
class MFA_ENABLED_RULE(ConfigRule):

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

        username = configuration_item.get("resourceName")

        iam_client = client_factory.build_client("iam")

        response = iam_client.list_mfa_devices(UserName=username)

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

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

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

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

3. 下一步是使用控制台或在 AWS 其中安装 RDKLib 层。 AWS AWS CLI RDKLib 设计为作为一个 AWS Lambda 层工作。它允许您使用库，而无需将库包含在部署包中。

   - 要使用 AWS 控制台安装 RDKLib 层，请执行以下步骤：

     1. 打开 AWS Serverless Application Repository 控制台，网址为 https://console.aws.amazon.com/serverlessrepo。
     2. 在左侧导航菜单上，选择可用应用程序。
     3. 搜索`rdklib`并选择 rdk lib。
     4. 查看函数详细信息，然后进行部署。您无需进行任何更改。

5. 在概述页面的资源部分，复制 Lambda 层的亚马逊资源名称 (ARN)。部署规则时，需要 Lambda 层的 ARN。

- 要使用安装 RDKLib 层 AWS CLI，请运行以下命令：

1. 为 RDKlib 层创建更改集。

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

返回以下输出：

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

2. 执行此更改集。您可以复制/粘贴完整的变更集 ARNChangeSetId（来自上一步中生成的输出），以自定义以下命令：

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

3. 返回作为已部署堆栈一部分的所有关联资源。

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

返回以下输出：

```
{
    "StackResources": [
        {
            "StackName": "serverlessrepo-RDKlib-Layer",
            "StackId": "arn:aws:cloudformation:us-east-1:123456789012:stack/
serverlessrepo-RDKlib-Layer/365436a0-a58a-11ea-9b04-12ae8fb95b53",
            "LogicalResourceId": "RdklibLayercf22317faf",
```

```
            "PhysicalResourceId": "arn:aws:lambda:us-
east-1:123456789012:layer:rdklib-layer:1",
            "ResourceType": "AWS::Lambda::LayerVersion",
            "Timestamp": "2020-06-03T11:26:30.501Z",
            "ResourceStatus": "CREATE_COMPLETE",
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

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

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

4. 下一步是为 Lambda 函数提供一个要代入的角色。默认情况下，Lambda 函数会尝试代入 `AWSServiceRoleForConfig` 角色，但这是不允许的。您需要使用 `AWS_ConfigRole` 托管策略创建角色。该角色必须与 AWS Config 具有信任关系，并且 /rdk/ 路径下的所有角色都应代入该角色。以下是信任策略的示例：

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

```
      }
    }
  ]
}
```

使用此信任策略运行以下命令：

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

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

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

您还可以使用 rdk modify 通过以下标记来更新变更触发的规则详细信息：

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

5. 最后一步是部署规则。要部署规则，请使用步骤 3 中的 Lambda 层的 ARN 运行以下命令：

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

6. 现已部署此规则。您可以使用 AWS Config 控制台检查规则是否按预期运行。

定期规则

1. 要为指定的资源类型创建定期触发的规则，请运行以下命令：

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

以下示例将为 AWS::IAM::User 资源类型创建每 24 小时触发一次的规则：

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

您可将以下标记与 `rdk create` 命令一起用于定期规则：

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

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

运行 `rdk create` 后，您应该会看到一个带有规则名称的新目录，里面有 3 个文件：

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

2. 下一步是编写规则逻辑。您只需编辑 *RULE_NAME*.py 文件即可。如果打开 *RULE_NAME*.py 文件，会看到一个模板，可以在其中添加规则逻辑。以下是为 MFA_ENABLED_RULE 生成的模板：

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

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

class MFA_ENABLED_RULE(ConfigRule):

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

```
        ##############################

        return [Evaluation(ComplianceType.NOT_APPLICABLE)]

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

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

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

此模板默认为变更触发的规则。但需要在 `evaluate_periodic` 方法中添加您的逻辑。以下示例是具有规则逻辑的 MFA_ENABLED_RULE 模板的编辑后版本。此规则检查 IAM 用户是否已启用多重身份验证 (MFA)。如果 IAM 用户未启用 MFA，则该规则 NON_COMPLIANT。有关模板中提供的规则逻辑和方法的更多信息，请参阅规则逻辑。

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

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

class MFA_ENABLED_RULE(ConfigRule):l

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

        iam_client = client_factory.build_client("iam")

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

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

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

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

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

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

3. 下一步是使用控制台或在 AWS 其中安装 RDKLib 层。 AWS AWS CLI RDKLib 设计为作为一个 AWS Lambda 层工作。它允许您使用库，而无需将库包含在部署包中。

   - 要使用 AWS 控制台安装 RDKLib 层，请执行以下步骤：

     1. 打开 AWS Serverless Application Repository 控制台，网址为 https://console.aws.amazon.com/serverlessrepo。
     2. 在左侧导航菜单上，选择可用应用程序。
     3. 搜索`rdklib`并选择 rdk lib。
     4. 查看函数详细信息，然后进行部署。您无需进行任何更改。
     5. 在概述页面的资源部分，复制 Lambda 层的亚马逊资源名称 (ARN)。部署规则时，需要 Lambda 层的 ARN。

   - 要使用安装 RDKLib 层 AWS CLI，请运行以下命令：

     1. 为 RDKlib 层创建更改集。

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

返回以下输出：

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

2. 执行此更改集。您可以复制/粘贴完整的变更集 ARNChangeSetId（来自上一步中生成的输出），以自定义以下命令：

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

3. 返回作为已部署堆栈一部分的所有关联资源。

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

返回以下输出：

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

```
            "DriftInformation": {
                "StackResourceDriftStatus": "NOT_CHECKED"
            }
        }
    ]
}
```

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

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

4. 下一步是为 Lambda 函数提供一个要代入的角色。默认情况下，Lambda 函数会尝试代入 `AWSServiceRoleForConfig` 角色，但这是不允许的。您需要使用 `AWS_ConfigRole` 托管策略创建角色。该角色必须与 AWS Config 具有信任关系，并且 /rdk/ 路径下的所有角色都应代入该角色。以下是信任策略的示例：

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

使用此信任策略运行以下命令：

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

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

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

您还可以使用 rdk modify 通过以下标记来更新定期规则详细信息：

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

5. 最后一步是部署规则。要部署规则，请使用步骤 3 中的 Lambda 层的 ARN 运行以下命令：

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

6. 现已部署此规则。您可以使用 AWS Config 控制台检查规则是否按预期运行。

规则逻辑

以下 Python 代码示例是使用 RDK 和 RDKLib 编写规则的模板。只应在 evaluate_parameters、evaluate_change 和 evaluate_periodic 方法中进行更改，或者在需要时编写全新的函数来为逻辑提供帮助。有关使用 RDK 和 RDKlib 编写规则的先决条件，请参阅先决条件 。

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

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

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

    def evaluate_parameters(self, rule_parameters):
        return rule_parameters

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

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

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

APPLICABLE_RESOURCES

`APPLICABLE_RESOURCES` 是规则所针对的资源类型。如果使用，它应该是一个全局变量，设置为规则所针对的资源类型。有关支持的资源类型列表，请参阅支持的资源类型。

evaluate_parameters

描述

此方法用于检查规则的输入参数是否有效。以下是最佳实践：

- 检查是否列出了正确数量的参数。
- 检查参数名称是否正确。
- 检查参数值的类型是否正确。
- 如果参数是整数，请检查该参数是否在合理的范围内。
- 如果该参数的可能选项数量有限，请检查该参数是否是这些选项之一。

- 如果参数是字符串，请检查其长度是否合理，并删除该值前后的空格。
- 检查是否正确处理了大小写。
- 尽可能限制参数输入。例如，如果收到以逗号分隔的 ARN 列表，请确保唯一允许的字符是逗号和 ARN 支持的字符。

参数

`rule_parameters` 是规则输入参数字典。

返回语法

如果其中一个参数无效，可能会引发 `InvalidParametersError` 错误：

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

如果参数全部有效，则该方法应返回一个字典：

```
return valid_rule_parameters
```

evaluate_change

描述

此方法用于评估变更触发的规则的逻辑。

参数

`event`是由提供的 AWS Lambda 事件 AWS Config。此事件是一个 JSON 格式的文档，其中包含 Lambda 函数要操作的数据。有关示例，请参阅AWS Config 规则的示例事件。

`client_factory`是要用于规则的 ClientFactory 对象。该 ClientFactory 类创建或重复使用 boto3 客户端，该客户端为服务提供低级接口。 AWS boto3 客户端方法与 AWS 服务 API 映射，这意味着服务操作映射到同名的客户端方法并提供对相同操作参数的访问权限。有关可用服务的列表，请参阅 Boto3 Docs 文档中的可用服务。

`client_factory` 的请求语法如下：

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

例如：

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

> **Note**
>
> 必须输入 AWS 服务的 boto3 名称。

`configuration_item` 是完整配置项的字典，即使超大。配置项目表示所支持 AWS 资源的各种属性的 point-in-time 视图。有关内容的信息`ConfigurationItem`，请参阅 AWS Config API 参考ConfigurationItem中的。

`valid_rule_parameters` 是 `evaluate_parameters()` 方法的输出。

返回语法

此方法应返回以下一项或多项：

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

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

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

> **Note**
>
> 报告已删除资源的规则应返回 `NOT_APPLICABLE` 的评估结果，以避免不必要的规则评估。

对于所有不合规的评估，您都应使用注释。例如：

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

evaluate_periodic

描述

此方法用于评估定期规则。

参数

`event`是由提供的 AWS Lambda 事件 AWS Config。此事件是一个 JSON 格式的文档，其中包含 Lambda 函数要操作的数据。有关示例，请参阅AWS Config 规则的示例事件。

`client_factory`是要用于规则的 ClientFactory 对象。该 ClientFactory 类创建或重复使用 boto3 客户端，该客户端为服务提供低级接口。 AWS boto3 客户端方法与 AWS 服务 API 映射，这意味着服务操作映射到同名的客户端方法并提供对相同操作参数的访问权限。有关可用服务的列表，请参阅 Boto3 Docs 文档中的可用服务。

`client_factory` 的请求语法如下：

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

例如：

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

> **Note**
>
> 必须输入 AWS 服务的 boto3 名称。

`valid_rule_parameters` 是 `evaluate_parameters()` 方法的输出。

返回语法

此方法应返回以下一项或多项：

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

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

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

> **Note**
>
> 报告已删除资源的规则应返回 NOT_APPLICABLE 的评估结果，以避免不必要的规则评估。

对于所有不合规的评估，您都应使用注释。例如：

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

lambda_handler

描述

无需修改此方法。Lambda 处理程序用于处理事件。该函数在将`event`对象 AWS Lambda 传递给`handler`方法时运行。有关更多信息，请参阅 Python 中的 Lambda 函数处理程序中的。

参数

`event`是由提供的 AWS Lambda 事件 AWS Config。此事件是一个 JSON 格式的文档，其中包含 Lambda 函数要操作的数据。有关示例，请参阅AWS Config 规则的示例事件。

`context` 是在运行时由 Lambda 传递给函数的对象。此对象提供方法和属性，这些方法和属性提供函数运行时可以使用的信息和方法。请注意，在新版本的 Lambda 中，不再使用上下文。

AWS Config 规则的评估模式和触发器类型

在向账户添加规则时，您可以指定在资源创建和管理过程中何 AWS Config 时评估您的资源。资源创建和管理过程称为资源预置。您可以选择评估模式来指定在此过程中何 AWS Config 时评估您的资源。

根据规则， AWS Config 可以在部署资源之前、部署资源之后或两者兼而有之地评估您的资源配置。在资源部署之前对其进行评估是主动评估。在资源部署之后对其进行评估是侦查评估。

您也可以选择触发器类型来指定您的 AWS Config 规则评估资源的频率。当配置发生更改时，可以按定期计划或按选择的频率对资源进行评估。

触发器类型

向账户添加规则后， AWS Config 将您的资源与规则的条件进行比较。在这次初始评估之后，每次触发评估时都会 AWS Config 继续运行评估。规则中会定义评估触发器，可以包括以下类型：

触发器类型	描述
配置更改	AWS Config 当存在与规则范围匹配的资源并且资源的配置发生变化时，会对规则进行评估。评估将在 AWS Config 发送配置项目变更通知后运行。 通过定义规则的范围来选择哪些资源启动评估。范围可以包括： • 一个或多个资源类型 • 资源类型和资源 ID 的组合 • 标签键和值的组合 • 当创建、更新或删除任何记录的资源时 AWS Config 当它检测到与规则范围相匹配的资源发生变化时，就会运行评估。您可以使用范围来定义哪些资源启动评估。
定期	AWS Config 按您选择的频率对规则进行评估；例如，每 24 小时运行一次。
混合	有些规则既有配置更改也有定期触发器。对于这些规则，它 AWS Config 会在检测到配置更改时以及按照您指定的频率评估您的资源。

评估模式

有两种评估模式：

主动模式

使用主动评估在资源部署之前对其进行评估。这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。

资源类型架构说明了资源的属性。您可以在 AWS CloudFormation 注册表的 “AWS 公共扩展” 中找到资源类型架构，也可以使用以下 CLI 命令找到：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

有关更多信息，请参阅《 AWS CloudFormation 用户指南》中参考的通过 AWS CloudFormation 注册表管理扩展以及AWS 资源和属性类型。

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

主动评估的托管规则列表

有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。

支持主动评估的资源类型列表

以下是支持主动评估的资源类型列表：

- `AWS::ApiGateway::Stage`
- `AWS::AutoScaling::AutoScalingGroup`
- `AWS::EC2::EIP`
- `AWS::EC2::Instance`
- `AWS::EC2::Subnet`
- `AWS::Elasticsearch::Domain`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::Redshift::Cluster`
- `AWS::S3::Bucket`
- `AWS::SNS::Topic`

主动评估的规则示例

主动规则示例

1. 您可以将 AWS Config 托管规则添加到您的账户`S3_BUCKET_LOGGING_ENABLED`，以检查您的 S3 存储桶是否启用了日志记录。

2. 对于评估模式，请在 AWS 管理控制台中选择 “开启主动评估”，或者在 PutConfigRuleAPI `EvaluationModes` 中启用`PROACTIVE`。

开启主动评估后，您可以使用 StartResourceEvaluationAPI 和 GetResourceEvaluationSummaryAPI 来检查您的账户中尚未部署到生产环境的存储桶是否未启用日志记录。这允许您在部署之前测试资源配置，并重新评估是否要将资源部署到生产环境。

例如，从 StartResourceEvaluation API 开始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::S3::Bucket",
                                     "ResourceConfiguration": "{\"BucketName\": \"my-
bucket\", \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您应该会在输出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然后，使用`ResourceEvaluationId`带有 GetResourceEvaluationSummary API 的来检查评估结果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您应收到类似以下内容的输出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
```

```
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration": "{\"BucketName\": \"my-bucket\",
 \"LoggingConfiguration\": {\"DestinationBucketName\": \"my-log-bucket\",
\"LogFilePrefix\":\"my-log\"}}",

    }
}
```

要查看有关评估结果的更多信息，例如哪条规则将资源标记为 “不合规”，请使用 API。GetComplianceDetailsByResource

侦查模式

使用侦查评估来评估已部署的资源。这允许您评估现有资源的配置设置。

侦查评估的规则示例

变更触发的规则示例

1. 向账户添加托管规则 `S3_BUCKET_LOGGING_ENABLED`，以检查您的 S3 存储桶是否启用了日志记录。
2. 该规则的触发器类型是配置更改。 AWS Config 在创建、更改或删除 S3 存储桶时对规则进行评估。
3. 当存储桶更新时，配置更改会启动此规则， AWS Config 会评估存储桶是否符合此规则。

定期规则示例

1. 向账户添加托管规则 `IAM_PASSWORD_POLICY`。此规则检查您的 IAM 用户的密码策略是否符合您的账户策略，如最小长度或特定字符要求。
2. 该规则的触发器类型是周期性的。 AWS Config 按您指定的频率（例如每 24 小时）对规则运行评估。
3. 该规则每 24 小时启动一次，并 AWS Config 评估您的 IAM 用户的密码是否符合该规则。

具有配置更改和定期触发器的混合规则示例

1. 创建自定义规则，评估您账户中的 AWS CloudTrail 跟踪是否已开启并记录所有区域。

2. 每次创建、更新或删除跟踪时，您都希望 AWS Config 对规则进行评估。您还 AWS Config 想每 12 小时运行一次规则。
3. 对于触发器类型，您可以为配置更改和定期触发器编写逻辑。有关更多信息，请参阅AWS Config 规则的组成部分：编写规则。

关闭配置记录器时的规则评估

如果您关闭配置记录器，则 AWS Config 会停止记录对资源配置的更改。这会在以下方面影响到您的规则评估：

- 定期规则继续以指定的频率运行评估。
- 变更触发的规则不运行评估。
- 混合规则仅以指定的频率运行评估。规则不为配置更改运行评估。
- 如果您针对具有配置更改触发器的规则运行按需评估，则规则将评估资源的最后已知状态，这是最后一个记录的配置项目。

> **Important**
>
> 避免不必要的 AWS Config 评估
>
> 除非删除定期规则和混合规则，否则即使已关闭配置记录器，定期规则和混合规则也将继续运行。这些规则只评估在关闭配置记录器之前记录的配置项目，这意味着如果没有新信息，这些规则将重现相同的评估结果。关闭配置记录器时，请删除定期规则和混合规则，以避免不必要的活动和规则评估。

AWS Config 托管规则

AWS Config 提供AWS 托管规则，这些规则是预定义的可自定义规则， AWS Config 用于评估您的 AWS 资源是否符合常见的最佳实践。例如，您可以使用一个托管规则来快速开始评估您的 Amazon Elastic Block Store (Amazon EBS) 卷是否已加密，或者特定标签是否已应用于您的资源。 AWS Config 控制台将引导您完成配置和激活托管规则的过程。您还可以使用 AWS Command Line Interface 或 AWS Config API 传递定义托管规则配置的 JSON 代码。

您可以自定义托管规则的行为以满足您的需求。例如，您可以定义规则的范围以便限定触发规则评估的资源，例如 EC2 实例或卷。您可以自定义规则的参数，以便定义您的资源为符合规则而必须具备的属性。例如，您可以自定义一个参数，以指定您的安全组应阻止传输到特定端口号的传入流量。

与成本相关的注意事项

有关资源记录相关费用的详细信息，请参阅AWS Config 定价。

建议：在删除规则之前停止记录资源合规性

强烈建议您在删除账户中的规则之前，停止记录该`AWS::Config::ResourceCompliance`资源类型。删除规则会为配置记录器创建配置项目 (CI)，`AWS::Config::ResourceCompliance`并可能影响您的 AWS Config 配置记录器成本。如果您要删除评估大量资源类型的规则，则可能会导致记录的 CI 数量激增。

最佳实践：

1. 停止录制 `AWS::Config::ResourceCompliance`
2. 删除规则
3. 开启录制 `AWS::Config::ResourceCompliance`

触发器类型

向账户添加规则后， AWS Config 将您的资源与规则的条件进行比较。在这次初始评估之后，每次触发评估时都会 AWS Config 继续运行评估。评估触发器被定义为规则的一部分，它们可以包括以下类型。

触发器类型	描述
配置更改	AWS Config 当存在与规则范围匹配的资源并且资源的配置发生变化时，会对规则进行评估。评估将在 AWS Config 发送配置项目更改通知后运行。 通过定义规则的范围来选择哪些资源启动评估。范围可以包括： • 一个或多个资源类型 • 资源类型和资源 ID 的组合 • 标签键和值的组合 •

触发器类型	描述
	当创建、更新或删除任何记录的资源时 AWS Config 当它检测到与规则范围相匹配的资源发生变化时运行评估。您可以使用范围来定义哪些资源启动评估。
定期	AWS Config 按您选择的频率对规则进行评估；例如，每 24 小时运行一次。
混合	有些规则既有配置更改也有定期触发器。对于这些规则，它 AWS Config 会在检测到配置更改时以及按照您指定的频率评估您的资源。

评估模式

AWS Config 规则有两种评估模式。

评估模式	描述
主动	使用主动评估在资源部署之前对其进行评估。这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。 有关更多信息，请参阅评估模式。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。
侦查	使用侦查评估来评估已部署的资源。这允许您评估现有资源的配置设置。

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

主题

- AWS Config 托管规则列表
- 按评估模式列出的 AWS Config 托管规则列表
- 按触发器类型列出的 AWS Config 托管规则列表
- 按区域可用性列出的 AWS Config 托管规则列表
- 服务相关规则 AWS Config
- 使用 AWS CloudFormation 模板创建 AWS Config 托管规则

AWS Config 托管规则列表

AWS Config 目前支持以下托管规则。

注意事项

托管规则的默认值

只有在使用 AWS 控制台时，才会预先填充为托管规则指定的默认值。未提供 API、CLI 或 SDK 的默认值。

不支持目录存储桶

在评估亚马逊简单存储服务 (Amazon S3) 资源时，托管规则仅支持通用存储桶。 AWS Config 不记录目录存储桶的配置更改。有关通用存储桶和目录存储桶的更多信息，请参阅 Amazon S3 用户指南中的存储桶概述和目录存储桶。

托管规则和全球 IAM 资源类型

2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。

为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

主题

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest

- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled

- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloudtrail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured

- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled

- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-systems-manager
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair

- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan

- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled

- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam 服务器证书到期检查
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- restricted-ssh
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- ec2-instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access

- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloudtrail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled

- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-common-ports
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled

- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

access-keys-rotated

检查活动 IAM 访问密钥是否在 `maxAccessKeyAge` 中指定的天数内轮换（更改）。如果访问密钥未在指定时间段内轮换，则此规则为 NON_COMPLIANT。默认值为 90 天。

> **Warning**
>
> 请不要向未经授权方提供访问密钥，即便是为了帮助找到您的账户标识符也不行。如果您这样做，可能会向某人提供对您的账户的永久访问权限。安全最佳实践是，在用户不再需要密码和访问密钥时将其删除。

> **Note**
>
> 控制台中标记为 “不合规” 的资源类型
>
> 如果此规则发现您的任何访问密钥不合规，则该`AWS::IAM::User`资源类型也将在控制台中标记为不合规。 AWS
>
> 托管规则和全球 IAM 资源类型
>
> 2022 年 2 月之前加入的全球 IAM 资源类型
>
> （`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。
>
> 如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。
>
> 为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。
>
> 限制
>
> 此规则不适用于 AWS 账户根用户访问密钥。要删除或轮换您的根用户访问密钥，请使用您的根用户凭据登录到位于的 “我的安全证书” 页面https://aws.amazon.com/console/。 AWS Management Console

标识符：ACCESS_KEYS_ROTATED

资源类型： AWS::IAM::User

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大AccessKey年龄, 类型：int, 默认值：90

最长不轮换天数。默认值：90。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

account-part-of-organizations

检查 AWS 账户是否是 Organization AWS s 的一部分。如果账户不属于组织或 AWS AWS 组织主 AWS 账户 ID 与规则参数不匹配，则该规则为 NON_COMPLIMENT。`MasterAccountId`

> **Note**
>
> 托管规则和全球 IAM 资源类型
>
> 2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。
>
> 如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。
>
> 为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

标识符：ACCOUNT_PART_OF_ORGANIZATIONS

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

MasterAccountId （可选），类型：字符串

账户的主账户 ID。 AWS

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

acm-certificate-expiration-check

检查您账户中的 Certifice Manager AWS 证书是否被标记为在指定的天数内到期。将自动续订由 ACM 提供的证书。ACM 不会自动续订您导入的证书。如果您的证书即将过期，则此规则为 NON_COMPLIANT。

标识符：ACM_CERTIFICATE_EXPIRATION_CHECK

资源类型： AWS::ACM::Certificate

触发器类型：配置更改和定期

AWS 区域: 所有支持的 AWS 区域

参数：

daysToExpiration （可选），类型：int, 默认值：14

指定规则将 ACM 证书标记为不合规之前的天数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

acm-certificate-rsa-check

检查由 Certificate Manager (ACM) 管理的 RSA AWS 证书的密钥长度是否至少为 '2048' 位。如果最小密钥长度小于 2048 位，则该规则不合规。

标识符：ACM_CERTIFICATE_RSA_CHECK

资源类型： AWS::ACM::Certificate

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

acm-pca-root-ca-disabled

检查 AWS 私有证书颁发机构（AWS 私有 CA）是否有已禁用的根 CA。对于状态不为 DISABLED 的根 CA，该规则为 NON_COMPLIANT。

标识符：ACM_PCA_ROOT_CA_DISABLED

资源类型： AWS::ACMPCA::CertificateAuthority

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

exemptedCAArns（可选），类型：CSV

可以启用的 CA 的 Amazon 资源名称 (ARN) 列表（以逗号分隔）。可以为其他 CA 提供此值，例如可以启用的特定根 CA 或中间 CA。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

alb-desync-mode-check

检查应用程序负载均衡器 (ALB) 是否已配置为用户定义的取消同步缓解模式。如果 ALB 取消同步缓解模式与用户定义的取消同步缓解模式不匹配，则此规则为 NON_COMPLIANT。

标识符：ALB_DESYNC_MODE_CHECK

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

desyncMode, 类型：CSV

逗号分隔列表，客户可选择其中的最多 2 个值：“defensive”、“strictest”和“monitor”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

alb-http-drop-invalid-header-enabled

检查规则是否评估 AWS 应用程序负载均衡器 (ALB)，以确保它们配置为丢弃 http 标头。如果 routing.http.drop_invalid_header_fields.enabled 的值设置为 false，则此规则为 NON_COMPLIANT。

标识符：ALB_HTTP_DROP_INVALID_HEADER_ENABLED

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

alb-http-to-https-redirection-check

检查是否在应用程序负载均衡器的所有 HTTP 侦听器上都配置了 HTTP 到 HTTPS 重定向。如果应用程序负载均衡器的一个或多个 HTTP 侦听器未配置 HTTP 到 HTTPS 重定向，则此规则为 NON_COMPLIANT。如果多个 HTTP 侦听器中的一个转发到 HTTP 侦听器而不是重定向，则此规则也为 NON_COMPLIANT。

标识符：ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

alb-waf-enabled

检查应用程序负载均衡器 (ALB) 上是否启用了 AWS WAF。如果 key: waf.enabled 设置为 false，则此规则为 NON_COMPLIANT。

标识符：ALB_WAF_ENABLED

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

wafWebAclIds （可选），类型：CSV

用于检查 ALB 关联的 Web ACL ID（对于 WAF）或 Web ACL ARN（对于 WAFV2）的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

api-gwv2-access-logs-enabled

检查 Amazon API Gateway V2 阶段是否启用了访问日志功能。如果舞台配置中没有 “访问权限 LogSettings”，则该规则不兼容。

标识符：API_GWV2_ACCESS_LOGS_ENABLED

资源类型： AWS::ApiGatewayV2::Stage

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

api-gwv2-authorization-type-configured

检查 Amazon API Gatewayv2 API 路由是否设置了授权类型。如果授权类型为 NONE，则此规则为 NON_COMPLIANT。

标识符：API_GWV2_AUTHORIZATION_TYPE_CONFIGURED

资源类型： AWS::ApiGatewayV2::Route

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

authorizationType（可选），类型：字符串

用于检查 API 路由的授权类型的参数。与 CUSTOM、 AWS_IAM、JWT 匹配的字符串参数有效。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

api-gw-associated-with-waf

检查 Amazon API Gateway API 阶段是否在使用 AWS WAF 网络访问控制列表 (Web ACL)。如果未使用 AWS WAF Web ACL 或者使用的 Web ACL 与规则参数中列出的内容不匹配，则该规则不兼容。AWS

标识符：API_GW_ASSOCIATED_WITH_WAF

资源类型： AWS::ApiGateway::Stage

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

WebAclArns （可选），类型：CSV

Web ACL Amazon 资源名称 (ARN) 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

api-gw-cache-enabled-and-encrypted

检查 Amazon API Gateway 阶段中的所有方法是否都启用了缓存并对缓存进行了加密。如果 Amazon API Gateway 阶段中的任何方法未配置为缓存或者缓存未加密，则此规则为 NON_COMPLIANT。

标识符：API_GW_CACHE_ENABLED_AND_ENCRYPTED

资源类型： AWS::ApiGateway::Stage

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

api-gw-endpoint-type-check

检查 Amazon API Gateway API 是否属于规则参数 `endpointConfigurationType` 中指定的类型。如果 REST API 与规则参数中配置的终端节点类型不匹配，则规则返回 NON_COMPLIANT。

标识符：API_GW_ENDPOINT_TYPE_CHECK

资源类型： AWS::ApiGateway::RestApi

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

端点 ConfigurationTypes, 类型：字符串

> 以逗号分隔的允许列表。 endpointConfigurationTypes允许的值包括 REGIONAL、PRIVATE 和 EDGE。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

api-gw-execution-logging-enabled

检查 Amazon API Gateway 阶段中的所有方法是否均已启用日志记录。如果未启用日志记录，或者 `loggingLevel` 既不是 ERROR 也不是 INFO，则此规则为 NON_COMPLIANT。

标识符：API_GW_EXECUTION_LOGGING_ENABLED

资源类型： AWS::ApiGateway::Stage, AWS::ApiGatewayV2:: Stage

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

loggingLevel（可选），类型：字符串, 默认值：ERROR、INFO

特定日志记录级别的逗号分隔列表（例如，ERROR, INFO 或 ERROR,INFO）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

api-gw-ssl-enabled

检查 REST API 阶段是否使用 SSL 证书。如果 REST API 阶段没有关联的 SSL 证书，则此规则为 NON_COMPLIANT。

> **Note**
>
> `NOT_APPLICABLE`如果 GetIntegrationAPI 以类型形式返回`AWS`，则此规则返回。

标识符：API_GW_SSL_ENABLED

资源类型： AWS::ApiGateway::Stage

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

CertificateIDs（可选），类型：CSV

在 REST API 阶段配置的客户端证书 ID 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

api-gw-xray-enabled

检查 Amazon API Gateway REST API 上是否启用了 AWS X-REST 追踪。如果已启用 X-Ray 跟踪，则此规则为 COMPLIANT，否则为 NON_COMPLIANT。

标识符：API_GW_XRAY_ENABLED

资源类型： AWS::ApiGateway::Stage

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "TracingEnabled": BOOLEAN,
   "RestApiId": "my-rest-api-Id",
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

approved-amis-by-id

检查正在运行的 EC2 实例是否使用指定的亚马逊机器映像 (AMI)。指定批准的 AMI ID 的列表。其 AMI 不在此列表中的正在运行的实例为 NON_COMPLIANT。

标识符：APPROVED_AMIS_BY_ID

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

amiIds, 类型：CSV

AMI ID（逗号分隔列表，最多 21 个 AMI ID 或总共 1024 个字符，以先到者为准）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

approved-amis-by-tag

检查正在运行的实例是否使用指定的亚马逊机器映像 (AMI)。指定标识 AMI 的标签。其 AMI 未包含至少一个指定标签的正在运行的实例为 NON_COMPLIANT。

标识符：APPROVED_AMIS_BY_TAG

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

amis Value ByTag KeyAnd, 类型: StringMap, 默认：tag-key:tag-value,other-tag-key

按标签划分的 AMI（逗号分隔列表，最多 10 个；例如，`tag-key:tag-value`；即 `tag-key1` 与具有 `tag-key1` 的 AMI 匹配，`tag-key2:value2` 与具有 value2 的 `tag-key2` 匹配）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

appsync-associated-with-waf

检查 AWS AppSync API 是否与 AWS WAFv2 网络访问控制列表 (ACL) 关联。如果 AWS AppSync API 未与 Web ACL 关联，则该规则不合规。

标识符：APPSYNC_ASSOCIATED_WITH_WAF

资源类型： AWS::AppSync::GraphqlaPi

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

waf WebAcl ARN（可选）, 类型：CSV

授权 Web ACL 的 Amazon 资源名称 (ARN) 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

appsync-authorization-check

检查 AWS AppSync API 是否使用允许的授权机制。如果使用的是未经批准的授权机制，则此规则为 NON_COMPLIANT。

标识符：APPSYNC_AUTHORIZATION_CHECK

资源类型： AWS::AppSync::GraphqlaPi

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

AllowedAuthorization类型, 类型：CSV

以逗号分隔的允许 AWS AppSync 授权机制列表。允许的值是：“API_KEY”、“AWS_LAMBDA”、“AWS_IAM”、“OPENID_CONNECT”、“AMAZON_COGNITO_USER

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

appsync-cache-encryption-at-rest

检查 AWS AppSync API 缓存是否启用了静态加密。如果 “AtRestEncryptionEnabled” 为假，则此规则不合规。

标识符：APPSYNC_CACHE_ENCRYPTION_AT_REST

资源类型： AWS::AppSync::GraphqlaPi

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

appsync-logging-enabled

检查 AWS AppSync API 是否启用了日志记录。如果未启用日志记录，或者 “字段LogLevel” 既不是错误也不是全部，则该规则不兼容。

标识符：APPSYNC_LOGGING_ENABLED

资源类型： AWS::AppSync::GraphqlaPi

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

fieldLoggingLevel （可选）, 类型：CSV

特定字段日志记录级别的的逗号分隔列表（例如，ERROR, ALL）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

athena-workgroup-encrypted-at-rest

检查 Amazon Athena 工作组是否启用了静态加密。如果未为 Athena 工作组启用静态数据加密，则此规则为 NON_COMPLIANT。

标识符：ATHENA_WORKGROUP_ENCRYPTED_AT_REST

资源类型： AWS::Athena::WorkGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

aurora-last-backup-recovery-point-created

检查是否已为 Amazon Aurora 数据库集群创建了恢复点。如果 Amazon Relational Database Service (Amazon RDS) 数据库集群没有在指定时间段内创建相应的恢复点，则此规则为 NON_COMPLIANT。

标识符：AURORA_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型：AWS::RDS::DBCluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Aurora 数据库集群的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 Aurora 数据库集群的 ID。

恢复PointAgeValue （可选）, 类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit （可选）, 类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

aurora-meets-restore-time-target

检查 Amazon Aurora 数据库集群的还原时间是否符合指定的持续时间。如果 Aurora 数据库集群 LatestRestoreExecutionTimeMinutes 的大于 maxRestoreTime 分钟，则该规则不合规。

标识符：AURORA_MEETS_RESTORE_TIME_TARGET

资源类型：AWS::RDS::DBCluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大 RestoreTime, 类型：int

允许的最大还原运行时间的数值。

resourceTags（可选）, 类型：字符串

规则要检查的 Aurora 数据库集群的标签，采用 JSON 格式。

resourceId（可选）, 类型：字符串

此规则要检查的 Aurora 数据库集群的 ID。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

aurora-mysql-backtracking-enabled

检查 Amazon Aurora MySQL 集群是否启用了回溯功能。如果 Aurora 集群使用 MySQL 且未启用回溯功能，则此规则为 NON_COMPLIANT。

标识符：AURORA_MYSQL_BACKTRACKING_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域：仅适用于亚太地区（孟买）、欧洲（巴黎）、美国东部（俄亥俄州）、欧洲（爱尔兰）、欧洲（法兰克福）、美国东部（弗吉尼亚北部）、亚太地区（首尔）、欧洲（伦敦）、亚太地区（东京）、美国西部（俄勒冈）、美国西部（加利福尼亚北部）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）、中国（宁夏）、欧洲（苏黎世）区域

参数：

BacktrackWindowInHours （可选）, 类型：双精度

回溯 Aurora MySQL 集群的时间，以小时为单位（最多 72 小时）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

aurora-resources-protected-by-backup-plan

检查 Amazon Aurora 数据库集群是否受备份计划的保护。如果 Amazon Relational Database Service (Amazon RDS) 数据库集群未受备份计划保护，则此规则为 NON_COMPLIANT。

标识符：AURORA_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型：AWS::RDS::DBCluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Aurora 数据库集群的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 Aurora 数据库集群的 ID。

crossRegionList （可选）, 类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （可选）, 类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （可选）, 类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （可选）, 类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选）, 类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

autoscaling-capacity-rebalancing

检查使用多种实例类型的 Amazon EC2 Auto Scaling 组是否启用了容量再平衡。如果容量再平衡未启用，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_CAPACITY_REBALANCING

资源类型： AWS::AutoScaling::AutoScaling组

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

autoscaling-group-elb-healthcheck-required

检查与弹性负载均衡器关联的 Amazon EC2 Auto Scaling 组是否使用 Elastic Load Balancing 运行状况检查。如果 Amazon EC2 Auto Scaling 组未使用 Elastic Load Balancing 运行状况检查，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_GROUP_ELB_HEALTHCHECK_REQUIRED

资源类型： AWS::AutoScaling::AutoScaling组

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "LoadBalancerNames": "[my-load-balancer-1, my-load-balancer-2, my-load-balancer-3, ...]",
   "HealthCheckType": HealthCheckType*"
}
...
```

*有效值为 EC2（默认值）、ELB 和 VPC_LATTICE。VPC_LATTICE 运行状况检查类型专门保留以与预览版 VPC Lattice 结合使用，VPC Lattice 将来可能会发生变化。有关更多信息，请参阅《Amazon EC2 Auto Scaling 用户指南》中的 Auto Scaling 实例的运行状况检查。

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

autoscaling-launchconfig-requires-imdsv2

检查是否只启用了 IMDSv2。如果启动配置中未包含元数据版本，或者同时启用了元数据 V1 和 V2，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_LAUNCHCONFIG_REQUIRES_IMDSV2

资源类型： AWS::AutoScaling::LaunchConfiguration

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

autoscaling-launch-config-hop-limit

检查元数据令牌可以传输的网络跃点数。如果元数据响应跃点限制大于 1，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_LAUNCH_CONFIG_HOP_LIMIT

资源类型： AWS::AutoScaling::LaunchConfiguration

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

autoscaling-launch-config-public-ip-disabled

检查 Amazon EC2 Auto Scaling 组是否通过启动配置启用了公有 IP 地址。如果 Amazon EC2 Auto Scaling 组的启动配置已 AssociatePublicIpAddress 设置为 “true”，则该规则不合规。

标识符：AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED

资源类型： AWS::AutoScaling::LaunchConfiguration

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

autoscaling-launch-template

检查 Amazon Elastic Compute Cloud (EC2) Auto Scaling 组是否是根据 EC2 启动模板创建的。如果扩展组不是根据 EC2 启动模板创建的，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_LAUNCH_TEMPLATE

资源类型： AWS::AutoScaling::AutoScaling组

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

autoscaling-multiple-az

检查 Auto Scaling 组是否跨越多个可用区。如果 Auto Scaling 组不跨越多个可用区，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_MULTIPLE_AZ

资源类型： AWS::AutoScaling::AutoScaling组

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

minAvailabilityZones （可选），类型：int

预期可用区的最小数量。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

autoscaling-multiple-instance-types

检查 Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组是否使用多种实例类型。如果 Amazon EC2 Auto Scaling 组仅定义了一个实例类型，则此规则为 NON_COMPLIANT。

标识符：AUTOSCALING_MULTIPLE_INSTANCE_TYPES

资源类型： AWS::AutoScaling::AutoScaling组

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

backup-plan-min-frequency-and-min-retention-check

检查备份计划的备份规则是否满足所需的频率和保留期。如果创建恢复点的频率未达到指定频率，或在指定期限之前过期，则此规则为 NON_COMPLIANT。

标识符：BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK

资源类型： AWS::Backup::BackupPlan

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

requiredFrequencyValue （可选）, 类型：int, 默认值：1

所需备份频率的数值。最多 24 小时，或 31 天。

requiredRetentionDays （可选）, 类型：int, 默认值：35

以天为单位的所需保留期。

requiredFrequencyUnit （可选）, 类型：字符串, 默认值：days

所需备份频率的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

backup-recovery-point-encrypted

检查恢复点是否已加密。如果恢复点未加密，则此规则为 NON_COMPLIANT。

标识符：BACKUP_RECOVERY_POINT_ENCRYPTED

资源类型： AWS::Backup::RecoveryPoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

backup-recovery-point-manual-deletion-disabled

检查备份保管库是否附有防止删除恢复点的、基于资源的策略。如果 Backup Vault 没有基于资源的策略或策略没有合适的 “拒绝” 语句（带有 backup: DeleteRecovery Point、backup: 和 backup: 权限的语句）UpdateRecoveryPointLifecycle，则该规则不合规。PutBackupVaultAccessPolicy

标识符：BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED

资源类型： AWS::Backup::BackupVault

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

principalArnList （可选）, 类型：CSV

以逗号分隔的 AWS 身份和访问管理 (IAM) Amazon 资源名称 (ARN) 列表，供规则不要检查。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

backup-recovery-point-minimum-retention-check

检查恢复点的过期时间是否不早于指定时间段。如果恢复点的保留期短于所需的保留期，则此规则为 NON_COMPLIANT。

标识符：BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK

资源类型： AWS::Backup::RecoveryPoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

requiredRetentionDays （可选）, 类型：int, 默认值：35

以天为单位的所需保留期。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

beanstalk-enhanced-health-reporting-enabled

检查 E AWS lastic Beanstalk 环境是否已配置为增强型运行状况报告。如果环境配置为进行增强运行状况报告，则此规则为 COMPLIANT。如果环境配置为进行基本运行状况报告，则此规则为 NON_COMPLIANT。

标识符：BEANSTALK_ENHANCED_HEALTH_REPORTING_ENABLED

资源类型： AWS::ElasticBeanstalk::Environment

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

clb-desync-mode-check

检查经典负载均衡器 (CLB) 是否配置了用户定义的取消同步缓解模式。如果 CLB 取消同步缓解模式与用户定义的取消同步缓解模式不匹配，则此规则为 NON_COMPLIANT。

标识符：CLB_DESYNC_MODE_CHECK

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

desyncMode, 类型：CSV

值的逗号分隔列表。您最多可以选择两个。有效值包括“Defensive”、“Strictest”和“Monitor”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

clb-multiple-az

检查经典负载均衡器是否跨越多个可用区 (AZ)。如果经典负载均衡器跨越 2 个以下可用区，或未跨越 `minAvailabilityZones` 参数（如果提供）中提及的可用区数量，则此规则为 NON_COMPLIANT。

标识符：CLB_MULTIPLE_AZ

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

minAvailabilityZones （可选）, 类型：int

所需的最小预期可用区数量。有效值介于 2 到 10 之间，包括 2 和 10。如果未指定参数，则默认值为 2。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudformation-stack-drift-detection-check

检查 AWS CloudFormation (AWS CloudFormation) 堆栈的实际配置是否与预期配置不同或有所偏差。如果堆栈的一个或多个资源与其预期配置不同，则将堆栈视为已偏离。当堆栈偏差状态为 IN_SYNC 时，规则和堆栈都是 COMPLIANT。当堆栈偏离状态为 DRIFTED 时，规则为 NON_COMPLIANT。

> **Note**
>
> 此规则对您账户中的每个堆栈执行 DetectStackDrift 操作。该 DetectStackDrift 操作最多可能需要几分钟，具体取决于堆栈中包含的资源数量。鉴于此规则的最长执行时间限制为 15 分钟，因此此规则可能会在完成对您账户中所有堆栈的评估之前超时。
> 如果您遇到此问题，建议您使用标签来限制规则范围内的堆栈数量。您可执行以下操作：
>
> 1. 将您的堆栈分成几组，每个组有一个不同的标签。
> 2. 将相同的标签应用于该组中的所有堆栈。
> 3. 在您的账户中设置此规则的多个实例，每个实例使用不同的标签。这允许规则的每个实例仅处理具有其作用域中提及的相应标签的堆栈。

标识符：CLOUDFORMATION_STACK_DRIFT_DETECTION_CHECK

资源类型： AWS::CloudFormation::Stack

触发器类型：配置更改和定期

AWS 区域: 所有支持的 AWS 区域

参数：

云层形成 RoleArn, 类型：字符串

具有策略权限的 IAM 角色的 Amazon 资源名称 (ARN)，用于检测堆栈偏差。 AWS CloudFormation 有关该角色所需 IAM 权限的信息，请参阅 AWS CloudFormation 用户指南中的检测堆栈和资源的非托管配置更改 | 检测偏差时的注意事项。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudformation-stack-notification-check

检查您的 CloudFormation 堆栈是否向 Amazon SNS 主题发送事件通知。还可以检查是否使用了指定的 Amazon SNS 主题。如果 CloudFormation 堆栈不发送通知，则该规则不合规。

标识符：CLOUDFORMATION_STACK_NOTIFICATION_CHECK

资源类型： AWS::CloudFormation::Stack

触发器类型： 配置更改

AWS 区域：仅适用于中国（北京）、亚太地区（孟买）、美国东部（俄亥俄州）、欧洲（爱尔兰）、欧洲（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚北部）、亚太地区（首尔）、欧洲（伦敦）、亚太地区（东京）、美国西部（俄勒冈）、美国西部（加利福尼亚北部）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）、中国（宁夏）) 区域

参数：

snsTopic1（可选）, 类型：字符串

SNS 主题 ARN。

snsTopic2（可选）, 类型：字符串

SNS 主题 ARN。

snsTopic3（可选）, 类型：字符串

SNS 主题 ARN。

snsTopic4（可选）, 类型：字符串

SNS 主题 ARN。

snsTopic5（可选）, 类型：字符串

SNS 主题 ARN。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-accesslogs-enabled

检查 Amazon CloudFront 分配是否配置为向 Amazon S3 存储桶传输访问日志。如果 CloudFront 分配未配置日志记录，则该规则为 NON_Complift。

标识符：CLOUDFRONT_ACCESSLOGS_ENABLED

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

S3BucketName （可选），类型：字符串

访问服务器访问日志所用的 Amazon S3 存储桶的名称。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-associated-with-waf

检查亚马逊 CloudFront 发行版是否与网络应用程序防火墙 (WAF) 或 WAFv2 网络访问控制列表 (ACL) 关联。如果 CloudFront 分配未与 WAF Web ACL 关联，则该规则不兼容。

标识符：CLOUDFRONT_ASSOCIATED_WITH_WAF

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

wafWebAclIds （可选），类型：CSV

WAF 的 Web ACL ID 或 WAFV2 的 Web ACL Amazon 资源名称 (ARN) 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-custom-ssl-certificate

检查与 Amazon CloudFront 分配关联的证书是否为默认 SSL 证书。如果 CloudFront 分配使用默认 SSL 证书，则该规则不兼容。

标识符：CLOUDFRONT_CUSTOM_SSL_CERTIFICATE

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-default-root-object-configured

检查 Amazon CloudFront 分配是否配置为返回默认根对象的特定对象。如果 Amazon CloudFront 分发没有配置默认根对象，则该规则不合规。

标识符：CLOUDFRONT_DEFAULT_ROOT_OBJECT_CONFIGURED

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-no-deprecated-ssl-protocols

检查 CloudFront 分发是否使用已弃用的 SSL 协议进行 CloudFront 边缘站点和自定义源站之间的 HTTPS 通信。如果任何 “OriginSsl协议” 包含 “slv3”，则此规则不符合 CloudFront 发行版。

标识符：CLOUDFRONT_NO_DEPRECATED_SSL_PROTOCOLS

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-origin-access-identity-enabled

检查使用 Amazon S3 Origin 类型的 CloudFront 分配是否配置了源站访问身份。如果 CloudFront 分配由 S3 支持且任何源类型未配置 OAI，或者源不是 S3 存储桶，则该规则不合规。

> **Note**
>
> 如果源不是 S3 存储桶，则规则不会返回 NOT_APPLICABLE。

标识符：CLOUDFRONT_ORIGIN_ACCESS_IDENTITY_ENABLED

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-origin-failover-enabled

检查是否将一个起源组配置为分配亚马逊源组中至少两个起源 CloudFront。如果该分配没有源组，则此规则为 NON_COMPLIANT。

标识符：CLOUDFRONT_ORIGIN_FAILOVER_ENABLED

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-s3-origin-access-control-enabled

检查使用亚马逊简单存储服务 (Amazon S3) Service Origin 类型的亚马逊 CloudFront 配送是否启用了源站访问控制 (OAC)。对于源自 Amazon S3 但未启用 OAC 的 CloudFront 分配，该规则不合规。

标识符：CLOUDFRONT_S3_ORIGIN_ACCESS_CONTROL_ENABLED

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-s3-origin-non-existent-bucket

检查 Amazon CloudFront 分配是否指向不存在的 S3 存储桶。如果 CloudFront 分发点指向不存在的 S3 OriginConfig 存储桶，则该规则不合规。此规则不评估使用静态网站托管的 S3 存储桶。

标识符：CLOUDFRONT_S3_ORIGIN_NON_EXISTENT_BUCKET

资源类型： AWS::CloudFront::Distribution

触发器类型： 定期

AWS 区域：仅在中国（北京）和美国东部（弗吉尼亚州北部）区域内提供

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-security-policy-check

检查 Amazon CloudFront 发行版是否使用最低安全策略和 TLSv1.2 或更高版本的密码套件进行查看者连接。如果 CloudFront 发行版低于 TLSV1.2_2018，则此规则 minimumProtocolVersion 不合规。

标识符：CLOUDFRONT_SECURITY_POLICY_CHECK

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-sni-enabled

检查亚马逊 CloudFront 分发是否使用自定义 SSL 证书，以及是否配置为使用 SNI 来处理 HTTPS 请求。如果关联了自定义 SSL 证书，但 SSL 支持方法是专用 IP 地址，则此规则为 NON_COMPLIANT。

标识符：CLOUDFRONT_SNI_ENABLED

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-traffic-to-origin-encrypted

检查 Amazon CloudFront 分配是否正在加密流向自定义来源的流量。如果 “OriginProtocol策略” 为 “仅限 http”，或者 “策略” 为 “匹配查看器” 且 “OriginProtocol政策” 为 “allow-all”，则该规则不合规。ViewerProtocol

标识符：CLOUDFRONT_TRAFFIC_TO_ORIGIN_ENCRYPTED

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudfront-viewer-policy-https

检查您的 Amazon CloudFront 分配是否使用 HTTPS（直接使用或通过重定向）。如果将或的值设置 ViewerProtocolPolicy 为 “allow-all”，则该 DefaultCacheBehavior 规则不合规。 CacheBehaviors

标识符：CLOUDFRONT_VIEWER_POLICY_HTTPS

资源类型： AWS::CloudFront::Distribution

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudtrail-all-read-s3 数据事件检查

检查是否启用了 AWS CloudTrail 多区域跟踪，并记录存储桶的所有读取 S3 数据事件。如果没有多区域跟踪记录所有当前和未来 S3 存储桶的所有读取 S3 数据事件类型，则该规则不合规。

标识符：CLOUDTRAIL_ALL_READ_S3_DATA_EVENT_CHECK

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudtrail-all-write-s3 数据事件检查

检查是否启用了 AWS CloudTrail 多区域跟踪，并记录存储桶的所有写入 S3 数据事件。如果没有多区域跟踪记录所有当前和未来的 S3 存储桶的所有写入 S3 数据事件类型，则该规则不合规。

标识符：CLOUDTRAIL_ALL_WRITE_S3_DATA_EVENT_CHECK

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudtrail-s3 存储桶访问日志

检查您的 AWS CloudTrail 日志的 S3 存储桶配置是否启用了 Amazon S3 服务器访问日志记录。如果 CloudTrail 跟踪的至少一个 S3 存储桶未启用 S3 服务器访问日志记录，则该规则不合规。

标识符：CLOUDTRAIL_S3_BUCKET_AC CESS_LOG

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudtrail-s3 bucket-bucket-禁止公共访问

检查您的 AWS CloudTrail 日志的 S3 存储桶配置是否阻止了公共访问。如果 CloudTrail 跟踪中至少有一个可公开访问的 S3 存储桶，则该规则为 NON_Complift。

标识符：CLOUDTRAIL_S3_BUCKET_BUCKET_PUBLIC_

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudtrail-s3-dataevents-enabled

检查是否至少有一个 AWS CloudTrail 跟踪记录了所有 S3 存储桶的亚马逊简单存储服务 (Amazon S3) Service 数据事件。如果有跟踪或者没有跟踪记录 S3 数据事件，则此规则为 NON_COMPLIANT。

标识符：CLOUDTRAIL_S3_DATAEVENTS_ENABLED

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

S3BucketNames （可选），类型：字符串

逗号分隔的 S3 存储桶名称列表，应为其启用数据事件日志记录。默认行为会检查所有 S3 存储桶。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudtrail-security-trail-enabled

检查是否至少有一 AWS CloudTrail 条使用安全最佳实践定义的跟踪。如果至少有一个跟踪满足以下所有条件，则此规则为 COMPLIANT：

- 记录全局服务事件
- 是一个多区域跟踪
- 已启用日志文件验证
- 使用 KMS 密钥加密
- 记录读取和写入事件
- 记录管理事件
- 不排除任何管理事件

如果没有跟踪符合上述所有条件，则此规则为 NON_COMPLIANT。

标识符：CLOUDTRAIL_SECURITY_TRAIL_ENABLED

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudwatch-alarm-action-check

检查 CloudWatch 警报是否为 “警报”、“数据不足” 或 “正常” 状态配置了操作。（可选）检查是否有任何操作与指定 ARN 匹配。如果没有为警报或可选参数指定任何操作，则此规则为 NON_COMPLIANT。

标识符：CLOUDWATCH_ALARM_ACTION_CHECK

资源类型： AWS::CloudWatch::Alarm

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

警报 ActionRequired, 类型：字符串, 默认：True

警报具有至少一个操作。

不足DataAction必须, 类型：字符串, 默认：True

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

好的 ActionRequired, 类型：字符串, 默认：false

当警报从任意其他状态转换为 OK 状态时，警报至少有一个操作。

action1（可选）, 类型：字符串

要执行的操作，指定为 ARN。

action2（可选）, 类型：字符串

要执行的操作，指定为 ARN。

action3（可选）, 类型：字符串

要执行的操作，指定为 ARN。

action4（可选）, 类型：字符串

要执行的操作，指定为 ARN。

action5（可选）, 类型：字符串

要执行的操作，指定为 ARN。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudwatch-alarm-action-enabled-check

检查 Amazon CloudWatch 警报操作是否处于启用状态。如果 CloudWatch 警报操作未处于启用状态，则该规则为 “不合规”。

标识符：CLOUDWATCH_ALARM_ACTION_ENABLED_CHECK

资源类型： AWS::CloudWatch::Alarm

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudwatch-alarm-resource-check

检查资源类型是否有针对指定指标的 CloudWatch 警报。对于资源类型，您可以指定 EBS 卷、EC2 实例、Amazon RDS 集群或 S3 存储桶。如果指定指标具有资源 ID 和 CloudWatch 警报，则该规则合规。

标识符：CLOUDWATCH_ALARM_RESOURCE_CHECK

资源类型： AWS::EC2::Instance、 AWS::RDS::DBCluster, AWS::S3::Bucket、 AWS::EC2::Volume

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceType, 类型：字符串

AWS 资源类型。该值可以是以下值之一： AWS::EC2::Volume、 AWS::EC2::Instance、AWS::RDS::DBCluster, or AWS::S3::Bucket。

metricName, 类型：字符串

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

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudwatch-alarm-settings-check

检查具有给定指标名称的 CloudWatch 警报是否具有指定的设置。

标识符：CLOUDWATCH_ALARM_SETTINGS_CHECK

资源类型： AWS::CloudWatch::Alarm

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

metricName, 类型：字符串

与警报关联的指标的名称。

threshold（可选）, 类型：int

指定统计数据的比较值。

evaluationPeriods（可选）, 类型：int

其间的数据将与指定阈值进行比较的期间数。

period（可选）, 类型：int, 默认：300

在其中应用指定统计数据的期间 (秒数)。

comparisonOperator（可选）, 类型：字符串

用于比较指定统计数据和阈值的操作（例如，“GreaterThan阈值”）。

statistic（可选），类型：字符串

与警报关联的指标的统计数据（例如，“Average”或“Sum”）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudwatch-log-group-encrypted

检查 Amazon CloudWatch 日志组是否使用任何 AWS KMS 密钥或指定的 K AWS MS 密钥 ID 进行加密。如果 CloudWatch 日志组未使用 KMS 密钥加密，或者使用规则参数中未提供的 KMS 密钥进行加密，则该规则不合规。

标识符：CLOUDWATCH_LOG_GROUP_ENCRYPTED

资源类型： AWS::Logs::LogGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

KmsKeyId （可选），类型：字符串

用于加密日志组的 KMS 密钥的 ID 的 Amazon 资源名称 (ARN)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloud-trail-cloud-watch-logs-enabled

检查是否将 AWS CloudTrail 跟踪配置为向日志发送 CloudWatch 日志。如果跟踪的 CloudWatchLogsLogGroupArn 属性为空，则该跟踪不兼容。

标识符：CLOUD_TRAIL_CLOUD_WATCH_LOGS_ENABLED

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

预期DeliveryWindowAge （可选），类型：int

最近一次向符合合规性的 CloudWatch 日志交付的最大时长（以小时为单位）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloudtrail-enabled

> **Important**
>
> 对于此规则，规则标识符 (CLOUD_TRAIL_ENABLED) 和规则名称 (cloudtrail-enabled) 是不同的。

检查您的 AWS 账户中是否启用了 AWS CloudTrail 跟踪。如果跟踪未启用，则规则为 NON_COMPLIANT。或者，该规则会检查特定的 S3 存储桶、亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题和日志组 CloudWatch 。

标识符：CLOUD_TRAIL_ENABLED

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

s3BucketName （可选），类型：字符串

用于 CloudTrail 向其传送日志文件的 S3 存储桶的名称。

snsTopicArn （可选），类型：字符串

CloudTrail 用于通知的 SNS 主题 ARN。

云WatchLogsLogGroupArn （可选），类型：字符串

CloudWatch CloudTrail 要向其发送数据的日志组 ARN。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloud-trail-encryption-enabled

检查 AWS CloudTrail 是否配置为使用服务器端加密 (SSE) AWS Key Management Service (AWS KMS) 加密。如果定义了，则该规则 KmsKeyId 是合规的。

标识符：CLOUD_TRAIL_ENCRYPTION_ENABLED

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cloud-trail-log-file-validation-enabled

检查是否 AWS CloudTrail 创建了带有日志的签名摘要文件。 AWS 建议必须在所有轨迹上启用文件验证。如果未启用验证，则此规则为 NON_COMPLIANT。

标识符：CLOUD_TRAIL_LOG_FILE_VALIDATION_ENABLED

资源类型： AWS::CloudTrail::Trail

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cmk-backing-key-rotation-enabled

检查是否为每个密钥启用了自动密钥轮换，并与客户创建的 KMS 密钥的密 AWS 钥 ID 相匹配。如果资源的 Confi AWS g 记录器角色没有 kms: DescribeKey 权限，则该规则不兼容。

> **Note**
>
> 对于非对称 KMS 密钥、HMAC KMS 密钥、带有导入密钥材料的 KMS 密钥或自定义密钥存储区中的 KMS 密钥，不支持自动密钥轮换。

标识符：CMK_BACKING_KEY_ROTATION_ENABLED

资源类型： AWS::KMS::Key

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codebuild-project-artifact-encryption

检查 AWS CodeBuild 项目是否为其所有构件启用了加密。如果任何主要或次要（如果存在）构件配置的“encryptionDisabled”设置为“true”，则此规则为 NON_COMPLIANT。

标识符：CODEBUILD_PROJECT_ARTIFACT_ENCRYPTION

资源类型： AWS::CodeBuild::Project

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codebuild-project-environment-privileged-check

检查 AWS CodeBuild 项目环境是否启用了特权模式。如果 “权限模式” 设置为 “true”，则 CodeBuild 该项目规则不合规。

标识符：CODEBUILD_PROJECT_ENVIRONMENT_PRIVILEGED_CHECK

资源类型： AWS::CodeBuild::Project

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

exemptedProjects（可选），类型：CSV

允许具有 “权限模式” 且值为 “true” 的 CodeBuild 项目名称的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codebuild-project-envvar-awscred-check

检查项目是否包含环境变量 AWS_ACCESS_KEY_ID 和 _SECRET_ACCESS_KEY。 AWS如果项目环境变量包含明文凭证，则此规则为 NON_COMPLIANT。

标识符：CODBUILD_PROJECT_ENVVAR_ AWSCRED_CHECK

资源类型： AWS::CodeBuild::Project

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codebuild-project-logging-enabled

检查 AWS CodeBuild 项目环境是否至少启用了一个日志选项。如果所有现有日志配置的状态都设置为“DISABLED”，则此规则为 NON_COMPLIANT。

标识符：CODEBUILD_PROJECT_LOGGING_ENABLED

资源类型： AWS::CodeBuild::Project

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

s3BucketNames （可选），类型：字符串

逗号分隔的 Amazon S3 存储桶名称列表，如果配置了 S3 日志，则应将日志发送到这些存储桶。

云WatchGroupNames （可选），类型：字符串

以逗号分隔的 Amazon CloudWatch 日志组名称列表，如果配置了日志，则应将 CloudWatch 日志发送到这些名称。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codebuild-project-s3-logs-encrypted

检查配置了 Amazon S3 日志的 AWS CodeBuild 项目是否为其日志启用了加密。如果在项目的 S3 LogsConfig 中将 “encryptionDisabled” 设置为 “true”，则该规则不合规。 CodeBuild

标识符：CODEBUILD_PROJECT_S3_LOGS_ENCRYPTED

资源类型： AWS::CodeBuild::Project

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

exemptedProjects（可选），类型：CSV

允许输出未加密日志的 CodeBuild 项目名称列表，以逗号分隔。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codebuild-project-source-repo-url-check

检查 Bitbucket 源存储库 URL 是否包含登录凭证。如果 URL 包含任何登录信息，则此规则为 NON_COMPLIANT；如果不包含任何登录信息，则此规则为 COMPLIANT。

标识符：CODEBUILD_PROJECT_SOURCE_REPO_URL_CHECK

资源类型： AWS::CodeBuild::Project

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codedeploy-auto-rollback-monitor-enabled

检查部署组是否配置了自动部署回滚和附带警报的部署监控。如果 AutoRollbackConfiguration 或 AlarmConfiguration 尚未配置或未启用，则该规则不兼容。

标识符：CODEDEPLOY_AUTO_ROLLBACK_MONITOR_ENABLED

资源类型： AWS::CodeDeploy::DeploymentGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codedeploy-ec2-minimum-healthy-hosts-configured

检查 EC2/本地计算平台的部署组配置的运行正常的主机队列最小百分比或主机数量是否大于等于输入阈值。如果任一项低于阈值，则此规则为 NON_COMPLIANT。

标识符：CODEDEPLOY_EC2_MINIMUM_HEALTHY_HOSTS_CONFIGURED

资源类型： AWS::CodeDeploy::DeploymentGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

最低HealthyHostsFleetPercent （可选），类型：int, 默认值：66

部署期间，队列中运行正常的主机的最低百分比。默认值设置为 66%。

最低HealthyHostsHostCount （可选），类型：int, 默认值：1

部署期间，队列中运行正常的主机的最小数量。默认值设置为 1。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codedeploy-lambda-allatonce-traffic-shift-disabled

检查 Lambda 计算平台的部署组是否未使用默认部署配置。如果部署组使用部署配置 “默认”CodeDeploy，则该规则不兼容。 LambdaAllAtOnce'。

标识符：CODEDEPLOY_LAMBDA_ALLATONCE_TRAFFIC_SHIFT_DISABLED

资源类型： AWS::CodeDeploy::DeploymentGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codepipeline-deployment-count-check

检查的第一个部署阶段是否 AWS CodePipeline 执行了多个部署。（可选）检查后续剩余阶段的每个部署是否都超过指定的部署数量 (`deploymentLimit`)。

标识符：CODEPIPELINE_DEPLOYMENT_COUNT_CHECK

资源类型： AWS::CodePipeline::Pipeline

触发器类型： 配置更改

AWS 区域：仅在以下区域提供：亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、亚太地区（首尔）、欧洲地区（伦敦）、亚太地区（东京)、美国西部（俄勒冈州）、美国西部（北加利福尼亚）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）。

参数：

deploymentLimit（可选），类型：int

每个阶段可执行的部署的最大数目。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

codepipeline-region-fanout-check

检查每个阶段 AWS CodePipeline 部署的区域数量是否超过之前所有合并阶段中部署的 AWS CodePipeline 区域数量的 N 倍，其中 N 是区域扇出数字。第一个部署阶段可以部署到最多一个区域，第二个部署阶段可以部署到 `regionFanoutFactor` 中指定的最大数量的区域。如果未提供 `regionFanoutFactor`，则默认情况下，该值为 3。例如：如果第一个部署阶段部署到 1 个区域，第二个部署阶段部署到 3 个区域，则第三个部署阶段可以部署到 12 个区域，即前面阶段的总和乘以区域扇出数 (3)。如果在第一阶段部署在多个区域，在第二阶段部署在 3 个区域或在第三阶段部署在 12 个区域，则此规则为 NON_COMPLIANT。

标识符：CODEPIPELINE_REGION_FANOUT_CHECK

资源类型： AWS::CodePipeline::Pipeline

触发器类型： 配置更改

AWS 区域：仅在以下区域提供：亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、亚太地区（首尔）、欧洲地区（伦敦）、亚太地区（东京)、美国西部（俄勒冈州）、美国西部（北加利福尼亚）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）。

参数：

regionFanoutFactor （可选）, 类型：int, 原定设置值：3

在之前的所有阶段中部署到的区域数量是任何阶段可以部署到的可接受区域数量。 AWS CodePipeline

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

custom-eventbus-policy-attached

检查 Amazon EventBridge 自定义事件总线是否附加了基于资源的策略。如果自定义事件总线策略没有附加基于资源的策略，则此规则为 NON_COMPLIANT。

标识符：CUSTOM_EVENTBUS_POLICY_ATTACHED

资源类型： AWS::Events::EventBus

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

custom-schema-registry-policy-attached

检查自定义 Amazon EventBridge 架构注册表是否附加了资源政策。对于未附加资源策略的自定义架构注册表，规则为 NON_COMPLIANT。

标识符：CUSTOM_SCHEMA_REGISTRY_POLICY_ATTACHED

资源类型： AWS::EventSchemas::Registry

触发器类型： 定期

AWS 区域：仅适用于欧洲（斯德哥尔摩）、亚太地区（孟买）、欧洲（巴黎）、美国东部（俄亥俄州）、欧洲（爱尔兰）、欧洲（法兰克福）、南美洲（圣保罗）、亚太地区（香港）、美国东部（弗吉尼亚北部）、亚太地区（首尔）、欧洲（伦敦）、亚太地区（东京）、美国西部（俄勒冈）、美国西部（加利福尼亚北部）、亚太地区（新加坡）、亚太地区（新加坡）、亚太地区（伦敦）、亚太地区（东京）、美国西部（俄勒冈）、美国西部（加利福尼亚北部）、亚太地区（新加坡）、亚太地区（新加坡）、亚太地区（伦敦）、亚太地区（东京）、美国西部（（悉尼）、加拿大（中部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

cw-loggroup-retention-period-check

检查 Amazon CloudWatch LogGroup 保留期是否设置为大于 365 天，或者是否设置为指定的保留期。如果保留期小于（如果指定），则该规则不合规`MinRetentionTime`，否则为 365 天。

> **Note**
> 如果日志组的保留设置为“永不过期”，则此规则将被标记为 COMPLIANT。

标识符：CW_LOGGROUP_RETENTION_PERIOD_CHECK

资源类型： AWS::Logs::LogGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

LogGroupNames （可选），类型：CSV

要检查保留期的日志组名称的逗号分隔列表。

MinRetentionTime （可选），类型：int

指定保留时间。有效值为：
1、3、5、7、14、30、60、90、120、150、180、365、400、545、731、1827 和 3653。默认保留期为 365 天。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dax-encryption-enabled

检查 Amazon DynamoDB Accelerator (DAX) 集群是否已加密。如果 DAX 集群未加密，则此规则为 NON_COMPLIANT。

标识符：DAX_ENCRYPTION_ENABLED

资源类型： AWS::DAX::Cluster

触发器类型： 定期

AWS 区域：仅在以下区域提供：亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、欧洲地区（伦敦）、亚太地区（东京)、美国西部（俄勒冈州）、美国西部（北加利福尼亚）、亚太地区（新加坡）、亚太地区（悉尼）

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dax-tls-端点加密

检查您的亚马逊 DynamoDB 加速器 (DAX) 集群是否 ClusterEndpointEncryptionType 已设置为 TLS。如果 DAX 集群未通过传输层安全 (TLS) 加密，则该规则不合规。

标识符：DAX_TLS_端点_加密

资源类型： AWS::DAX::Cluster

触发器类型： 定期

AWS 区域：仅在以下区域提供：亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、欧洲地区（伦敦）、亚太地区（东京)、美国西部（俄勒冈州）、美国西部（北加利福尼亚）、亚太地区（新加坡）、亚太地区（悉尼）

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

db-instance-backup-enabled

检查 RDS 数据库实例是否已启用备份。（可选）此规则将检查备份保留期和备份时段。

标识符：DB_INSTANCE_BACKUP_ENABLED

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

backupRetentionPeriod （可选）, 类型：int

备份的保留期。

backupRetentionMinimum （可选）, 类型：int

备份的最短保留期。

preferredBackupWindow （可选）, 类型：字符串

创建备份的时间范围。

checkReadReplicas （可选）, 类型：布尔值

检查 RDS 数据库实例是否已针对只读副本启用备份。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

desired-instance-tenancy

检查 EC2 实例的“tenancy”值。还检查 AMI ID 是否指定从这些 AMI 启动，或者主机 ID 是否在这些专属主机上启动。如果实例与列表中的主机和 AMI（如果指定）匹配，则此规则为 COMPLIANT。

标识符：DESIRED_INSTANCE_TENANCY

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

租期, 类型：字符串

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

imageId（可选）, 类型：CSV

规则仅评估从具有指定 ID 的 AMI 启动的实例。用英文逗号分隔多个 AMI ID。

hostId（可选）, 类型：CSV

EC2 专属主机的 ID，要在该主机上启动实例。用英文逗号分隔多个主机 ID。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

desired-instance-type

检查 EC2 实例是否属于特定的实例类型。如果参数列表中未指定 EC2 实例，则此规则为 NON_COMPLIANT。有关支持的 EC2 实例类型的列表，请参阅《适用于 Linux 实例的 EC2 用户指南》中的“实例类型”。

标识符：DESIRED_INSTANCE_TYPE

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

instanceType, 类型：CSV

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

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dms-auto-minor-version-upgrade-check

检查 AWS 数据库迁移服务 (AWS DMS) 复制实例是否启用了自动次要版本升级。如果 AWS DMS 复制实例未配置自动次要版本升级，则该规则不合规。

标识符：DMS_AUTO_MINOR_VERSION_UPGRADE_CHECK

资源类型： AWS::DMS::ReplicationInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dms-endpoint-ssl-configured

检查 AWS 数据库迁移服务 (AWS DMS) 端点是否配置了 SSL 连接。如果 AWS DMS 未配置 SSL 连接，则该规则不合规。

标识符：DMS_ENDPOINT_SSL_CONFIGURED

资源类型： AWS::DMS::Endpoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 dms-mongo-db 身份验证

检查 MongoDb 数据存储的AWS D AWS atabase Migration Service (DMS) 端点是否已启用基于密码的身份验证和访问控制。如果未启用基于密码的身份验证和访问控制，则该规则不兼容。

标识符：DMS_MONGO_DB_Authentication _ENABLED

资源类型： AWS::DMS::Endpoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 dms-neptune-iam 授权

检查 Amazon Neptune AWS 数据库的数据库迁移服务 (AWS DMS) 终端节点是否配置了 IAM 授权。如果以 Neptune 为目标的 AWS DMS 端点设置为 false，则该规则不兼容。 IamAuthEnabled

标识符：DMS_NEPTUNE_IAM_AUTHORIZAT ION_ENABLED

资源类型： AWS::DMS::Endpoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

启用 dms-redis-tls

检查 Redis 数据存储的AWS Dat AWS abase Migration Service (DMS) 端点是否已启用，以便对与其他端点通信的数据进行 TLS/SSL 加密。如果未启用 TLS/SSL 加密，则该规则不兼容。

标识符：DMS_REDIS_TLS_ ENABLED

资源类型： AWS::DMS::Endpoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dms-replication-not-public

检查 AWS 数据库迁移服务 (AWS DMS) 复制实例是否为公共实例。如果 PubliclyAccessible 字段设置为 true，则该规则不兼容。

标识符： DMS_REPLICATION_NOT_PUBLIC

资源类型： AWS::DMS::ReplicationInstance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dms-replication-task-sourcedb-logging

检查是否为源数据库的 AWS DMS 复制任务启用了有效的严重性级别的日志记录。如果未启用日志记录或源数据库的 DMS 复制任务的日志的严重性级别无效，则此规则为 NON_COMPLIANT。

标识符：DMS_REPLICATION_TASK_SOURCEDB_LOGGING

资源类型： AWS::DMS::ReplicationTask

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dms-replication-task-targetdb-logging

检查是否为目标数据库的 AWS DMS 复制任务事件启用了有效的严重性级别的日志记录。如果未启用日志记录或目标数据库的复制任务日志记录的严重性级别无效，则此规则为 NON_COMPLIANT。

标识符：DMS_REPLICATION_TASK_TARGETDB_LOGGING

资源类型： AWS::DMS::ReplicationTask

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

docdb-cluster-audit-logging-enabled

检查 Amazon DocumentDB（兼容 MongoDB）实例集群是否为审计日志启用了 CloudWatch 日志导出功能。如果 Amazon DocumentDB 实例集群 CloudWatch 没有为审计日志启用日志导出功能，则该规则不合规。

标识符：DOCDB_CLUSTER_AUDIT_LOGGING_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域：仅在以下区域提供：亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、亚太地区（首尔）、欧洲地区（伦敦）、欧洲地区（米兰）、亚太地区（东京)、美国西部（俄勒冈州）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）、中国（宁夏）

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

docdb-cluster-backup-retention-check

检查 Amazon Document 数据库集群的保留期是否设置为特定的天数。如果保留期小于参数指定的值，则此规则为 NON_COMPLIANT。

标识符：DOCDB_CLUSTER_BACKUP_RETENTION_CHECK

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域：仅在以下区域提供：亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、亚太地区（首尔）、欧洲地区（伦敦）、欧洲地区（米兰）、亚太地区（东京)、美国西部（俄勒冈州）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）、中国（宁夏）

参数：

最低BackupRetentionPeriod （可选）, 类型：int

备份应保留最少天数。有效值为 1 到 35，默认值为 7。如果值大于 “RetentionPeriod备份”，则此规则不合规。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

docdb-cluster-deletion-protection-enabled

检查 Amazon DocumentDB（与 MongoDB 兼容）集群是否启用了删除保护。如果 Amazon DocumentDB 集群的 deletionProtection 字段设置为 false，则此规则为 NON_COMPLIANT。

标识符：DOCDB_CLUSTER_DELETION_PROTECTION_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域：仅在以下区域提供：亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、亚太地区（首尔）、欧洲地区（伦敦）、欧洲地区（米兰）、亚太地区（东京)、美国西部（俄勒冈州）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）、中国（宁夏）

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

docdb-cluster-encrypted

检查您的 Amazon DocumentDB（与 MongoDB 兼容）集群是否启用了存储加密。如果未启用存储加密，则此规则为 NON_COMPLIANT。

标识符：DOCDB_CLUSTER_ENCRYPTED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域：仅在以下区域提供：亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、亚太地区（首尔）、欧洲地区（伦敦）、欧洲地区（米兰）、亚太地区（东京)、美国西部（俄勒冈州）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）、中国（宁夏）

参数：

kmsKeyArns （可选），类型：CSV

以逗号分隔的 KMS 密钥 ARN 列表，用于与加密集群的 KmsKey ID 进行比较。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

docdb-cluster-snapshot-public-prohibited

检查 Amazon DocumentDB 手动集群快照是否为公开快照。如果任何 Amazon DocumentDB 手动集群快照是公开快照，则此规则为 NON_COMPLIANT。

标识符：DOCDB_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

资源类型：AWS:: RDS:: DB ClusterSnapshot

触发器类型： 配置更改

AWS 区域：仅在以下区域提供：亚太地区（孟买）、欧洲地区（巴黎）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、亚太地区（首尔）、欧洲地区（伦敦）、欧洲地区（米兰）、亚太地区（东京)、美国西部（俄勒冈州）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-autoscaling-enabled

检查 Amazon DynamoDB 表或全局二级索引是否可以使用按需模式或启用自动扩缩的预置模式处理读/写容量。如果在未启用自动扩缩的情况下使用任一模式，则此规则为 NON_COMPLIANT

标识符：DYNAMODB_AUTOSCALING_ENABLED

资源类型： AWS::DynamoDB::Table

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

分钟ProvisionedReadCapacity （可选）, 类型：int

应在自动扩缩组中对读取容量配置的最小单位数。

最大ProvisionedReadCapacity （可选）, 类型：int

应在自动扩缩组中对读取容量配置的最大单位数。

targetReadUtilization （可选）, 类型：双精度

读取容量的目标使用率百分比。目标使用率以占用容量与预置容量的比值来表示。

分钟ProvisionedWriteCapacity （可选）, 类型：int

应在自动扩缩组中对写入容量配置的最小单位数。

最大ProvisionedWriteCapacity （可选）, 类型：int

应在自动扩缩组中对写入容量配置的最大单位数。

targetWriteUtilization （可选）, 类型：双精度

写入容量的目标使用率百分比。目标使用率以占用容量与预置容量的比值来表示。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-in-backup-plan

检查备份计划中是否有 Amazon DynamoDB 表。 AWS 如果任何备份计划中都没有 Amazon DynamoDB 表，则该规则不合规。 AWS

标识符：DYNAMODB_IN_BACKUP_PLAN

资源类型： AWS::DynamoDB::Table

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-last-backup-recovery-point-created

检查是否在指定时间段内为 Amazon DynamoDB 表创建了恢复点。如果 DynamoDB 表没有在指定时间段内创建相应的恢复点，则此规则为 NON_COMPLIANT。

标识符：DYNAMODB_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型： AWS::DynamoDB::Table

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 DynamoDB 表的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 DynamoDB 表的名称。

恢复PointAgeValue （可选）, 类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit （可选）, 类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-meets-restore-time-target

检查 Amazon DynamoDB 表的还原时间是否符合指定的持续时间。如果 DynamoDB 表 LatestRestoreExecutionTimeMinutes 的大于分钟，则该规则不合规。 maxRestoreTime

标识符：DYNAMODB_MEETS_RESTORE_TIME_TARGET

资源类型： AWS::DynamoDB::Table

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大 RestoreTime, 类型：int

允许的最大还原运行时间的数值。

resourceTags（可选）, 类型：字符串

规则要检查的 DynamoDB 表的标签，采用 JSON 格式。

resourceId（可选）, 类型：字符串

此规则要检查的 DynamoDB 表的名称。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-pitr-enabled

检查是否为亚马逊 DynamoDB 表启用了 point-in-time 恢复 (PITR)。如果 DynamoDB 表未启用 PITR，则此规则为 NON_COMPLIANT。

Identifier (标识符)：DYNAMODB_PITR_ENABLED

资源类型： AWS::DynamoDB::Table

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-resources-protected-by-backup-plan

检查 Amazon DynamoDB 表是否受备份计划的保护。如果 DynamoDB 表不在备份计划范围内，则此规则为 NON_COMPLIANT。

标识符：DYNAMODB_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型： AWS::DynamoDB::Table

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选），类型：字符串

此规则要检查的 DynamoDB 表的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选），类型：字符串

此规则要检查的 DynamoDB 表的名称。

crossRegionList （可选），类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （可选），类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （可选），类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （可选），类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选），类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-table-deletion-protection-enabled

检查 Amazon DynamoDB 表是否已将删除保护设置为已启用。如果该表的删除保护设置为禁用，则该规则为 NON_COMPLIANT。

标识符：DYNAMODB_TABLE_DELETION_PROTECTION_ENABLED

资源类型： AWS::DynamoDB::Table

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-table-encrypted-kms

检查 Amazon DynamoDB 表是否 AWS 使用密钥管理服务 (KMS) 加密。如果 Amazon DynamoDB 表未使用 KMS 加密，则该规则不合规。 AWS 如果`kmsKeyArns`输入参数中不存在加密的 AWS KMS 密钥，则该规则也属于 NON_Complift。

Identifier (标识符)：DYNAMODB_TABLE_ENCRYPTED_KMS

资源类型： AWS::DynamoDB::Table

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyArns （可选），类型：CSV

允许加密亚马逊 DynamoDB 表的 AWS KMS 密钥 ARN 列表，以逗号分隔。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-table-encryption-enabled

检查 Amazon DynamoDB 表是否已加密并检查其状态。如果状态为已启用或正在启用，则此规则为 COMPLIANT。

标识符：DYNAMODB_TABLE_ENCRYPTION_ENABLED

资源类型： AWS::DynamoDB::Table

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

dynamodb-throughput-limit-check

检查为 DynamoDB 预配置的吞吐量是否正在接近账户最大限制。默认情况下，此规则检查预置的吞吐量是否超过您的账户限制的阈值 (80%)。

标识符：DYNAMODB_THROUGHPUT_LIMIT_CHECK

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

AccountRCUThresholdPercentage （可选）, 类型：int, 默认值：80

为您的账户预配置的读取容量单位数的百分比。当达到此值时，规则将被标记为不合规。

账户 WCUThresholdPercentage （可选）, 类型：int, 默认值：80

为您的账户预配置的写入容量单位数的百分比。当达到此值时，规则将被标记为不合规。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ebs-in-backup-plan

检查 Backup 的备份计划中是否添加了亚马逊 Elastic Block Store (Amazon EBS) 卷。 AWS 如果备份计划中未包含 Amazon EBS 卷，则此规则为 NON_COMPLIANT。

标识符：EBS_IN_BACKUP_PLAN

资源类型： AWS::EC2::Volume

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ebs-last-backup-recovery-point-created

检查是否为 Amazon Elastic Block Store (Amazon EBS) 创建了恢复点。如果 Amazon EBS 卷没有在指定时间段内创建相应的恢复点，则此规则为 NON_COMPLIANT。

标识符：EBS_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型： AWS::EC2::Volume

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Amazon EBS 卷的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon EBS 卷的 ID。

恢复PointAgeValue （可选）, 类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit （可选）, 类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ebs-meets-restore-time-target

检查 Amazon Elastic Block Store (Amazon EBS) 卷的还原时间是否符合指定的持续时间。如果 Amazon EBS LatestRestoreExecutionTimeMinutes 的交易量大于分钟，则该规则不合规。
maxRestoreTime

标识符：EBS_MEETS_RESTORE_TIME_TARGET

资源类型： AWS::EC2::Volume

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大 RestoreTime, 类型：int

允许的最大还原运行时间的数值。

resourceTags（可选）, 类型：字符串

规则要检查的 Amazon EBS 卷的标签，采用 JSON 格式。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon EBS 卷的 ID。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ebs-optimized-instance

检查是否为可进行 Amazon EBS 优化的 Amazon Elastic Compute Cloud (Amazon EC2) 实例启用了 Amazon EBS 优化。如果未为可进行 EBS 优化的 Amazon EC2 实例启用 EBS 优化，则此规则为 NON_COMPLIANT。

> **Note**
>
> 默认情况下经过 EBS 优化的 EC2 实例的规则评估总是会返回 `COMPLIANT`。

标识符： EBS_OPTIMIZED_INSTANCE

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ebs-resources-protected-by-backup-plan

检查 Amazon Elastic Block Store (Amazon EBS) 卷是否受备份计划的保护。如果备份计划不涵盖 Amazon EBS 卷，则此规则为 NON_COMPLIANT。

标识符：EBS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型： AWS::EC2::Volume

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选），类型：字符串

此规则要检查的 Amazon EBS 卷的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选），类型：字符串

此规则要检查的 Amazon EBS 卷的 ID。

crossRegionList （可选），类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （可选），类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （可选），类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （可选），类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选），类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ebs-snapshot-public-restorable-check

检查 Amazon Elastic Block Store (Amazon EBS) 是否不可公开还原。如果将一个或多个带 RestorableByUserIds 字段的快照设置为全部，即 Amazon EBS 快照是公开的，则该规则不合规。

标识符：EBS_SNAPSHOT_PUBLIC_RESTORABLE_CHECK

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-client-vpn-connection-log-enabled

检查 AWS Client VPN 端点是否启用了客户端连接日志记录。如果 “配置”，则该规则不兼容。ConnectionLogOptions.Enabled' 设置为 false。

标识符：EC2_CLIENT_VPN_CONNECTION_LOG_ENABLED

资源类型： AWS::EC2::ClientVpn端点

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-client-vpn-not-authorize-all

检查 AWS Client VPN 授权规则是否授权所有客户端进行连接访问。如果 “AccessAll” 存在且设置为 true，则该规则不兼容。

标识符：EC2_CLIENT_VPN_NOT_AUTHORIZE_ALL

资源类型： AWS::EC2::ClientVpn端点

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-ebs-encryption-by-default

检查 Amazon Elastic Block Store (EBS) 加密是否已默认启用。如果未启用加密，则规则为 NON_COMPLIANT。

Identifier (标识符)：EC2_EBS_ENCRYPTION_BY_DEFAULT

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-imdsv2-check

检查您的 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据版本是否配置了实例元数据服务版本 2 (IMDSv2)。如果设置为可选，则该 HttpTokens 规则不兼容。

标识符：EC2_IMDSV2_CHECK

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-instance-detailed-monitoring-enabled

检查是否已为 EC2 实例启用详细监控。如果未启用详细监控，则此规则为 NON_COMPLIANT。

标识符：EC2_INSTANCE_DETAILED_MONITORING_ENABLED

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-instance-managed-by-systems-manager

> **Important**
>
> 对于此规则，规则标识符 (EC2_INSTANCE_MANAGED_BY_SSM) 和规则名称 (ec2-instance-managed-by-systems-manager) 不同。

检查您的 Amazon EC2 实例是否由 AWS Systems Manager 代理（SSM 代理）管理。如果 EC2 实例正在运行且 SSM 代理已停止，或者 EC2 实例正在运行且 SSM 代理已终止，则该规则不合规。

> **Note**
>
> 如果 EC2 实例已停止且 SSM 代理正在运行，则该规则不会返回 NON_COMPLIBLITY。

标识符：EC2_INSTANCE_MANAGED_BY_SSM

资源类型： AWS::EC2::Instance, AWS::SSM::ManagedInstance库存

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-instance-multiple-eni-check

检查 Amazon Elastic Compute Cloud (Amazon EC2) 是否使用多个弹性网络接口 (ENI) 或 Elastic Fabric Adapter (EFA)。如果 Amazon EC2 实例使用多个网络接口，则此规则为 NON_COMPLIANT。

标识符：EC2_INSTANCE_MULTIPLE_ENI_CHECK

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

NetworkInterfaceIds （可选），类型：CSV

网络实例 ID 的逗号分隔列表

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "NetworkInterfaces": "[NetworkInterfaceId-1, NetworkInterfaceId-2,
 NetworkInterfaceId-3, ...]"
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-instance-no-public-ip

检查 EC2 实例是否有公有 IP 关联。如果 EC2 实例配置项中存在 publicIp 字段，则此规则为 NON_COMPLIANT。此规则仅适用于 IPv4。

背景：公有 IP 地址可以使 EC2 实例能够从互联网上直接访问到，但从安全或合规的角度来看，此类地址并不总是可取的：

- 安全：许多情况下，您可能不希望自己的 EC2 实例拥有公有 IP 地址，除非它们需要可供公众访问。拥有公有 IP 地址会使 EC2 实例面临潜在的安全风险，如未经授权的访问或攻击。
- 合规：PCI、DSS 或 HIPAA 等各种合规标准对网络分段和访问控制都有特定的要求。确保 EC2 实例没有不必要的公有 IP 地址，有助于符合这些要求。
- 成本管理：公有 IP 地址可能会产生额外费用，尤其是在这些地址持续关联 EC2 实例的情况下。通过识别不需要公有 IP 地址但拥有公有 IP 地址的 EC2 实例，您有可能可以降低成本。

标识符：EC2_INSTANCE_NO_PUBLIC_IP

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-instance-profile-attached

检查 EC2 实例是否附加了 AWS 身份和访问管理 (IAM) 配置文件。如果 EC2 实例未附加 IAM 配置文件，则此规则为 NON_COMPLIANT。

标识符：EC2_INSTANCE_PROFILE_ATTACHED

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

IamInstanceProfileArnList （可选）, 类型：CSV

可以附加到 Amazon EC2 实例的 IAM 配置文件 Amazon 资源名称 (ARN) 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-last-backup-recovery-point-created

检查是否为 Amazon Elastic Compute Cloud (Amazon EC2) 实例创建了恢复点。如果 Amazon EC2 实例没有在指定时间段内创建相应的恢复点，则此规则为 NON_COMPLIANT。

标识符：EC2_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型： AWS::EC2::Instance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Amazon EC2 实例的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon EC2 实例 ID。

恢复PointAgeValue （可选）, 类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit （ 可选 ）, 类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-launch-template-public-ip-disabled

检查 Amazon EC2 启动模板是否设置为向网络接口分配公有 IP 地址。如果 EC2 启动模板的默认版本至少有 1 个网络接口，且将 “” 设置为 “true AssociatePublicIpAddress”，则该规则不合规。

标识符：EC2_LAUNCH_TEMPLATE_PUBLIC_IP_DISABLED

资源类型： AWS::EC2::LaunchTemplate

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

exemptedLaunchTemplates （ 可选 ）, 类型：CSV

以逗号分隔的豁免的 EC2 启动模板 ID 列表，这些模板允许网络接口的 AssociatePublicIpAddress 值设置为 “true”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-managedinstance-applications-blacklisted

检查实例上是否未安装指定的任何应用程序。（ 可选 ）指定版本。较新的版本不会被列入拒绝名单。根据需要指定平台，仅针对运行该平台的实例应用规则。

标识符：EC2_MANAGEDINSTANCE_APPLICATIONS_BLACKLISTED

资源类型： AWS::SSM::ManagedInstance库存

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

applicationNames, 类型：CSV

以逗号分隔的应用程序名称列表。（可选）指定附加有“:”的版本（例如，“Chrome: 0.5.3，FireFox”）。

> **Note**
>
> 应用程序名称必须完全匹配。例如，在 Linux 上使用 **`firefox`** 或在 Amazon Linux 上使用 **`firefox-compat`**。此外，目前 AWS Config 不支持 ApplicationN ames 参数的通配符（例如**`firefox*`**）。

platformType（可选），类型：字符串

平台类型（例如，“Linux”或“Windows”）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-managedinstance-applications-required

检查实例上是否安装了所有指定的应用程序。(可选) 指定可接受的最低版本。您还可以指定平台，仅针对运行该平台的实例应用规则。

> **Note**
>
> 确保 SSM 代理已在 EC2 实例上运行，并且已创建用于收集应用程序软件清单的关联。如果未安装 SSM 代理或尚未创建或运行关联，则此规则将返回 NOT_APPLICABLE。

标识符：EC2_MANAGEDINSTANCE_APPLICATIONS_REQUIRED

资源类型： AWS::SSM::ManagedInstance库存

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

applicationNames, 类型：CSV

以逗号分隔的应用程序名称列表。（可选）指定附加有“:”的版本（例如，“Chrome: 0.5.3，FireFox”）。

> **Note**
>
> 应用程序名称必须完全匹配。例如，在 Linux 上使用 **`firefox`** 或在 Amazon Linux 上使用 **`firefox-compat`**。此外，目前 AWS Config 不支持 ApplicationN ames 参数的通配符（例如**`firefox*`**）。

platformType（可选），类型：字符串

平台类型（例如，“Linux”或“Windows”）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-managedinstance-association-compliance-status-check

在实例上执行关联后，检查 AWS Systems Manager 关联合规性的状态是合规还是不合规。如果字段状态为 COMPLIANT，则此规则为合规。有关关联的更多信息，请参阅什么是关联？

标识符：EC2_MANAGEDINSTANCE_ASSOCIATION_COMPLIANCE_STATUS_CHECK

资源类型： AWS::SSM::AssociationCompliance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-managedinstance-inventory-blacklisted

检查由 Amazon EC2 Systems Manager 托管的实例是否已配置为收集黑名单中的清单类型。

标识符：EC2_MANAGEDINSTANCE_INVENTORY_BLACKLISTED

资源类型： AWS::SSM::ManagedInstance库存

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

inventoryNames, 类型：CSV

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

platformType（可选）, 类型：字符串

平台类型（例如，“Linux”）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-managedinstance-patch-compliance-status-check

在实例上安装补丁后，检查 AWS Systems Manager 补丁合规性的合规状态是合规还是不兼容。如果字段状态为 COMPLIANT，则此规则为合规。

标识符：EC2_MANAGEDINSTANCE_PATCH_COMPLIANCE_STATUS_CHECK

资源类型： AWS::SSM::PatchCompliance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-managedinstance-platform-check

检查 EC2 托管实例是否具有所需的配置。

标识符：EC2_MANAGEDINSTANCE_PLATFORM_CHECK

资源类型： AWS::SSM::ManagedInstance库存

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

platformType, 类型：字符串

平台类型（例如，“Linux”）。

platformVersion（可选）, 类型：字符串

平台版本（例如，“2016.09”）。

agentVersion（可选）, 类型：字符串

代理版本（例如，“2.0.433.0”）。

platformName（可选）, 类型：字符串

平台版本（例如，“2016.09”）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-meets-restore-time-target

检查 Amazon Elastic Compute Cloud (Amazon EC2) 实例的还原时间是否符合指定的持续时间。如果 Amazon EC2 实例 LatestRestoreExecutionTimeMinutes 的大于 maxRestoreTime 分钟，则该规则不合规。

标识符：EC2_MEETS_RESTORE_TIME_TARGET

资源类型： AWS::EC2::Instance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大 RestoreTime, 类型：int

允许的最大还原运行时间的数值。

resourceTags（可选）, 类型：字符串

规则要检查的 Amazon EC2 实例的标签，采用 JSON 格式。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon EC2 实例 ID。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-no-amazon-key-pair

检查正在运行的 Amazon Elastic Compute Cloud (EC2) 实例是否是使用亚马逊密钥对启动的。如果正在运行的 EC2 实例是使用密钥对启动的，则此规则为 NON_COMPLIANT。

标识符：EC2_NO_AMAZON_KEY_PAIR

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-paravirtual-instance-check

检查 EC2 实例的虚拟化类型是否为准虚拟化。如果 EC2 实例的“virtualizationType”设置为“paravirtual”，则此规则为 NON_COMPLIANT。

标识符：EC2_PARAVIRTUAL_INSTANCE_CHECK

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域：仅在以下区域提供：中国（北京）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、亚太地区（东京）、美国西部（俄勒冈州）、美国西部（北加利福尼亚）、亚太地区（新加坡）、亚太地区（悉尼）

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-resources-protected-by-backup-plan

检查 Amazon Elastic Compute Cloud (Amazon EC2) 实例是否受备份计划的保护。如果备份计划不涵盖 Amazon EC2 实例，则此规则为 NON_COMPLIANT。

> **Note**
> 此规则仅适用于正在运行的 Amazon EC2 实例，不适用于电源已关闭的实例。

标识符：EC2_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型： AWS::EC2::Instance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选），类型：字符串

此规则要检查的 Amazon EC2 实例的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选），类型：字符串

此规则要检查的 Amazon EC2 实例 ID。

crossRegionList （可选），类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （可选），类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （可选），类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （可选），类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选），类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-security-group-attached-to-eni

检查是否已将非默认安全组附加到弹性网络接口。如果安全组未与网络接口相关联，则此规则为 NON_COMPLIANT。

标识符：EC2_SECURITY_GROUP_ATTACHED_TO_ENI

资源类型： AWS::EC2::SecurityGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-security-group-attached-to-eni-periodic

检查是否已将非默认安全组附加到弹性网络接口 (ENI)。如果安全组未与 ENI 相关联，则此规则为 NON_COMPLIANT。不属于调用账户的安全组将评估为 NOT_APPLICABLE。

> **Note**
>
> 此规则将报告 `AWS::EC2::SecurityGroup` 资源类型。但是，为了让规则有效运行，必须启用 `AWS::EC2::NetworkInterface` 资源类型的记录。

标识符：EC2_SECURITY_GROUP_ATTACHED_TO_ENI_PERIODIC

资源类型： AWS::EC2::SecurityGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-stopped-instance

检查是否有 Amazon Elastic Compute Cloud (Amazon EC2) 实例已停止运行超过允许的天数。如果 Amazon EC2 实例的停止时间超过允许的天数，或无法确定时间长度，则此规则为 NON_COMPLIANT。

标识符：EC2_STOPPED_INSTANCE

资源类型： AWS::EC2::Instance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

AllowedDays （可选），类型：int, 默认：30

在规则为 NON_COMPLIANT 之前，Amazon EC2 实例可停止运行的天数。默认天数为 30。

> **Note**
>
> 所选天数必须少于配置的保留期，因为此规则依赖于收集的历史数据。有关历史数据保留的更多信息，请参阅删除 AWS Config 数据。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-token-hop-limit-check

检查 Amazon Elastic Compute Cloud (EC2) 实例元数据指定的令牌跃点限制是否低于所需限制。如果实例的跃点限制值高于预期限制，则此规则为 NON_COMPLIANT。

标识符：EC2_TOKEN_HOP_LIMIT_CHECK

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

tokenHopLimit （可选）, 类型：int

所需的令牌跃点限制。有效值介于 1 到 64 之间，包括 1 和 64。如果未指定参数，则默认值为 1。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-transit-gateway-auto-vpc-attach-disabled

检查亚马逊弹性计算云 (Amazon EC2) Elastic Compute Gateway AutoAccept SharedAttachments s 是否已启用 “”。如果 “” 设置为 “启用 AutoAcceptSharedAttachments”，则 Transit Gateway 的规则不合规。

标识符：EC2_TRANSIT_GATEWAY_AUTO_VPC_ATTACH_DISABLED

资源类型： AWS::EC2::TransitGateway

触发器类型： 配置更改

AWS 区域：仅在欧洲（斯德哥尔摩）、欧洲（巴黎）、美国东部（俄亥俄州）、非洲（开普敦）、欧洲（爱尔兰）、欧洲（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚北部）、亚太地区（首尔）、欧洲（伦敦）、欧洲（米兰）、亚太地区（东京）、美国西部（俄勒冈）、美国西部（加利福尼亚北部）、亚太地区（新加坡）、亚太地区（新加坡）、亚太地区（伦敦）、欧洲（米兰）、亚太地区（东京）、美国西部（俄勒冈）、美国西部（加利福尼亚北部）、亚太地区（新加坡）、亚太地区（悉尼）)、加拿大（中部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-volume-inuse-check

检查 EBS 卷是否附加到 EC2 实例。(可选) 检查 EBS 卷是否已标记为在实例终止时删除。

如果 EBS 卷附加到正在运行的 EC2 实例，则此规则为 COMPLIANT。在这种情况下，当 EC2 实例正在使用 EBS 卷时，它就是 COMPLIANT。

如果 EBS 卷未附加到任何 EC2 实例，或者附加到已停止或已终止的 EC2 实例，则此规则为 NON_COMPLIANT。在这种情况下，当 EC2 实例未积极使用 EBS 卷时，它就是 NON_COMPLIANT。

标识符：EC2_VOLUME_INUSE_CHECK

资源类型： AWS::EC2::Volume

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

deleteOnTermination （可选），类型：布尔值

EBS 卷已标记为在实例终止时删除。可能的值：True 或 False（其他输入值将被标记为 NON_COMPLIANT）。如果设置为 `True`，且未将已终止的 EBS 卷标记为删除，则此规则为 NON_COMPLIANT。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecr-private-image-scanning-enabled

检查私有 Amazon Elastic Container Registry (Amazon ECR) 存储库是否已启用映像扫描。如果私有 Amazon ECR 存储库的扫描频率不是“推送时扫描”或“连续扫描”，则此规则为 NON_COMPLIANT。有关启用映像扫描的更多信息，请参阅《Amazon ECR 用户指南》中的映像扫描。

标识符：ECR_PRIVATE_IMAGE_SCANNING_ENABLED

资源类型： AWS::ECR::Repository

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecr-private-lifecycle-policy-configured

检查私有 Amazon Elastic Container Registry (ECR) 存储库是否配置了至少一项生命周期策略。如果没有为 ECR 私有存储库配置生命周期策略，则此规则为 NON_COMPLIANT。

标识符：ECR_PRIVATE_LIFECYCLE_POLICY_CONFIGURED

资源类型： AWS::ECR::Repository

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecr-private-tag-immutability-enabled

检查私有 Amazon Elastic Container Registry (ECR) 存储库是否已启用标签不可变性。如果没有为私有 ECR 存储库启用标签不可变性，则此规则为 NON_COMPLIANT。

标识符：ECR_PRIVATE_TAG_IMMUTABILITY_ENABLED

资源类型： AWS::ECR::Repository

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-awsvpc-networking-enabled

检查活动弹性云服务器的联网模式是否设置TaskDefinitions 为 “awsvpc”。如果活动 ECS 未设置为 “awsvpc”TaskDefinitions ，则此规则不合规。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS AWSVPC_NETWORKING _ _ENABLED

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-containers-nonprivileged

检查 ECS 容器定义中的特权参数是否设置TaskDefinitions 为 “true”。如果特权参数为“true”，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_CONTAINERS_NONPRIVILEGED

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-containers-readonly-access

检查 Amazon Elastic Container Service (Amazon ECS) 容器是否只能对其根文件系统进行只读访问。如果 ECS 的容器定义中的 readonlyRootFilesystem 参数设置为 “false”，则该规则TaskDefinitions 不合规。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识：ECS_CONTAINERS_READONLY_ACCESS

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-container-insights-enabled

检查 Amazon Elastic Container Service 集群是否启用了容器洞察。如果未启用容器洞察，则此规则为 NON_COMPLIANT。

标识符：ECS_CONTAINER_INSIGHTS_ENABLED

资源类型： AWS::ECS::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-fargate-latest-platform-version

检查 ECS Fargate 服务是否设置为最新平台版本。如果 Fargate PlatformVersion 的启动类型未设置为 LATEST，或者两者均未作为参数提供，则该规则 latestLinuxVersion 不`latestWindowsVersion`兼容。

标识符：ECS_FARGATE_LATEST_PLATFORM_VERSION

资源类型： AWS::ECS::Service

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

latestLinuxVersion （可选），类型：字符串

最新的 Linux 支持语义版本控制 (SemVer) 格式PlatformVersion的 “”。如果部署了 Fargate 并且明确指定了 “PlatformVersion” 或将其用作 “” CodeDeploy ，则可能需要参数 DeploymentController

latestWindowsVersion （可选），类型：字符串

最新的 Windows 支持语义版本控制 (SemVer) 格式PlatformVersion的 “”。如果部署了 Fargate 并且明确指定了 “PlatformVersion” 或将其用作 “” CodeDeploy ，则可能需要参数 DeploymentController

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-no-environment-secrets

检查机密是否作为容器环境变量传递。如果一个或多个环境变量键与“`secretKeys`”参数中列出的键匹配（不包括来自其他位置的环境变量，例如 Amazon S3），则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_NO_ENVIRONMENT_SECRETS

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

secretKeys, 类型：CSV

逗号分隔的键名列表，用于在任务定义中容器定义的环境变量中搜索。将删除多余的空格。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-task-definition-log-configuration

检查是否在活动的 ECS 任务定义上设置了 logConfiguration。如果活动 ECS TaskDefinition 没有定义日志配置资源，或者在至少一个容器定义中日志配置的值为空，则此规则不合规。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_TASK_DEFINITION_LOG_CONFIGURATION

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-task-definition-memory-hard-limit

检查 Amazon Elastic Container Service (ECS) 任务定义是否为其容器定义设置了内存限制。如果任务定义的一个容器定义中没有“memory”参数，则此规则为 NON_COMPLIANT。

> **Note**
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_TASK_DEFINITION_MEMORY_HARD_LIMIT

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-task-definition-nonroot-user

检查 ECS 是否为亚马逊弹性容器服务 (Amazon ECS) Elastic Container Service TaskDefinitions 指定了一个用户来运行 EC2 启动类型的容器。如果“user”参数不存在或设置为“root”，则此规则为 NON_COMPLIANT。

> **Note**
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_TASK_DEFINITION_NONROOT_USER

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-task-definition-pid-mode-check

检查 ECS TaskDefinitions 是否配置为与其亚马逊弹性容器服务 (Amazon ECS) 容器共享主机的进程命名空间。如果 PidMode 参数设置为“host”，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则仅评估 Amazon ECS 任务定义的最新活跃版本。

标识符：ECS_TASK_DEFINITION_PID_MODE_CHECK

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ecs-task-definition-user-for-host-mode-check

检查最新活动的 Amazon Elastic Container Service (Amazon ECS) 任务定义中 `NetworkMode` 设置为 host 的未授权权限。对于 `NetworkMode` 设置为 host 的任务定义，以及 `privileged` 设置为 false 或空且 `user` 设置为 root 或空的容器定义，此规则为 NON_COMPLIANT。

> **Important**
>
> 建议您从 Amazon ECS 任务定义中删除提升的权限。如果`privileged`为 true，则容器在宿主容器实例上获得提升的权限（与`root`用户类似）。运行使用 `host` 网络模式的任务时，请勿使用根用户（UID 0）运行容器，以获得更好的安全性。作为安全最佳实践，请始终使用非根用户。

标识符：ECS_TASK_DEFINITION_USER_FOR_HOST_MODE_CHECK

资源类型： AWS::ECS::TaskDefinition

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

SkipInactiveTaskDefinitions （可选），类型：布尔值

布尔值标志，避免检查处于 INACTIVE 状态的 Amazon EC2 任务定义。如果设置为“true”，则此规则将不会评估处于 INACTIVE 状态的 Amazon EC2 任务定义。如果设置为“false”，则此规则将评估处于 INACTIVE 状态的 Amazon EC2 任务定义的最新版本。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

efs-access-point-enforce-root-directory

检查 Amazon Elastic File System (Amazon EFS) 接入点是否配置为强制使用根目录。如果“Path”的值设置为“/”（文件系统的默认根目录），则此规则为 NON_COMPLIANT。

标识符：EFS_ACCESS_POINT_ENFORCE_ROOT_DIRECTORY

资源类型： AWS::EFS::AccessPoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

approvedDirectories（可选），类型：CSV

已批准强制使用 Amazon EFS 接入点根目录的子目录路径的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

efs-access-point-enforce-user-identity

检查 Amazon Elastic File System (Amazon EFS) 接入点是否已配置为强制使用用户身份。如果未定义 “PosixUser” 或提供了参数但对应的参数中没有匹配项，则该规则为 NON_COMPLIMENT。

标识符：EFS_ACCESS_POINT_ENFORCE_USER_IDENTITY

资源类型： AWS::EFS::AccessPoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

approvedUids（可选），类型：CSV

获准用于 EFS 接入点用户强制执行的 POSIX 用户 ID 的逗号分隔列表。

approvedGids（可选），类型：CSV

获准用于 EFS 接入点用户强制执行的 POSIX 组 ID 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

efs-encrypted-check

检查是否将 Amazon Elastic File System (Amazon EFS) 配置为使用 AWS Key Management Service (AWS KMS) 加密文件数据。如果在 `DescribeFileSystems` 上将加密密钥设置为 false，

或者 `DescribeFileSystems` 上的 `KmsKeyId` 密钥与 `KmsKeyId` 参数不匹配，则此规则为 NON_COMPLIANT。

标识符：EFS_ENCRYPTED_CHECK

资源类型： AWS::EFS::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

KmsKeyId （可选），类型：字符串

用于加密 EFS 文件系统的 KMS 密钥的 Amazon 资源名称 (ARN)。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

efs-in-backup-plan

检查 Backup 的备份计划中是否添加了 Amazon Elastic File System (Amazon EFS) 文件系统。 AWS 如果备份计划中不包括 EFS 文件系统，则此规则为 NON_COMPLIANT。

标识符：EFS_IN_BACKUP_PLAN

资源类型： AWS::EFS::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

efs-last-backup-recovery-point-created

检查是否为 Amazon Elastic File System (Amazon EFS) 文件系统创建了恢复点。如果 Amazon EFS 文件系统没有在指定时间段内创建相应的恢复点，则此规则为 NON_COMPLIANT。

标识符：EFS_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型： AWS::EFS::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Amazon EFS 文件系统的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 EFS 文件系统的 ID。

恢复PointAgeValue （可选）, 类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit （可选）, 类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

efs-meets-restore-time-target

检查 Amazon Elastic File System (Amazon EFS) 文件系统的还原时间是否符合指定的持续时间。如果 LatestRestoreExecutionTimeMinutes Amazon EFS 文件系统的时间大于 maxRestoreTime 分钟，则该规则不合规。

标识符：EFS_MEETS_RESTORE_TIME_TARGET

资源类型： AWS::EFS::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大 RestoreTime, 类型：int

允许的最大还原运行时间的数值。

resourceTags（可选）, 类型：字符串

规则要检查的 Amazon EFS 文件系统的标签，采用 JSON 格式。

resourceId（可选）, 类型：字符串

此规则要检查的 EFS 文件系统的 ID。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

efs挂载目标可公开访问

检查 Amazon Elastic File System (Amazon EFS) 挂载目标是否未与公有子网关联。如果 Amazon EFS 挂载目标与公有子网关联，则该规则不合规。

标识符：EFS_MOUNT_TARGET_PUBL

资源类型： AWS::EFS::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

efs-resources-protected-by-backup-plan

检查 Amazon Elastic File System (Amazon EFS) 文件系统是否受备份计划的保护。如果 EFS 文件系统不在备份计划范围内，则此规则为 NON_COMPLIANT。

标识符：EFS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型： AWS::EFS::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 EFS 文件系统的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 EFS 文件系统的 ID。

crossRegionList （可选）, 类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （可选）, 类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （可选）, 类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （可选）, 类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选）, 类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

eip-attached

检查分配给 AWS 账户的所有弹性 IP 地址是否都连接到 EC2 实例或正在使用的弹性网络接口。如果弹性 IP 地址的 “AssociationId” 为空，则该规则不合规。

> **Note**
>
> 评估发生后，可能需要最多 6 小时才能获得结果。

标识符：EIP_ATTACHED

资源类型：AWS::EC2::EIP

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "InstanceId": "my-instance-Id"
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

eks-cluster-logging-enabled

检查 Amazon Elastic Kubernetes Service (Amazon EKS) 集群是否配置为启用日志记录。如果未为所有日志类型启用 Amazon EKS 集群的日志记录，则此规则为 NON_COMPLIANT。

标识符：EKS_CLUSTER_LOGGING_ENABLED

资源类型： AWS::EKS::Cluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

eks-cluster-log-enabled

检查 Amazon Elastic Kubernetes Service (Amazon EKS) 集群是否配置为启用日志记录。如果未启用 Amazon EKS 集群的日志记录，或者未启用上述日志类型的日志记录，则此规则为 NON_COMPLIANT。

标识符：EKS_CLUSTER_LOG_ENABLED

资源类型： AWS::EKS::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

logTypes（可选），类型：CSV

应启用的 EKS 集群控制层面日志类型列表（以逗号分隔）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

eks-cluster-oldest-supported-version

检查 Amazon Elastic Kubernetes Service (EKS) 集群是否运行的是支持的最旧版本。如果 EKS 集群运行的是支持的最旧版本（等于参数“`oldestVersionSupported`”），则此规则为 NON_COMPLIANT。

标识符：EKS_CLUSTER_OLDEST_SUPPORTED_VERSION

资源类型： AWS::EKS::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

最老的 VersionSupported, 类型：字符串

AWS上支持的最旧版本的 Kubernetes 的值。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

eks集群密钥已加密

检查 Amazon EKS 集群是否配置为使用 KMS 加密 Kubernetes 密钥。 AWS 如果 EKS 集群没有 EncryptionConfig 资源或者 EncryptionConfig 没有将机密命名为资源，则该规则不合规。

标识符：EKS_CLUSTER_SECRETS_C

资源类型： AWS::EKS::Cluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyArns （可选），类型：CSV

获准使用 EKS 的 KMS 密钥亚马逊资源名称 (ARN) 列表，以逗号分隔。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

eks-cluster-supported-version

检查 Amazon Elastic Kubernetes Service (EKS) 集群是否正在运行支持的 Kubernetes 版本。如果 EKS 集群正在运行不受支持的版本（小于参数“`oldestVersionSupported`”），则此规则为 NON_COMPLIANT。

标识符：EKS_CLUSTER_SUPPORTED_VERSION

资源类型： AWS::EKS::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

最老的 VersionSupported, 类型：字符串

AWS上支持的最旧版本的 Kubernetes 的值。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

eks-endpoint-no-public-access

检查 Amazon Elastic Kubernetes Service (Amazon EKS) 终端节点是否不可公开访问。如果终端节点可公开访问，则此规则为 NON_COMPLIANT。

标识符：EKS_ENDPOINT_NO_PUBLIC_ACCESS

资源类型： AWS::EKS::Cluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

eks-secrets-encrypted

检查 Amazon Elastic Kubernetes Service 集群是否配置为使用 (KMS) 密钥加密 Kubernetes 密钥。AWS Key Management Service

- 如果 EKS 集群的 encryptionConfig 使用某个资源作为机密，则此规则为 COMPLIANT。
- 如果用于加密 EKS 机密的密钥与参数匹配，则此规则也为 COMPLIANT。
- 如果 EKS 集群没有 encryptionConfig 或 encryptionConfig 资源不包含机密，则此规则为 NON_COMPLIANT。
- 如果用于加密 EKS 机密的密钥与参数不匹配，则此规则也为 NON_COMPLIANT。

标识符：EKS_SECRETS_ENCRYPTED

资源类型： AWS::EKS::Cluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyArns （可选），类型：CSV

KMS 密钥的 Amazon 资源名称 (ARN) 的逗号分隔列表，这些 ARN 应在 EKS 集群中用于加密的机密。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticache-auto-minor-version-upgrade-check

检查 Amazon f ElastiCache or Redis 集群是否启用了自动次要版本升级。如果 ElastiCache 集群使用 Redis 引擎，且 “” 未设置为 “true AutoMinorVersionUpgrade”，则该规则不合规。

标识符：ELASTICACHE_AUTO_MINOR_VERSION_UPGRADE_CHECK

资源类型： AWS::ElastiCache::CacheCluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticache-rbac-auth-enabled

检查 Amazon ElastiCache 复制组是否启用了 RBAC 身份验证。如果 Redis 版本为 6 或更高版本，且 “UserGroupID” 缺失、为空或与 “” 参数提供的条目不匹配，则该规则不兼容。`allowedUserGroupIDs`

标识符：ELASTICACHE_RBAC_AUTH_ENABLED

资源类型： AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

允许UserGroup的 ID（可选），类型：CSV

以逗号分隔的获准访问 ElastiCache 复制组的用户组 ID 列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticache-redis-cluster-automatic-backup-check

检查 Amazon ElastiCache Redis 集群是否已开启自动备份。如果 Redis 集群的规则小于 SnapshotRetentionLimit 参数，则该规则不合规。 SnapshotRetentionPeriod 例如：如果参数为 15，则如果介于 0-15 之间，则规则不合规。 snapshotRetentionPeriod

标识符：ELASTICACHE_REDIS_CLUSTER_AUTOMATIC_BACKUP_CHECK

资源类型： AWS::ElastiCache::CacheCluster， AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

snapshotRetentionPeriod （可选），类型：int, 默认值：15

Redis 集群的最短快照保留期（以天为单位）。默认值为 15 天。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticache-repl-grp-auto-failover-enabled

检查 Amazon ElastiCache Redis 复制组是否启用了自动故障转移。如果 “” 未设置为 “已启用 AutomaticFailover”，则 ElastiCache 复制组的规则不兼容。

标识符：ELASTICACHE_REPL_GRP_AUTO_FAILOVER_ENABLED

资源类型： AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticache-repl-grp-encrypted-at-rest

检查 Amazon ElastiCache 复制组是否已 encryption-at-rest 启用。如果禁用 “AtRestEncryptionEnabled” 或 KMS 密钥 ARN 与 ApprovedKMS 参数不匹配，则该 ElastiCache 复制组的规则不兼容。KeyArns

标识符：ELASTICACHE_REPL_GRP_ENCRYPTED_AT_REST

资源类型： AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

已批准的 DKMKeyIds （可选）, 类型：CSV

经批准使用的 KMS 密钥 ID 列表，以 ElastiCache 逗号分隔。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticache-repl-grp-encrypted-in-transit

检查 Amazon ElastiCache 复制组是否已 encryption-in-transit 启用。如果 “已TransitEncryption启用” 设置为 “false”，则 ElastiCache 复制组的规则不兼容。

标识符：ELASTICACHE_REPL_GRP_ENCRYPTED_IN_TRANSIT

资源类型： AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticache-repl-grp-redis-auth-enabled

检查亚马逊 ElastiCache 复制组是否启用了 Redis 身份验证。如果 ElastiCache 复制组节点的 Redis 版本低于 6（版本 6+ 使用 Redis ACL）并且 “AuthToken” 缺失或为空/空，则该复制组的规则不合规。

标识符：ELASTICACHE_REPL_GRP_REDIS_AUTH_ENABLED

资源类型： AWS::ElastiCache::ReplicationGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticache-subnet-group-check

检查 Amazon ElastiCache 集群是否配置了自定义子网组。如果 ElastiCache 集群使用默认子网组，则该规则不合规。

标识符：ELASTICACHE_SUBNET_GROUP_CHECK

资源类型： AWS::ElastiCache::CacheCluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticache-supported-engine-version

检查 ElastiCache 集群运行的版本是否高于或等于推荐的引擎版本。如果 ElastiCache 集群的 “EngineVersion” 低于其给定引擎的指定推荐版本，则该规则为 NON_COMPLIMITY。

标识符：ELASTICACHE_SUPPORTED_ENGINE_VERSION

资源类型： AWS::ElastiCache::CacheCluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最新 MemcachedVersion, 类型：字符串

Memcached 的最新推荐引擎版本。有效值采用语义版本控制 (SemVer) 格式，主版本、次要版本和补丁版本（例如，1.6.6，而不是 1.6）为 3 个组成部分。

最新 RedisVersion, 类型：字符串

Redis 的最新推荐引擎版本。有效值采用语义版本控制 (SemVer) 格式，主版本、次要版本和补丁版本（例如 7.0.5，而不是 7.0）为 3 个组成部分。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticsearch-encrypted-at-rest

检查亚马逊 OpenSearch 服务（以前称为 Elasticsearch）域名是否启用了静态加密配置。如果未启用该 EncryptionAtRestOptions 字段，则该规则不兼容。

标识符：ELASTICSEARCH_ENCRYPTED_AT_REST

资源类型： AWS::Elasticsearch::Domain

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticsearch-in-vpc-only

检查亚马逊 OpenSearch 服务（以前称为 Elasticsearch）域名是否位于亚马逊虚拟私有云（亚马逊 VPC）中。如果 OpenSearch 服务域终端节点是公共的，则该规则不合规。

标识符：ELASTICSEARCH_IN_VPC_ONLY

资源类型： AWS::Elasticsearch::Domain

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticsearch-logs-to-cloudwatch

检查亚马逊 OpenSearch 服务域是否配置为向亚马逊日志发送 CloudWatch 日志。如果为 Amazon ES 域启用了日志，则此规则为 COMPLIANT。如果未配置日志记录，则此规则为 NON_COMPLIANT。

标识符：ELASTICSEARCH_LOGS_TO_CLOUDWATCH

资源类型： AWS::Elasticsearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

logTypes（可选），类型：CSV

已启用的日志的逗号分隔列表。有效值为“search”、“index”、“error”。

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "LogPublishingOptions": "{Key : Value, ...}"*
}
...
```

*具有以下一个或多个键的对象：SEARCH_SLOW_LOGS、ES_APPLICATION_LOGS、INDEX_SLOW_LOGS、AUDIT_LOGS，具体取决于要发布的日志类型。每个键都需要一个有效的 LogPublishingOption 值。

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elasticsearch-node-to-node-encryption-check

检查 OpenSearch 服务（以前称为 Elasticsearch）节点是否经过端到端加密。如果未在域上启用 node-to-node 加密，则该规则不兼容。

标识符：ELASTICSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

资源类型： AWS::Elasticsearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
```

```
...
{
   "NodeToNodeEncryptionOptions": BOOLEAN
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elastic-beanstalk-logs-to-cloudwatch

检查 E AWS lastic Beanstalk 环境是否配置为向亚马逊日志发送日志。 CloudWatch 如果 StreamLogs `的值为假，则该规则不合规。

标识符：ELASTIC_BEANSTALK_LOGS_TO_CLOUDWATCH

资源类型： AWS::ElasticBeanstalk::Environment

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

RetentionInDays （可选），类型：字符串

检查日志事件在到期前保留的天数。有效值为：1、3、5、7、14、30、60、90、120、150、180、365、400、545、731、1827 和 3653。如果值为 “logs”，则该规则不兼容。 RetentionInDays`与该参数不匹配。

DeleteOnTerminate （可选），类型：字符串

检查日志是否配置为在环境终止时删除。有效值为“true”或“false”。如果值为 “logs”，则该规则不兼容。 DeleteOn终止`与该参数不匹配。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elastic-beanstalk-managed-updates-enabled

检查 AWS Elastic Beanstalk 环境中的托管平台更新是否已启用。如果 `ManagedActionsEnabled` 的值设置为 true，则此规则为 COMPLIANT。如果 `ManagedActionsEnabled` 的值设置为 false，或者提供了参数但其值与现有配置不匹配，则此规则为 NON_COMPLIANT。

标识符：ELASTIC_BEANSTALK_MANAGED_UPDATES_ENABLED

资源类型： AWS::ElasticBeanstalk::Environment

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

UpdateLevel （可选），类型：字符串

表示更新级别是设置为“minor”版本更新还是“patch”版本更新。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elbv2-acm-certificate-required

检查应用程序负载均衡器和网络负载均衡器的侦听器是否配置为使用来自 AWS Certificate Manager (ACM) 的证书。如果至少 1 个负载平衡器中有至少 1 个侦听器在配置时没有 ACM 证书或配置的证书与 ACM 证书不同，则此规则为 NON_COMPLIANT。

标识符：ELBV2_ACM_CERTIFICATE_REQUIRED

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

AcmCertificatesAllowed （可选），类型：CSV

证书的 Amazon 资源名称 (ARN) 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elbv2-multiple-az

检查 Elastic Load Balancer V2（应用程序、网络或网关负载均衡器）是否映射到多个可用区 (AZ)。如果 Elastic Load Balancer V2 映射到的可用区少于 2 个，则此规则为 NON_COMPLIANT。有关更多信息，请参阅应用程序负载均衡器的可用区。

标识符：ELBV2_MULTIPLE_AZ

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

minAvailabilityZones （可选），类型：int

预期可用区的最小数量（介于 2 到 10 之间，含 2 和 10）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elb-acm-certificate-required

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

标识符：ELB_ACM_CERTIFICATE_REQUIRED

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elb-cross-zone-load-balancing-enabled

检查经典负载均衡器是否启用了跨区域负载均衡。如果经典负载均衡器未启用跨区域负载均衡，则此规则为 NON_COMPLIANT。

标识符：ELB_CROSS_ZONE_LOAD_BALANCING_ENABLED

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elb-custom-security-policy-ssl-check

检查您的经典负载均衡器 SSL 侦听器是否在使用自定义策略。此规则只适用于经典负载均衡器有 SSL 侦听器的情况。

标识符：ELB_CUSTOM_SECURITY_POLICY_SSL_CHECK

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

ssl ProtocolsAnd Ciphers, 类型：字符串

逗号分隔的密码和协议列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elb-deletion-protection-enabled

检查 Elastic Load Balancer 是否已启用删除保护。如果 deletion_protection.enabled 为 false，则此规则为 NON_COMPLIANT。

标识符：ELB_DELETION_PROTECTION_ENABLED

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elb-logging-enabled

检查应用程序负载均衡器和经典负载均衡器是否启用了日志记录。如果为假或不等于您提供`access_logs.s3.enabled`的 s3 `access_logs.S3.bucket`BucketName ，则该规则不合规。

> **Note**
>
> 此规则不适用于网络负载均衡器或网关负载均衡器。

标识符：ELB_LOGGING_ENABLED

资源类型： AWS::ElasticLoadBalancing::LoadBalancer，AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

s3BucketNames （可选）, 类型：CSV

逗号分隔的 Amazon S3 存储桶名称列表，Amazon ELB 将日志文件传送到这些存储桶。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elb-predefined-security-policy-ssl-check

检查您的经典负载均衡器 SSL 侦听器是否使用预定义的策略。如果经典负载均衡器 HTTPS/SSL 侦听器的策略不等于参数“`predefinedPolicyName`”的值，则此规则为 NON_COMPLIANT。

标识符：ELB_PREDEFINED_SECURITY_POLICY_SSL_CHECK

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

预定义的 PolicyName, 类型：字符串

预定义策略的名称。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

elb-tls-https-listeners-only

检查您的经典负载均衡器是否配置了 SSL 或 HTTPS 侦听器。如果侦听器未配置 SSL 或 HTTPS，则此规则为 NON_COMPLIANT。

- 如果经典负载均衡器未配置侦听器，则此规则将返回 NOT_APPLICABLE。
- 如果经典负载均衡器侦听器配置了 SSL 或 HTTPS，则此规则为 COMPLIANT。
- 如果侦听器未配置 SSL 或 HTTPS，则此规则为 NON_COMPLIANT。

标识符：ELB_TLS_HTTPS_LISTENERS_ONLY

资源类型： AWS::ElasticLoadBalancing::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

emr-block-public-access

检查使用 Amazon EMR 的账户是否启用了阻止公共访问的设置。如果为 false，则该规则不兼容；如果 BlockPublicSecurityGroupRules 为 true，则列出端口 22 以外的端口。PermittedPublicSecurityGroupRuleRanges

标识符：EMR_BLOCK_PUBLIC_ACCESS

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

emr-kerberos-enabled

检查 Amazon EMR 群集是否启用了 Kerberos。如果未将安全配置附加到群集或安全配置不满足指定的规则参数，则规则为 NON_COMPLIANT。

标识符：EMR_KERBEROS_ENABLED

资源类型： AWS::EMR::Cluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

TicketLifetimeInHours （可选），类型：int

群集 KDC 签发的 Kerberos 票证的有效期。

Realm（可选），类型：字符串

信任关系中另一领域的 Kerberos 领域名称。

Domain（可选），类型：字符串

信任关系中另一领域的域名。

AdminServer （可选），类型：字符串

信任关系的另一领域中的管理服务器的完全限定域名。

KdcServer （可选），类型：字符串

信任关系的另一领域中的 KDC 服务器的完全限定域名。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

emr-master-no-public-ip

检查 Amazon EMR 集群的主节点是否具有公有 IP。如果主节点具有公有 IP，则该规则为 NON_COMPLIANT。

> **Note**
>
> 此规则检查处于 RUNNING 或 WAITING 状态的集群。此规则要求您启用 `AWS::EC2::Instance` 资源类型的记录，以便进行准确的评估。

标识符：EMR_MASTER_NO_PUBLIC_IP

资源类型： AWS::EMR::Cluster， AWS::EC2::Instance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

encrypted-volumes

检查附加的 Amazon EBS 卷是否已加密，并可选择使用指定的 KMS 密钥进行加密。如果连接的 EBS 卷未加密或使用提供的参数中未包含的 KMS 密钥进行加密，则此规则为 NON_COMPLIANT。

标识符：ENCRYPTED_VOLUMES

资源类型： AWS::EC2::Volume

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

kmsId（可选）, 类型：字符串

用于加密卷的 KMS 密钥的 ID 或 ARN。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

fms-shield-resource-policy-check

检查应用程序负载均衡器、亚马逊 CloudFront 分配、Elastic Load Balancer 或弹性 IP 是否具有 AWS Shield 保护。它还会检查他们是否有与 Application Load Balancer 和 Amazon CloudFront 分配关联的 Web ACL。

标识符：FMS_SHIELD_RESOURCE_POLICY_CHECK

资源类型： AWS::CloudFront::Distribution, AWS::ElasticLoadBalancingV2::，BalancingV2::LoadBalancer AWS::WAFRegional::WebACL, AWS::EC2::EIP, AWS::ElasticLoad，LoadBalancer AWS::ShieldRegional::Protection AWS::Shield::Protection

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

webACLId, 类型：字符串

Web ACL 的 WebACLId。

resourceTypes, 类型：字符串

此配置规则将应用于的资源范围。

resourceTags（可选），类型：字符串

规则应与之关联的资源标签（例如，{ "tagKey1" : ["tagValue1"], "tagKey2" : ["tagValue2", "tagValue3"] }"）。

excludeResourceTags （可选），类型：布尔值

如果为 true，则排除与 resourceTags 匹配的资源。如果为 false，则包括与 resourceTags 匹配的所有资源。

fmsManagedToken （可选），类型：字符串

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

fmsRemediationEnabled （可选），类型：布尔值

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

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

fms-webacl-resource-policy-check

检查 Web ACL 是否与应用程序负载均衡器、API Gateway 阶段或亚马逊 CloudFront 分配相关联。AWS Firewall Manager 创建此规则时，FMS 策略所有者在 FMS 策略`WebACLId`中指定，并且可以选择启用补救。

标识符：FMS_WEBACL_RESOURCE_POLICY_CHECK

资源类型:: AWS::CloudFront::Distribution, AWS::ApiGateway: Stage、AWS::ElasticLoadBalancingV2::LoadBalancer、ACL AWS::WAFRegional::Web

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

webACLId, 类型：字符串

Web ACL 的 WebACLId。

resourceTags（可选）, 类型：字符串

规则应与之关联的资源标签（ApplicationLoad均衡 ApiGatewayStage 器和 CloudFront 分配）。（例如，{“tagKey1": [" tagValue1"]、“tagKey2"：[" tagValue2"、“tagValue3"]}）

excludeResourceTags （可选）, 类型：布尔值

如果为 true，则排除与 resourceTags 匹配的资源。

fmsManagedToken （可选）, 类型：字符串

Fi AWS rewall Manager 在客户账户中创建规则时生成的令牌。 AWS 当客户创建此规则时，Config 会忽略此参数。

fmsRemediationEnabled （可选）, 类型：布尔值

如果为 true，Fi AWS rewall Manager 将根据 FMS 策略更新不合规的资源。 AWS 当客户创建此规则时，Config 会忽略此参数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

fms-webacl-rulegroup-association-check

检查规则组是否与处于正确优先级的 Web ACL 关联。正确优先级由规则组在 ruleGroups 参数中的排名决定。 AWS Firewall Manager 创建此规则时，它会分配最高优先级 0，然后是 1、2，依此类推。FMS 策略所有者在 FMS 策略中指定 `ruleGroups` 排名，并且可以选择启用补救功能。

标识符：FMS_WEBACL_RULEGROUP_ASSOCIATION_CHECK

资源类型： AWS::WAF::WebACL、 AWS::WAFRegional::Web ACL

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

ruleGroups, 类型：字符串

以逗号分隔的 RuleGroupIds 和 WafOverrideAction 对列表。（例如， ruleGroupId-1: 无，2: COUNT） ruleGroupId

fmsManagedToken（可选）, 类型：字符串

Fi AWS rewall Manager 在客户账户中创建规则时生成的令牌。 AWS 当客户创建此规则时，Config 会忽略此参数。

fmsRemediationEnabled（可选）, 类型：布尔值

如果为 true，Fi AWS rewall Manager 将根据 FMS 策略更新不合规的资源。 AWS 当客户创建此规则时，Config 会忽略此参数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

fsx-last-backup-recovery-point-created

检查是否为 Amazon FSx 文件系统创建了恢复点。如果 Amazon FSx 文件系统没有在指定时间段内创建相应的恢复点，则此规则为 NON_COMPLIANT。

标识符：FSX_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型： AWS::FSx::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Amazon FSx 文件系统的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon FSx 文件系统的 ID。

恢复PointAgeValue（可选），类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit（可选），类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

fsx-lustre-copy-tags-to-backups

检查适用于 Lustre 的 Amazon FSx 文件系统是否配置为将标签复制到备份。如果 Lustre 文件系统未被配置为将标签复制到备份，则此规则为 NON_COMPLIANT。

标识符：FSX_LUSTRE_COPY_TAGS_TO_BACKUPS

资源类型： AWS::FSx::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

fsx-meets-restore-time-target

检查 Amazon FSx 文件系统的还原时间是否符合指定的持续时间。如果 Amazon FSx 文件系统的 LatestRestoreExecutionTimeMinutes 时间大于分钟，则该规则不合规。 maxRestoreTime

标识符：FSX_MEETS_RESTORE_TIME_TARGET

资源类型： AWS::FSx::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大 RestoreTime, 类型：int

允许的最大还原运行时间的数值。

resourceTags（可选）, 类型：字符串

规则要检查的 Amazon FSx 文件系统的标签，采用 JSON 格式。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon FSx 文件系统的 ID。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

fsx-openzfs-copy-tags-enabled

检查适用于 OpenZFS 的 Amazon FSx 文件系统是否配置为将标签复制到备份和卷。如果适用于 OpenZFS 的 FSx 文件系统未被配置为将标签复制到备份和卷，则此规则为 NON_COMPLIANT。

标识符：FSX_OPENZFS_COPY_TAGS_ENABLED

资源类型： AWS::FSx::FileSystem

触发器类型： 定期

AWS 区域：仅在以下区域提供：欧洲地区（斯德哥尔摩）、亚太地区（孟买）、美国东部（俄亥俄州）、欧洲地区（爱尔兰）、欧洲地区（法兰克福）、亚太地区（香港）、美国东部（弗吉尼亚州北部）、亚太地区（首尔）、欧洲地区（伦敦）、亚太地区（东京)、美国西部（俄勒冈州）、亚太地区（新加坡）、亚太地区（悉尼）、加拿大（中部）

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

fsx-resources-protected-by-backup-plan

检查 Amazon FSx 文件系统是否受备份计划的保护。如果备份计划不涵盖 Amazon FSx 文件系统，则此规则为 NON_COMPLIANT。

标识符：FSX_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型： AWS::FSx::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Amazon FSx 文件系统的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon FSx 文件系统的 ID。

crossRegionList （可选）, 类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （可选）, 类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （可选）, 类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （可选）, 类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选）, 类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

fsx-windows-audit-log-configured

检查适用于 Windows File Server 的 Amazon FSx 文件系统是否启用了文件访问审核。如果适用于 Windows File Server 的 FSx 文件系统未启用文件访问审核，则此规则为 NON_COMPLIANT。

标识符：FSX_WINDOWS_AUDIT_LOG_CONFIGURED

资源类型： AWS::FSx::FileSystem

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

global-endpoint-event-replication-enabled

检查是否为 Amazon EventBridge 全球终端节点启用了事件复制。如果未启用事件复制，则此规则为 NON_COMPLIANT。

标识符：GLOBAL_ENDPOINT_EVENT_REPLICATION_ENABLED

资源类型： AWS::Events::Endpoint

触发器类型： 配置更改

AWS 区域：仅在欧洲（斯德哥尔摩）、亚太地区（孟买）、欧洲（巴黎）、美国东部（俄亥俄州）、欧洲（爱尔兰）、欧洲（法兰克福）、南美洲（圣保罗）、美国东部（弗吉尼亚北部）、亚太地区（首尔）、亚太地区（大阪）、欧洲（伦敦）、亚太地区（东京）、美国西部（俄勒冈）、美国西部（加利福尼亚北部）、亚太地区（新加坡）、亚太地区（大阪）、欧洲（伦敦）、亚太地区（东京）、美国

西部（俄勒冈）、美国西部（加利福尼亚北部）、亚太地区（新加坡）、亚太地区（大阪）、欧洲（伦敦）、亚太地区（东京）、美国西部（悉尼)、加拿大（中部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 guardduty-eks 保护审计

检查您账户中的亚马逊探测器是否启用了亚马逊 Elastic Kubernetes Service（亚马逊 EKS）的审计日志监控。 GuardDuty 如果您的账户未启用 EKS 审核日志监控功能，则该规则不合规。

标识符：GUARDDUTY_EKS_PROTECTION_AUDIT

资源类型： AWS::GuardDuty::Detector

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

启用 guardduty-eks 保护运行时

检查您的账户中是否为 GuardDuty 检测器启用了具有自动代理管理功能的 Amazon EKS 运行时监控。如果您的账户未启用带有自动代理管理功能的 EKS 运行时监控，则 GuardDuty 该规则不合规。

标识符：GUARDDUTY_EKS_PROTECTION_RUNTIME

资源类型： AWS::GuardDuty::Detector

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

guardduty-enabled-centralized

检查您的 AWS 账户和 AWS 地区 GuardDuty 是否启用了亚马逊。如果您提供集中 AWS 账户，则该规则将评估集中账户中的 GuardDuty 结果。启用后，该规则 GuardDuty 即为合规。

标识符：GUARDDUTY_ENABLED_CENTRALIZED

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

CentralMonitoringAccount （可选）, 类型：字符串

以逗号分隔的 AWS 账户（12 位数）列表，允许集中管理亚马逊 GuardDuty 结果。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

启用 guardduty-lambda 保护

检查您账户中的亚马逊 GuardDuty 探测器是否启用了 Lambda 保护。如果您的账户未启用 Amazon 中的 Lambda 保护功能，则 GuardDuty 该规则不合规。

标识符：GUARDDUTY_LAMBDA_PROTECTION_

资源类型： AWS::GuardDuty::Detector

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 guardduty 恶意软件防护

检查您账户中的Amazon GuardDuty 探测器是否启用了恶意软件防护。如果您的账户未启用 Amazon 中的恶意软件防护功能，则 GuardDuty 该规则不合规。

标识符：GUARDDUTY_恶意软件_ 保护_已启用

资源类型： AWS::GuardDuty::Detector

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

guardduty-non-archived-findings

检查 Amazon 是否 GuardDuty 有未存档的调查结果。如果 GuardDuty 存在未存档的低/中/高严重性搜索结果早于 /days/参数中的指定数字，则该规则为 NON_COMPLIMENT。 daysLowSev MediumSev `daysHighSev`

标识符：GUARDDUTY_NON_ARCHIVED_FINDINGS

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

daysLowSev （可选）, 类型：int, 默认：30

允许 Amazon GuardDuty 低严重性调查结果处于非存档状态的天数。默认值为 30 天。

daysMediumSev （可选）, 类型：int, 默认：7

Amazon GuardDuty 中等严重性调查结果允许处于非存档状态的天数。默认值为 7 天。

daysHighSev （可选）, 类型：int, 默认值：1

允许 Amazon GuardDuty 高严重性调查结果处于非存档状态的天数。默认值为 1 天。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 guardduty-rds 保护

检查您账户中的亚马逊 GuardDuty 探测器是否启用了亚马逊关系数据库服务 (Amazon RDS) 保护。如果您的账户未启用亚马逊中的 Amazon RDS 保护功能，则 GuardDuty 该规则不合规。

标识符：启用 GUARDDUTY_RDS_PROTECTION_

资源类型： AWS::GuardDuty::Detector

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 guardduty-s3 保护

检查您账户中的亚马逊 GuardDuty 探测器是否启用了 S3 保护。如果您的账户未启用 Amazon 中的 S3 保护功能，则 GuardDuty 该规则不合规。

标识符：GUARDDUTY_S3_PROTECTION_ABLED

资源类型： AWS::GuardDuty::Detector

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-customer-policy-blocked-kms-actions

检查您创建的托管 AWS 身份和访问管理 (IAM) 策略是否不允许对 KMS 密钥执行阻止操作 AWS 。如果托管 IAM 策略允许对 AWS KMS 密钥执行任何阻止的操作，则该规则不合规。

> **Note**
>
> 此规则不评估 IAM 策略中的变量或条件。有关更多信息，请参阅 IAM 用户指南中的 IAM 策略元素：变量和 IAM JSON 策略元素：条件。

标识符：IAM_CUSTOMER_POLICY_BLOCKED_KMS_ACTIONS

资源类型： AWS::IAM::Policy

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

被封锁 ActionsPatterns, 类型：CSV

被阻止的 KMS 操作模式列表（以逗号分隔）。例如，您可以将 kms: decrypt* 或 kms: 列为已屏蔽的操作模式。ReEncrypt 如果托管式 IAM 策略允许此参数中列出的任何操作模式，则此规则为 NON_COMPLIANT。

排除PermissionBoundaryPolicy （可选）, 类型：布尔值

布尔标志，用于排除对用作权限边界的 IAM 策略的评估。如果设置为“true”，则此规则将不会在评估中包含权限边界。否则，当值设置为“false”时，系统会评估范围内的所有的 IAM 策略。默认值为“false”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam 外部访问分析器已启用

检查每个区域是否在您的账户中激活了用于外部访问的 IAM 访问分析器。如果该区域没有用于外部访问的分析器，或者 “状态” 属性未设置为 “活动”，则该规则为 “不合规”。

标识符：IAM_EXTERNAL_ACCESS_ANALYZER_ENABLED

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-group-has-users-check

检查 IAM 组是否至少拥有一个 IAM 用户。

标识符：IAM_GROUP_HAS_USERS_CHECK

资源类型： AWS::IAM::Group

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-inline-policy-blocked-kms-actions

检查附加到您的 IAM 用户、角色和群组的内联策略是否不允许对所有 AWS KMS 密钥执行阻止操作。如果允许对内联策略中的所有 AWS KMS 密钥执行任何阻止操作，则该规则为 NON_COMPLIMENT。

标识符：IAM_INLINE_POLICY_BLOCKED_KMS_ACTIONS

资源类型： AWS::IAM::Group、 AWS::IAM::Role、 AWS::IAM::User

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

被封锁 ActionsPatterns, 类型：CSV

以逗号分隔的已屏蔽的 KMS 操作模式列表，例如 kms: *、kms: *、kms: decrypt、kms: *。ReEncrypt

排除RoleByManagementAccount （可选）, 类型：布尔值

如果某个角色只能由组织管理账户代入，则将其排除在外。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-no-inline-policy-check

检查内联策略特征是否未使用。如果 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组有任何内联策略，则该规则不合规。

标识符：IAM_NO_INLINE_POLICY_CHECK

资源类型： AWS::IAM::User、 AWS::IAM::Role、 AWS::IAM::Group

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-password-policy

检查 AWS 身份和访问管理 (IAM) Management 用户的账户密码策略是否符合参数中指示的指定要求。如果账户密码策略不符合指定要求，则此规则为 NON_COMPLIANT。

> **Important**
>
> 规则参数的 `true` 和 `false` 值区分大小写。如果 `true` 未以小写形式提供，则将其视为 `false`.

> **Note**
>
> 默认 IAM 密码策略的评估结果

使用默认 IAM 密码策略时，此规则会被标记为 “不合规”。
托管规则和全球 IAM 资源类型
2022 年 2 月之前加入的全球 IAM 资源类型
（`AWS::IAM::GroupAWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。
如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。
为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

标识符：IAM_PASSWORD_POLICY

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

RequireUppercaseCharacters （可选）, 类型：布尔值, 默认：True

密码中要求至少包含一个大写字符。

RequireLowercaseCharacters （可选）, 类型：布尔值, 默认：True

密码中要求至少包含一个小写字符。

RequireSymbols （可选）, 类型：布尔值, 默认：True

密码中要求至少包含一个符号。

RequireNumbers （可选）, 类型：布尔值, 默认：True

密码中要求至少包含一个数字。

MinimumPasswordLength （可选）, 类型：int, 默认值：14

密码最小长度。

PasswordReusePrevention （可选）, 类型：int, 默认值：24

允许重用前的密码数。

MaxPasswordAge （可选）, 类型：int, 默认值：90

密码到期前的天数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-policy-blacklisted-check

检查每个 AWS 身份和访问管理 (IAM) Access Management 资源，输入参数中的策略亚马逊资源名称 (ARN) 是否附加到该 IAM 资源。如果策略 ARN 已附加到 IAM 资源，则此规则为 NON_COMPLIANT。

标识符：IAM_POLICY_BLACKLISTED_CHECK

资源类型： AWS::IAM::User、 AWS::IAM::Group、 AWS::IAM::Role

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

policyArns, 类型：CSV, 默认：arn: aws: iam:: aws: policy/ AdministratorAccess

IAM 策略 ARN 的逗号分隔列表，不应将这些 ARN 附加到任何 IAM 实体。

exceptionList（可选）, 类型：CSV

以逗号分隔的资源类型列表和资源名称对列表。例如，users:[user1;user2], groups:[group1;group2], roles:[role1;role2;role3]。

> **Note**
>
> 在例外列表中，请指定资源的名称而不是完整的 ARN。无效:`arn:aws:iam::444455556666:role/Admin`. 有效：`Admin`。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-policy-in-use

检查 IAM 策略 ARN 是否附加到 IAM 用户，或包含一个或多个 IAM 用户的组，或包含一个或多个受信任实体的 IAM 角色。

> **Note**
>
> 托管规则和全球 IAM 资源类型
>
> 2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。
>
> 如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。
>
> 为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

标识符： IAM_POLICY_IN_USE

资源类型： AWS::IAM::Policy

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

policyARN, 类型：字符串

要检查的 IAM 策略 ARN。

policyUsageType（可选），类型：字符串

指定是否希望将策略附加到 IAM 用户、组或角色。有效值为 IAM_USER、IAM_GROUP、IAM_ROLE 或 ANY。默认值为 ANY。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-policy-no-statements-with-admin-access

检查您创建的 AWS 身份和访问管理 (IAM) 策略是否包含允许语句，这些语句授予对所有资源执行所有操作的权限。如果任何客户管理型 IAM 策略语句具有 "Effect": "Allow" with "Action": "*" over "Resource": "*"，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则仅评估客户管理型策略。此规则不评估内联策略或 AWS 托管策略。有关差异的更多信息，请参阅《IAM 用户指南》中的托管式策略与内联策略。

以下策略为 NON_COMPLIANT：

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
```

以下策略为 COMPLIANT：

```
"Statement": [
{
"Sid": "VisualEditor",
"Effect": "Allow",
"Action": "service:*",
"Resource": "*"
```

```
}
```

标识符：IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS

资源类型： AWS::IAM::Policy

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

排除PermissionBoundaryPolicy （可选），类型：布尔值

布尔标志，用于排除对用作权限边界的 IAM 策略的评估。如果设置为“true”，则此规则将不会在评估中包含权限边界。否则，当值设置为“false”时，系统会评估范围内的所有的 IAM 策略。默认值为“false”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-policy-no-statements-with-full-access

检查您创建的 Ident AWS ity and Access Management (IAM) 策略是否授予对单个资源执行所有操作的权限。 AWS 如果任何客户托管的 IAM 策略允许对至少 1 AWS 项服务的完全访问权限，则该规则不合规。

上下文：根据最低权限原则，建议在向 AWS 服务授予权限时限制您的 IAM 策略中允许的操作。这种方法有助于确保您仅通过指定所需的确切操作来授予必要的权限，避免对服务使用不受限制的通配符，例如。`ec2:*`

在某些情况下，您可能希望允许使用相似前缀的多个操作，例如DescribeFlow日志和DescribeAvailability区域。在这些情况下，可以在常用前缀中添加带后缀的通配符（例如，）。`ec2:Describe*`分组相关操作有助于避免达到 I AM 策略大小限制。

如果您使用带有后缀通配符的前缀操作（例如），则此规则将返回COMPLIMENT。`ec2:Describe*`仅当您使用不受限制的通配符（例如）时，此规则才会返回NON_COMPLIMITY。`ec2:*`

> **Note**
>
> 此规则仅评估客户管理型策略。此规则不评估内联策略或 AWS 托管策略。有关差异的更多信息，请参阅《IAM 用户指南》中的托管式策略与内联策略。

标识符：IAM_POLICY_NO_STATEMENTS_WITH_FULL_ACCESS

资源类型： AWS::IAM::Policy

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

排除PermissionBoundaryPolicy （可选），类型：布尔值

布尔标志，用于排除对用作权限边界的 IAM 策略的评估。如果设置为“true”，则此规则将不会在评估中包含权限边界。否则，当值设置为“false”时，系统会评估范围内的所有的 IAM 策略。默认值为“false”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-role-managed-policy-check

检查托管策略列表中指定的所有托管策略是否都附加到 AWS 身份和访问管理 (IAM) 角色。如果管理型策略未附加到 IAM 角色中，则此规则为 NON_COMPLIANT。

标识符：IAM_ROLE_MANAGED_POLICY_CHECK

资源类型： AWS::IAM::Role

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

管理 PolicyArns, 类型：CSV

以逗号分隔的 AWS 托管策略 Amazon 资源名称 (ARN) 列表。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 资源名称 (ARN) 和 AWS 托管策略。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-root-access-key-check

检查根用户访问密钥是否可用。如果用户访问密钥不存在，则此规则为 COMPLIANT。否则，将为 NON_COMPLIANT。

> **Note**
>
> 托管规则和全球 IAM 资源类型
> 2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。
> 如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。
> 为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

标识符：IAM_ROOT_ACCESS_KEY_CHECK

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam 服务器证书到期检查

检查存储在 AWS IAM 中的 IAM SSL/TLS 服务器证书是否已过期。如果 IAM 服务器证书已过期，则该规则不合规。

标识符：IAM_SERVER_CERTICATE_EX PILATION_C

资源类型： AWS::IAM::ServerCertificate

触发器类型： 定期

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-user-group-membership-check

检查 IAM 用户是否为至少一个 IAM 组的成员。

标识符：IAM_USER_GROUP_MEMBERSHIP_CHECK

资源类型： AWS::IAM::User

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

groupNames（可选），类型：字符串

IAM 用户必须是其成员的 IAM 组的逗号分隔列表。

> **Note**
>
> 此规则不支持带有逗号的组名。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-user-mfa-enabled

检查 AWS 身份和访问管理 (IAM) Access Management 用户是否启用了多重身份验证 (MFA)。如果没有为至少一个 IAM 用户启用 MFA，则此规则为 NON_COMPLIANT。

> **Note**
>
> 托管规则和全球 IAM 资源类型
> 2022 年 2 月之前加入的全球 IAM 资源类型
> （`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。
> 如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。
> 为避免不必要的评估，您只应定期部署规则，向支持的区域之一报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

标识符：IAM_USER_MFA_ENABLED

资源类型： AWS::IAM::User

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-user-no-policies-check

检查您的 AWS 身份和访问管理 (IAM) Access Management 用户是否都没有附加策略。IAM 用户必须继承来自 IAM 组或角色的权限。如果至少有一个 IAM 用户附加了策略，则此规则为 NON_COMPLIANT。

标识符：IAM_USER_NO_POLICIES_CHECK

资源类型： AWS::IAM::User

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

iam-user-unused-credentials-check

检查您的 AWS Identity and Access Management (IAM) 用户是否拥有在您提供的指定天数内未使用的密码或有效访问密钥。如果存在最近未使用的非活动账户，则此规则为 NON_COMPLIANT。

> **Note**
>
> 重新评估时间表
>
> 在首次评估后的 4 小时内重新评估此规则将不会对结果产生影响。
>
> 托管规则和全球 IAM 资源类型

2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。

为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

标识符：IAM_USER_UNUSED_CREDENTIALS_CHECK

资源类型： AWS::IAM::User

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大CredentialUsage年龄, 类型：int, 默认值：90

无法使用凭证的最大天数。默认值为 90 天。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

restricted-ssh

> **Important**
>
> 对于此规则，规则标识符 (INCOMING_SSH_DISABLED) 和规则名称 (restricted-ssh) 是不同的。

检查安全组的传入 SSH 流量是否可访问。如果安全组中的传入 SSH 流量的 IP 地址受限（CIDR 而不是 0.0.0.0/0 或 ::/0），则此规则为 COMPLIANT。否则，将为 NON_COMPLIANT。

标识符：INCOMING_SSH_DISABLED

资源类型： AWS::EC2::SecurityGroup

触发器类型：配置更改和定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 inspector-ec2-scan

检查您的单账户或多账户环境是否已激活 Amazon Inspector V2 EC2 扫描，以检测您的 EC2 实例上的潜在漏洞和网络可访问性问题。如果未激活 EC2 扫描，则该规则不合规。

标识符：INSPECTOR_EC2_SCAN_ ENABLED

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

支持 inspector-ecr-scan

检查您的单账户或多账户环境是否已激活 Amazon Inspector V2 ECR 扫描，以检测容器映像中潜在的软件漏洞。如果未激活 ECR 扫描，则该规则不兼容。

标识符：INSPECTOR_ECR_SCAN_ ENABLED

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 inspector-lambda 代码扫描功能

检查您的单账户或多账户环境是否已激活 Amazon Inspector V2 Lambda 代码扫描，以检测潜在的代码漏洞。如果未激活 Lambda 代码扫描，则该规则不合规。

标识符：检查器_LAMBDA_CODE_SCAN_ENABLED

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域：仅在欧洲（斯德哥尔摩）、美国东部（俄亥俄州）、欧洲（爱尔兰）、欧洲（法兰克福）、美国东部（弗吉尼亚北部）、欧洲（伦敦）、亚太地区（东京）、美国西部（俄勒冈）、亚太地区（新加坡）、亚太地区（悉尼）地区提供

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 inspector-lambda 标准扫描功能

检查您的单账户或多账户环境是否已激活 Amazon Inspector V2 Lambda 标准扫描，以检测潜在的软件漏洞。如果未激活 Lambda 标准扫描，则该规则不合规。

标识符：INSPECTOR_LAMBDA_标准_ 扫描_启用

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ec2-instances-in-vpc

> **Important**
>
> 对于此规则，规则标识符 (INSTANCES_IN_VPC) 和规则名称 (ec2-instances-in-vpc) 是不同的。

检查您的 EC2 实例是否属于某个虚拟私有云 (VPC)。或者，您可以指定要与您的实例关联的 VPC ID。

标识符：INSTANCES_IN_VPC

资源类型： AWS::EC2::Instance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

vpcId（可选），类型：字符串

包含这些 EC2 实例的 VPC ID。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

internet-gateway-authorized-vpc-only

检查互联网网关是否连接到授权的虚拟私有云 (Amazon VPC)。如果互联网网关连接到未经授权的 VPC，则此规则为 NON_COMPLIANT。

标识符：INTERNET_GATEWAY_AUTHORIZED_VPC_ONLY

资源类型： AWS::EC2::InternetGateway

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

AuthorizedVpcIds （可选），类型：字符串

带有附加 iGW 的授权 VPC ID 的逗号分隔列表。如果未提供此参数，则所有附加的 IGW 将为 NON_COMPLIANT。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

kinesis-firehose-delivery-stream 加密

检查 Amazon Kinesis Data Firehose 传送流是否使用服务器端加密进行静态加密。如果 Kinesis Data Firehose 传输流未使用服务器端加密进行静态加密，则该规则不合规。

标识符：KINESIS_FIREHOSE_DELIVERY_DELIVERY_

资源类型： AWS::KinesisFirehose::DeliveryStream

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyArns （可选），类型：CSV

获准使用 Kinesis Firehose 的 KMS 密钥 Arn 列表，以逗号分隔。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

kinesis-stream-encrypted

检查 Amazon Kinesis 流是否使用服务器端加密进行加密。如果不存在 “StreamEncryption”，则该规则不符合 Kinesis 直播的规则。

背景：服务器端加密是 Amazon Kinesis Data Streams 中的一项功能，它使用 AWS KMS 密钥在数据静止之前自动对其进行加密。数据在写入 Kinesis 流存储层之前加密，并在从存储检索到之后进行解密。因此，在 Kinesis Data Streams 服务中对数据进行静态加密。这有助于您满足监管要求并增强您数据的安全性。有关更多信息，请参阅 Amazon Kinesis Data Streams 数据保护。

标识符：KINESIS_STREAM_ENCRYPTED

资源类型： AWS::Kinesis::Stream

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

kms-cmk-not-scheduled-for-deletion

检查 AWS 密钥管理服务 (AWS KMS) 密钥是否未计划在 AWS KMS 中删除。如果计划删除 KMS 密钥，则该规则不合规。

标识符：KMS_CMK_NOT_SCHEDULED_FOR_DELETION

资源类型： AWS::KMS::Key

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyIds （可选），类型：字符串

（可选）未计划删除的特定客户管理型密钥 ID 的逗号分隔列表。如果未指定任何密钥，则规则将检查所有密钥。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

lambda-concurrency-check

检查 Lambda 函数是否配置了函数级并发执行限制。如果 Lambda 函数未配置函数级并发执行限制，则此规则为 NON_COMPLIANT。

标识符：LAMBDA_CONCURRENCY_CHECK

资源类型： AWS::Lambda::Function

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

ConcurrencyLimitLow （可选）, 类型：字符串

最小并发执行限制

ConcurrencyLimitHigh （可选）, 类型：字符串

最大并发执行限制

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

lambda-dlq-check

检查 Lambda 函数是否配置了死信队列。如果 Lambda 函数未配置死信队列，则此规则为 NON_COMPLIANT。

标识符：LAMBDA_DLQ_CHECK

资源类型： AWS::Lambda::Function

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

dlqArns（可选）, 类型：字符串

必须配置为 Lambda 函数死信队列目标的 Amazon SQS 和 Amazon SNS ARN 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

lambda-function-public-access-prohibited

检查附加到 Lambda 资源的 AWS Lambda 函数策略是否禁止公开访问。如果 Lambda 函数策略允许公开访问，则此规则为 NON_COMPLIANT。

上下文：如果主体元素为空或包含通配符，则 lambda 函数策略被视为允许公开访问。例如，如果主元素为“”或{“AWS”: “”}。出于安全考虑，不建议授予公共访问权限。限制公开访问可以帮助您防止未经授权的 Lambda 函数被调用，这可能会危害您的数据或产生不必要的费用。

要限制对您的 Lambda 函数的访问，请指定可以调用这些函数的 IAM 用户、角色或服务的 AWS 账户 ID 或 Amazon 资源名称 (ARN)。有关更多信息，请参阅《AWS Lambda 开发者指南》中的向其他账户授予函数访问权限。

标识符：LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED

资源类型： AWS::Lambda::Function

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

lambda-function-settings-check

检查运行时间、角色、超时和内存大小的 AWS Lambda 函数设置是否与预期值相匹配。该规则忽略包类型为 “Image” 的函数和运行时设置为 “仅限操作系统的运行时” 的函数。如果 Lambda 函数设置与预期值不匹配，则此规则为 NON_COMPLIANT。

标识符：LAMBDA_FUNCTION_SETTINGS_CHECK

资源类型： AWS::Lambda::Function

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

runtime, 类型：CSV

以逗号分隔的 Lambda 运行 AWS 时值列表

role（可选）, 类型：字符串

Lambda AWS 执行角色的名称或 ARN

timeout（可选）, 类型：int, 原定设置值：3

AWS Lambda 函数超时时间（以秒为单位）

memorySize（可选）, 类型：int, 默认值：128

AWS Lambda 函数的大小（以兆字节为单位）

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
    "MemorySize": Integer*,
    "Role": String*,
    "Runtime": String*,
    "Timeout": Integer*
}
...
```

* 有关这些输入有效值的更多信息，请参阅MemorySize《 AWS CloudFormation 用户指南》中的 “角色”、“运行时间” 和 “超时”。

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

lambda-inside-vpc

检查是否允许 Lambda 函数访问虚拟私有云 (VPC)。如果 Lambda 函数未启用 VPC，则此规则为 NON_COMPLIANT。

标识符：LAMBDA_INSIDE_VPC

资源类型： AWS::Lambda::Function

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

subnetIds（可选），类型：字符串

Lambda 函数必须与之关联的子网 ID 的逗号分隔列表。

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "VpcConfig": {
         "SubnetIds": "[SubnetId-1, SubnetId-2, SubnetId-3, ...]"
   }
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

lambda-vpc-multi-az-check

检查 Lambda 是否关联了多个可用区。如果只有 1 个可用区与 Lambda 关联，或关联的可用区数量少于可选参数中指定的数量，则此规则为 NON_COMPLIANT。

标识符：LAMBDA_VPC_MULTI_AZ_CHECK

资源类型： AWS::Lambda::Function

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

availabilityZones（可选），类型：int

预期的可用区数量。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

macie自动敏感数据发现检查

检查是否为 Amazon Macie 启用了自动敏感数据发现功能。如果禁用自动敏感数据发现，则该规则不合规。该规则适用于管理员帐户，而不适用于成员帐户。

标识符：MACIE_AUTO_SENSITIVE_DASCIVERY_CHEC

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

macie-status-check

检查每个区域的账户中是否启用了 Amazon Macie。如果“status”属性未设置为“ENABLED”，则此规则为 NON_COMPLIANT。

标识符：MACIE_STATUS_CHECK

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

mfa-enabled-for-iam-console-access

检查是否为 AWS 所有使用控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户启用了多重身份验证 (MFA)。如果已启用 MFA，则此规则为 COMPLIANT。

> **Note**
>
> 重新评估时间表
> 在首次评估后的 4 小时内重新评估此规则将不会对结果产生影响。
> 托管规则和全球 IAM 资源类型
> 2022 年 2 月之前加入的全球 IAM 资源类型
> （`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月

AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。
如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。
为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

标识符：MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS

资源类型： AWS::IAM::User

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

mq-active-deployment-mode

检查为 Amazon MQ ActiveMQ 代理引擎配置的部署模式。如果使用的是默认的单实例代理模式，则此规则为 NON_COMPLIANT。

标识符：MQ_ACTIVE_DEPLOYMENT_MODE

资源类型： AWS::AmazonMQ::Broker

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

mq-automatic-minor-version-upgrade-enabled

检查 Amazon MQ 代理是否启用了自动次要版本升级。如果未为 Amazon MQ 代理启用 AutoMinor VersionUpgrade “” 字段，则该规则不合规。

标识符：MQ_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

资源类型： AWS::AmazonMQ::Broker

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

mq-auto-minor-version-upgrade-enabled

检查 Amazon MQ 代理是否启用了自动次要版本升级。如果未为 Amazon MQ 代理启用 AutoMinor VersionUpgrade “” 字段，则该规则不合规。

标识符：MQ_AUTO_MINOR_VERSION_EVERSION_UP

资源类型： AWS::AmazonMQ::Broker

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

mq-cloudwatch-audit-logging-enabled

检查 Amazon MQ 经纪人是否启用了亚马逊 CloudWatch 审核日志。如果代理未启用审核日志记录，则此规则为 NON_COMPLIANT。

标识符：MQ_CLOUDWATCH_AUDIT_LOGGING_ENABLED

资源类型： AWS::AmazonMQ::Broker

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 mq-cloudwatch 审计日志

检查 Amazon MQ 代理是否启用了 CloudWatch 审计日志。如果代理未启用审核日志，则该规则为 NON_Complift。

标识符：已启用 MQ_CLOUDWATCH_AUDIT_

资源类型： AWS::AmazonMQ::Broker

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

mq-no-public-access

检查 Amazon MQ 代理是否不可公开访问。如果亚马逊 MQ 经纪商的 “PubliclyAccessible” 字段设置为 true，则该规则不合规。

标识符：MQ_NO_PUBLIC_ACCESS

资源类型： AWS::AmazonMQ::Broker

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

mq-rabbit-deployment-mode

检查为 Amazon MQ RabbitMQ 代理引擎配置的部署模式。如果使用的是默认的单实例代理模式，则此规则为 NON_COMPLIANT。

标识符：MQ_RABBIT_DEPLOYMENT_MODE

资源类型： AWS::AmazonMQ::Broker

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

msk-enhanced-monitoring-enabled

检查是否为设置为 PER_TOPIC_PER_BROKER 或 PER_TOPIC_PER_PARTITION 的 Amazon MSK 集群启用了增强监控。如果启用了增强监控并设置为 DEFAULT 或 PER_BROKER，则此规则为 NON_COMPLIANT。

标识符：MSK_ENHANCED_MONITORING_ENABLED

资源类型： AWS::MSK::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

msk-in-cluster-node-require-tls

检查 Amazon MSK 集群是否使用 HTTPS (TLS) 对集群的代理节点进行传输中加密。如果为集群内代理节点连接启用了纯文本通信，则此规则为 NON_COMPLIANT。

标识符：MSK_IN_CLUSTER_NODE_REQUIRE_TLS

资源类型： AWS::MSK::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

multi-region-cloudtrail-enabled

> **Important**
>
> 对于此规则，规则标识符 (MULTI_REGION_CLOUD_TRAIL_ENABLED) 和规则名称 (multi-region-cloudtrail-enabled) 是不同的。

检查是否至少有一个多区域 AWS CloudTrail。如果跟踪与输入参数不匹配，则此规则为 NON_COMPLIANT。如果该`ExcludeManagementEventSources`字段不为空或配置为排除管理事件（例如 AWS KMS 事件或 Amazon RDS 数据 API 事件），则 AWS CloudTrail 该规则不合规。

标识符：MULTI_REGION_CLOUD_TRAIL_ENABLED

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

s3BucketName（可选），类型：字符串

用于 AWS CloudTrail 向其传送日志文件的 Amazon S3 存储桶的名称。

snsTopicArn（可选），类型：字符串

用于通知的 Amazon SNS 主题 ARN AWS CloudTrail 。

云WatchLogsLogGroupArn（可选），类型：字符串

AWS CloudTrail 要向其发送数据的亚马逊 CloudWatch 日志组 ARN。

includeManagementEvents（可选），类型：布尔值

事件选择器，用于包括的管理事件 AWS CloudTrail。

readWriteType （可选），类型：字符串

要记录的事件的类型。有效值为 ReadOnly、 WriteOnly 和 ALL。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

nacl-no-unrestricted-ssh-rdp

检查网络访问控制列表 (NACL) 的 SSH/RDP 入口流量的默认端口是否不受限制。如果 NACL 入站条目允许端口 22 或 3389 使用源 TCP 或 UDP CIDR 块，则此规则为 NON_COMPLIANT。

标识符：NACL_NO_UNRESTRICTED_SSH_RDP

资源类型： AWS::EC2::NetworkAcl

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

neptune-cluster-backup-retention-check

检查 Amazon Neptune 数据库集群的保留期是否设置为特定天数。如果保留期小于参数指定的值，则此规则为 NON_COMPLIANT。

标识符：NEPTUNE_CLUSTER_BACKUP_RETENTION_CHECK

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

最低BackupRetentionPeriod （可选），类型：int

备份应保留最少天数。有效值为 1 到 35，默认值为 7。如果值大于 “RetentionPeriod备份”，则该规则不合规。如果值小于或等于 “备份RetentionPeriod”，则该规则合规。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

neptune-cluster-cloudwatch-log-export-enabled

检查 Amazon Neptune 集群是否为审计 CloudWatch 日志启用了日志导出功能。如果 Neptune 集群没有为审计日志启用 CloudWatch 日志导出功能，则该规则不合规。

标识符：NEPTUNE_CLUSTER_CLOUDWATCH_LOG_EXPORT_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

neptune-cluster-copy-tags-to-snapshot-enabled

检查 Amazon Neptune 集群是否配置为在创建快照时将所有标签复制到快照。如果 “复制TagsTo快照” 设置为 false，则该规则不兼容。

标识符：NEPTUNE_CLUSTER_COPY_TAGS_TO_SNAPSHOT_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

neptune-cluster-deletion-protection-enabled

检查 Amazon Neptune 数据库集群是否已启用删除保护。如果 Amazon Neptune 集群的 deletionProtection 字段设置为 false，则此规则为 NON_COMPLIANT。

标识符：NEPTUNE_CLUSTER_DELETION_PROTECTION_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

neptune-cluster-encrypted

检查您的 Amazon Neptune 数据库集群是否启用了存储加密。如果未启用存储加密，则此规则为 NON_COMPLIANT。

标识符：NEPTUNE_CLUSTER_ENCRYPTED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

KmsKeyArns （可选），类型：CSV

以逗号分隔的 KMS 密钥 ARN 列表，用于与加密集群 KmsKeyId 的密钥 ARN 进行比较。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

neptune-cluster-iam-database-authentication

检查 Amazon Neptune 集群是否启用了 AWS 身份和访问管理 (IAM) 数据库身份验证。如果 Amazon Neptune 集群未启用 IAM 数据库身份验证，则此规则为 NON_COMPLIANT。

标识符：NEPTUNE_CLUSTER_IAM_DATABASE_AUTHENTICATION

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

neptune-cluster-multi-az-enabled

检查 Amazon Neptune 集群是否配置了 Amazon RDS Multi-AZ 复制功能。如果未启用 Multi-AZ 复制功能，则此规则为 NON_COMPLIANT。

标识符：NEPTUNE_CLUSTER_MULTI_AZ_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

neptune-cluster-snapshot-encrypted

检查 Amazon Neptune 数据库集群是否已加密快照。如果 Neptune 集群没有加密快照，则此规则为 NON_COMPLIANT。

标识符：NEPTUNE_CLUSTER_SNAPSHOT_ENCRYPTED

资源类型：AWS:: RDS:: DB ClusterSnapshot

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

neptune-cluster-snapshot-public-prohibited

检查 Amazon Neptune 手动数据库集群快照是否是公有的。如果任何现有和新的 Neptune 集群快照是公有的，则此规则为 NON_COMPLIANT。

标识符：NEPTUNE_CLUSTER_SNAPSHOT_PUBLIC_PROHIBITED

资源类型：AWS:: RDS:: DB ClusterSnapshot

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

netfw-deletion-protection-enabled

检查 AWS Network Firewall 是否启用了删除保护。如果网络防火墙未启用删除保护，则此规则为 NON_COMPLIANT。

标识符：NETFW_DELETION_PROTECTION_ENABLED

资源类型： AWS::NetworkFirewall::Firewall

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

netfw-logging-enabled

检查 AWS Network Firewall 防火墙是否启用了日志记录。如果未配置日志记录类型，则此规则为 NON_COMPLIANT。您可以指定希望规则检查的日志记录类型。

标识符：NETFW_LOGGING_ENABLED

资源类型： AWS::NetworkFirewall::LoggingConfiguration

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

logType（可选），类型：字符串

要检查防火墙规则的日志类型：“alert”、“flow”或“both”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

netfw-multi-az-enabled

检查 AWS Network Firewall 防火墙是否部署在多个可用区域中。如果防火墙仅部署在一个可用区或少于可选参数中列出的数量的可用区，则此规则为 NON_COMPLIANT。

标识符：NETFW_MULTI_AZ_ENABLED

资源类型： AWS::NetworkFirewall::Firewall

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

availabilityZones（可选），类型：int

预期的可用区数量。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

netfw-policy-default-action-fragment-packets

检查 AWS Network Firewall 策略是否配置了针对碎片数据包的用户定义的无状态默认操作。如果针对分段数据包的无状态默认操作与用户定义的默认操作不匹配，则此规则为 NON_COMPLIANT。

标识符：NETFW_POLICY_DEFAULT_ACTION_FRAGMENT_PACKETS

资源类型： AWS::NetworkFirewall::FirewallPolicy

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无国籍FragmentDefault操作, 类型：CSV

值的逗号分隔列表。您最多可以选择两个。有效值包括“aws:pass”、“aws:drop”和“aws:forward_to_sfe”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

netfw-policy-default-action-full-packets

检查 AWS Network Firewall 策略是否配置了针对完整数据包的用户定义的默认无状态操作。如果针对完整数据包的默认无状态操作与用户定义的默认无状态操作不匹配，则此规则为 NON_COMPLIANT。

标识符：NETFW_POLICY_DEFAULT_ACTION_FULL_PACKETS

资源类型： AWS::NetworkFirewall::FirewallPolicy

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无国籍 DefaultActions, 类型：CSV

值的逗号分隔列表。您最多可以选择两个。有效值包括“aws:pass”、“aws:drop”和“aws:forward_to_sfe”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

netfw-policy-rule-group-associated

检查 AWS Network Firewall 策略是否与有状态或无状态规则组相关联。如果没有有状态或无状态规则组与网络防火墙策略相关联，则此规则为 NON_COMPLIANT；如果存在任一规则组，则此规则为 COMPLIANT。

标识符：NETFW_POLICY_RULE_GROUP_ASSOCIATED

资源类型： AWS::NetworkFirewall::FirewallPolicy

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

netfw-stateless-rule-group-not-empty

检查无状态网络防火墙规则组是否包含规则。如果无状态网络防火墙规则组中没有规则，则此规则为 NON_COMPLIANT。

标识符：NETFW_STATELESS_RULE_GROUP_NOT_EMPTY

资源类型： AWS::NetworkFirewall::RuleGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

nlb-cross-zone-load-balancing-enabled

检查网络负载均衡器 (NLB) 上是否启用了跨区域负载均衡。如果 NLB 未启用跨区域负载均衡，则此规则为 NON_COMPLIANT。

标识符：NLB_CROSS_ZONE_LOAD_BALANCING_ENABLED

资源类型： AWS::ElasticLoadBalancingV2::LoadBalancer

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

no-unrestricted-route-to-igw

检查路由表中是否有通向互联网网关 (IGW) 的公共路由。如果通向 IGW 的路由的目标 CIDR 块为“0.0.0.0/0”或“::/0”，或者目标 CIDR 块与规则参数不匹配，则此规则为 NON_COMPLIANT。

标识符：NO_UNRESTRICTED_ROUTE_TO_IGW

资源类型： AWS::EC2::RouteTable

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

routeTableIds （可选），类型：CSV

逗号分隔的路由表 ID 列表，这些路由表可以路由到目标 CIDR 块为“0.0.0.0/0”或“::/0”的互联网网关。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch-access-control-enabled

检查 Amazon S OpenSearch ervice 域名是否启用了精细访问控制。如果未为 OpenSearch 服务域启用该规则 AdvancedSecurityOptions ，则该规则不合规。

标识符：OPENSEARCH_ACCESS_CONTROL_ENABLED

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch-audit-logging-enabled

检查 Amazon S OpenSearch ervice 域是否启用了审核日志。如果 OpenSearch 服务域未启用审核日志，则该规则为 “不合规”。

标识符：OPENSEARCH_AUDIT_LOGGING_ENABLED

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

云WatchLogsLogGroupArnList （可选），类型：CSV

> 以逗号分隔的 Amazon CloudWatch 日志组的亚马逊资源名称 (ARN) 列表。该规则检查是否为审核日志配置了指定的日志组。
>
> 有效值包括：`arn:aws:logs:region:account-id:log-group:log_group_name:*` 和 `arn:aws:logs:region:account-id:log-group:log_group_name`。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch-data-node-fault-tolerance

检查 Amazon S OpenSearch ervice 域是否配置了至少三个数据节点，且 zoneAwarenessEnabled 该值为真。如果 “InstanceCount” 小于 3 或 “区域” 设置为 “false”，则该 OpenSearch 域的规则不合规。AwarenessEnabled

标识符：OPENSEARCH_DATA_NODE_FAULT_TOLERANCE

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch-encrypted-at-rest

检查 Amazon S OpenSearch ervice 域名是否启用了静态加密配置。如果 `EncryptionAtRestOptions` 字段未启用，则规则为 NON_COMPLIANT。

> **Note**
>
> 此规则不评估 Elasticsearch 域。

标识符：OPENSEARCH_ENCRYPTED_AT_REST

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch-https-required

检查与 OpenSearch 域的连接是否使用 HTTPS。如果亚马逊 OpenSearch 域名 “enforceHttps” 不是 “真” 或 “真”，而 “TLS” 不在 “SecurityPolicy” 中，则该规则不合规。`tlsPolicies`

标识符：OPENSEARCH_HTTPS_REQUIRED

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

tlsPolicies（可选），类型：CSV

以逗号分隔的 TLS 安全策略列表，用于对照 Ama OpensSearch zon 域进行检查。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch-in-vpc-only

检查亚马逊 OpenSearch 服务域名是否在亚马逊虚拟私有云 (VPC) 中。如果 OpenSearch 服务域终端节点是公共的，则该规则不合规。

> **Note**
>
> 此规则不评估 Elasticsearch 域。

标识符：OPENSEARCH_IN_VPC_ONLY

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch-logs-to-cloudwatch

检查亚马逊 OpenSearch 服务域是否配置为向亚马逊日志发送 CloudWatch 日志。如果未配置日志记录，则此规则为 NON_COMPLIANT。

> **Note**
> 此规则不评估 Elasticsearch 域。

标识符：OPENSEARCH_LOGS_TO_CLOUDWATCH

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

logTypes（可选），类型：CSV

已启用的日志的逗号分隔列表。有效值为“search”、“index”、“error”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch-node-to-node-encryption-check

检查亚马逊 OpenSearch 服务节点是否端到端加密。如果未在域上启用 node-to-node 加密，则该规则不兼容

> **Note**
> 此规则不评估 Elasticsearch 域。

标识符：OPENSEARCH_NODE_TO_NODE_ENCRYPTION_CHECK

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch 主节点容错能力

检查 Amazon S OpenSearch ervice 域是否配置了至少三个专用主节点。如果 “已DedicatedMaster启用” 设置为 “假” 或 “DedicatedMaster计数” 小于 3，则该 OpenSearch 服务域的规则不合规。

标识符：OPENSEARCH_PRIMARY_N ODE_PRAM

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

opensearch-update-check

检查 Amazon OpenSearch 服务版本更新是否可用但尚未安装。如果未安装最新的软件更新，则该 OpenSearch 域的规则不兼容。

标识符：OPENSEARCH_UPDATE_CHECK

资源类型： AWS::OpenSearch::Domain

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-aurora-mysql-audit-logging-enabled

检查兼容 Amazon Aurora MySQL 的版本集群是否配置为向亚马逊日志发布审核日志。 CloudWatch 如果 Aurora MySQL 兼容版集群未配置审核日志发布功能，则此规则为 NON_COMPLIANT。

标识符：RDS_AURORA_MYSQL_AUDIT_LOGGING_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-automatic-minor-version-upgrade-enabled

检查 Amazon Relational Database Service (Amazon RDS) 数据库实例是否配置为自动升级次要版本。如果 “自动MinorVersion升级” 的值为假，则该规则不合规。

标识符：RDS_AUTOMATIC_MINOR_VERSION_UPGRADE_ENABLED

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
    "AutoMinorVersionUpgrade": BOOLEAN*,
    "Engine": String*
}
...
```

* 有关这些输入有效值的更多信息，请参阅 AWS CloudFormation 用户指南中的 AutoMinorVersionUpgrade 和引擎。

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-cluster-auto-minor-version-upgrade-enable

检查是否为 Amazon RDS 多可用区集群部署启用了自动次要版本升级。如果将 “ autoMinorVersion升级” 设置为 false，则该规则不兼容。

标识符：RDS_CLUSTER_AUTO_MINOR_VERSION_UPGRADE_ENABLE

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-cluster-default-admin-check

检查 Amazon Relational Database Service (Amazon RDS) 数据库集群是否已将管理员用户名从其默认值更改为其他值。如果管理员用户名设置为默认值，则此规则为 NON_COMPLIANT。

标识符：RDS_CLUSTER_DEFAULT_ADMIN_CHECK

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

有效AdminUserNames （ 可选 ）, 类型：CSV

Amazon RDS 集群可以使用的管理员用户名的逗号分隔列表。不能将“postgres”或“admin”作为有效用户名，因为这些都是默认值。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-cluster-deletion-protection-enabled

检查 Amazon Relational Database Service (Amazon RDS) 集群是否启用了删除保护。如果 Amazon RDS 集群未启用删除保护，则此规则为 NON_COMPLIANT。

标识符：RDS_CLUSTER_DELETION_PROTECTION_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-cluster-encrypted-at-rest

检查 Amazon Relational Database Service (Amazon RDS) 集群是否进行了静态加密。如果 Amazon RDS 集群未进行静态加密，则此规则为 NON_COMPLIANT。

标识符：RDS_CLUSTER_ENCRYPTED_AT_REST

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-cluster-iam-authentication-enabled

检查亚马逊关系数据库服务 (Amazon RDS) 集群是否启用了 AWS 身份和访问管理 (IAM) Access Management 身份验证。如果 Amazon RDS 集群未启用 IAM 身份验证，则此规则为 NON_COMPLIANT。

标识符：RDS_CLUSTER_IAM_AUTHENTICATION_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-cluster-multi-az-enabled

检查是否在 Amazon Relational Database Service (Amazon RDS) 管理的 Amazon Aurora 和 Hermes 集群上启用了多可用区复制。如果 Amazon RDS 实例未配置多可用区，则此规则为 NON_COMPLIANT。

标识符：RDS_CLUSTER_MULTI_AZ_ENABLED

资源类型：AWS::RDS::DBCluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-db-security-group-not-allowed

检查是否存在非默认数据库安全组的任何 Amazon Relational Database Service (Amazon RDS) 数据库安全组。如果存在任何非默认数据库安全组的数据库安全组，则此规则为 NON_COMPLIANT。

标识符：RDS_DB_SECURITY_GROUP_NOT_ALLOWED

资源类型：AWS:: RDS:: DB SecurityGroup

触发器类型： 配置更改

AWS 区域：仅在以下区域提供：欧洲地区（爱尔兰）、南美洲（圣保罗）、美国东部（弗吉尼亚州北部）、亚太地区（东京）、美国西部（俄勒冈州）、美国西部（北加利福尼亚）、亚太地区（新加坡）、亚太地区（悉尼）

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-enhanced-monitoring-enabled

检查是否为 Amazon RDS 实例启用了增强监控。如果 RDS 实例的配置项中的“`monitoringInterval`”为“0”，或者“`monitoringInterval`”与规则参数值不匹配，则此规则为 NON_COMPLIANT。

标识符：RDS_ENHANCED_MONITORING_ENABLED

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

monitoringInterval（可选），类型：int

一个整数值，表示为数据库实例收集增强监控指标时，点之间的秒数。有效值为 1、5、10、15、30 和 60。

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
    "MonitoringInterval": Integer*,
    "Engine": String*
}
...
```

* 有关这些输入有效值的更多信息，请参阅 AWS CloudFormation 用户指南中的MonitoringInterval和引擎。

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-instance-default-admin-check

检查 Amazon Relational Database Service (Amazon RDS) 数据库是否已将管理员用户名从其默认值更改为其他值。此规则仅在 RDS 数据库实例上运行。如果管理员用户名设置为默认值，则此规则为 NON_COMPLIANT。

标识符：RDS_INSTANCE_DEFAULT_ADMIN_CHECK

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

有效AdminUserNames （ 可选 ）, 类型：CSV

Amazon RDS 实例可以使用的管理员用户名的逗号分隔列表。（ 不能将“postgres”或“admin”作为有效用户名，因为这些都是默认值。 ）

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-instance-deletion-protection-enabled

检查 Amazon Relational Database Service (Amazon RDS) 实例是否启用了删除保护。如果 Amazon RDS 实例未启用删除保护，例如，deletionProtection 设置为 false，则此规则为 NON_COMPLIANT。

> **Warning**
>
> 集群 (Aurora/DocumentDB) 中的某些 RDS 数据库实例将显示为不合规。

标识符：RDS_INSTANCE_DELETION_PROTECTION_ENABLED

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

databaseEngines（ 可选 ）, 类型：CSV

要包含在规则评估中的 RDS 数据库引擎的逗号分隔列表。例如，“mysql, postgres, mariadb”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-instance-iam-authentication-enabled

检查亚马逊关系数据库服务 (Amazon RDS) 实例是否启用了 AWS 身份和访问管理 (IAM) Access Management 身份验证。如果 Amazon RDS 实例未启用 IAM 身份验证，则此规则为 NON_COMPLIANT。

> **Note**
>
> 数据库引擎应该是“mysql”、“postgres”、“aurora”、“aurora-mysql”或“aurora-postgresql”之一。数据库实例的状态应为“available”、“backing-up”、“storage-optimization”或“storage-full”。

标识符：RDS_INSTANCE_IAM_AUTHENTICATION_ENABLED

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-instance-public-access-check

检查 Amazon Relational Database Service (Amazon RDS) 实例是否不可公开访问。如果实例配置项中的 publiclyAccessible 字段为 true，则此规则为 NON_COMPLIANT。

标识符：RDS_INSTANCE_PUBLIC_ACCESS_CHECK

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-in-backup-plan

检查 AWS 备份计划中是否存在亚马逊关系数据库服务（Amazon RDS）数据库。如果任何 AWS 备份计划中均未包含 Amazon RDS 数据库，则该规则不合规。

> **Note**
>
> 此规则仅适用于 Amazon Aurora 数据库实例。不支持数据库集群。

标识符：RDS_IN_BACKUP_PLAN

资源类型：AWS::RDS::DBInstance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-last-backup-recovery-point-created

检查是否为 Amazon Relational Database Service (Amazon RDS) 创建了恢复点。如果 Amazon RDS 实例没有在指定时间段内创建相应的恢复点，则此规则为 NON_COMPLIANT。

标识符：RDS_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型：AWS::RDS::DBInstance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Amazon RDS 实例的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon RDS 实例的 ID。

恢复PointAgeValue （可选）, 类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit （可选）, 类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-logging-enabled

检查是否启用了 Amazon Relational Database Service (Amazon RDS) 的相应日志。如果未启用任何日志记录，则此规则为 NON_COMPLIANT。

> **Note**
>
> 不处于“available”、“backing-up”、“storage-optimization”或“storage-full”状态的数据库实例评估为 `NOT_APPLICABLE`。

标识符：RDS_LOGGING_ENABLED

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

additionalLogs（可选），类型: StringMap

引擎名称和日志类型名称的逗号分隔列表。例如，"additionalLogs": "oracle: general, slowquery ; aurora: alert, slowquery"

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-meets-restore-time-target

检查 Amazon Relational Database Service (Amazon RDS) 实例的还原时间是否符合指定的持续时间。如果 Amazon RDS 实例 LatestRestoreExecutionTimeMinutes 的大于 maxRestoreTime 分钟，则该规则不合规。

标识符：RDS_MEETS_RESTORE_TIME_TARGET

资源类型：AWS::RDS::DBInstance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大 RestoreTime, 类型：int

允许的最大还原运行时间的数值。

resourceTags（可选）, 类型：字符串

规则要检查的 Amazon RDS 实例的标签，采用 JSON 格式。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon RDS 实例的 ID。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-multi-az-support

检查您的 RDS 数据库实例是否启用了高可用性。

在多可用区部署中，Amazon RDS 会自动在不同可用区中配置和维护一个同步备用副本。有关更多信息，请参阅《Amazon RDS 用户指南》中的高可用性（多可用区）。

> **Note**
>
> 此规则不评估 Amazon Aurora 数据库、Amazon DocumentDB 和 Amazon Neptune 数据库实例。

标识符：RDS_MULTI_AZ_SUPPORT

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
    "MultiAZ": BOOLEAN*,
    "Engine": String*
}
...
```

* 有关这些输入有效值的更多信息，请参阅 AWS CloudFormation 用户指南中的多可用区和引擎。

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-resources-protected-by-backup-plan

检查 Amazon Relational Database Service (Amazon RDS) 实例是否受备份计划的保护。如果备份计划不涵盖 Amazon RDS 数据库实例，则此规则为 NON_COMPLIANT。

标识符：RDS_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型：AWS::RDS::DBInstance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选），类型：字符串

此规则要检查的 Amazon RDS 实例的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选），类型：字符串

此规则要检查的 Amazon RDS 实例的 ID。

crossRegionList （可选），类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （可选），类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （可选），类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （可选），类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选），类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-snapshots-public-prohibited

检查 Amazon Relational Database Service (Amazon RDS) 快照是否是公有的。如果任何现有和新的 Amazon RDS 快照是公有的，则此规则为 NON_COMPLIANT。

> **Note**
>
> 系统最长可能需要 12 小时才会生成合规性结果。

标识符：RDS_SNAPSHOTS_PUBLIC_PROHIBITED

资源类型：AWS:: RDS:: dbSnapshot、AWS:: RDS:: DB ClusterSnapshot

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-snapshot-encrypted

检查 Amazon Relational Database Service (Amazon RDS) 数据库快照是否进行了加密。如果 Amazon RDS 数据库快照未加密，则此规则为 NON_COMPLIANT。

Identifier (标识符)：RDS_SNAPSHOT_ENCRYPTED

资源类型：AWS:: RDS:: dbSnapshot、AWS:: RDS:: DB ClusterSnapshot

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

rds-storage-encrypted

检查您的 Amazon Relational Database Service (Amazon RDS) 数据库实例是否启用了存储加密。如果未启用存储加密，则此规则为 NON_COMPLIANT。

标识符：RDS_STORAGE_ENCRYPTED

资源类型：AWS::RDS::DBInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyId （可选），类型：字符串

用于加密存储的 KMS 密钥 ID 或 Amazon 资源名称 (ARN)。

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "StorageEncrypted": BOOLEAN
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-audit-logging-enabled

检查 Amazon Redshift 集群是否正在将审核日志记录到特定的存储桶。如果没有为 Redshift 集群启用审核日志记录，或者虽然提供了“`bucketNames`”参数，但审核日志记录目标不匹配，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_AUDIT_LOGGING_ENABLED

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

bucketNames（可选），类型：CSV

用于存储审核日志的 Amazon S3 存储桶名称的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-backup-enabled

检查集群是否启用了 Amazon Redshift 自动快照。如果 `automatedSnapshotRetentionPeriod` 的值大于 `MaxRetentionPeriod` 或小于 `MinRetentionPeriod`，或者值为 0，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_BACKUP_ENABLED

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

MinRetentionPeriod （可选），类型：int

保留期的最小值。最小值为 1。

MaxRetentionPeriod （可选），类型：int

保留期的最大值。最大值为 35。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-cluster-configuration-check

检查 Amazon Redshift 集群是否具有指定的设置。如果 Amazon Redshift 集群未加密，或者是使用其他密钥加密的，或者集群未启用审核日志记录，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_CLUSTER_CONFIGURATION_CHECK

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

集群 DbEncrypted, 类型：布尔值, 默认：True

数据库加密已启用。

loggingEnabled, 类型：布尔值, 默认：True

审核日志记录已启用。

nodeTypes（可选）, 类型：CSV, 默认值：dc1.large

指定节点类型。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-cluster-kms-enabled

检查 Amazon Redshift 集群是否使用指定的 AWS Key Management Service (AWS KMS) 密钥进行加密。如果启用了加密并且集群是使用 `kmsKeyArn` 参数中提供的密钥进行加密的，则此规则为 COMPLIANT。如果集群未加密，或者是使用其他密钥加密的，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_CLUSTER_KMS_ENABLED

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyArns （可选）, 类型：CSV

以逗号分隔的 AWS KMS Amazon Redshift 集群中用于加密的关键亚马逊资源名称 (ARN) 列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-cluster-maintenancesettings-check

检查 Amazon Redshift 集群是否具有指定的维护设置。如果禁用自动升级到主要版本，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_CLUSTER_MAINTENANCESETTINGS_CHECK

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

允许 VersionUpgrade, 类型：布尔值, 默认：True

允许版本升级已启用。

preferredMaintenanceWindow （可选）, 类型：字符串

为集群计划的维护时段 (例如，周一 09:30 - 周一 10:00)。

自动SnapshotRetentionPeriod （可选）, 类型：int, 默认值：1

自动快照要被保留的天数。

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
    "AutomatedSnapshotRetentionPeriod": Integer*,
    "PreferredMaintenanceWindow": String*,
    "AllowVersionUpgrade": BOOLEAN*
}
```

```
...
```

* 有关这些输入有效值的更多信息 AutomatedSnapshotRetentionPeriod，请参阅《 AWS CloudFormation 用户指南》中的 PreferredMaintenance“窗口” 和 “AllowVersion升级”。

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-cluster-public-access-check

检查 Amazon Redshift 集群是否不可公开访问。如果集群配置项中的 publiclyAccessible 字段为 true，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "PubliclyAccessible": BOOLEAN
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-default-admin-check

检查 Amazon Redshift 集群是否已将管理员用户名从其默认值更改为其他值。如果 Redshift 集群的管理员用户名设置为“awsuser”，或者用户名与参数中列出的用户名不匹配，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_DEFAULT_ADMIN_CHECK

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

有效AdminUserNames （可选），类型：CSV

Redshift 集群要使用的管理员用户名的逗号分隔列表。注意：“awsuser”是默认值，不被接受。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-default-db-name-check

检查 Redshift 集群是否已将其数据库名称从默认值更改为其他名称。如果 Redshift 集群的数据库名称设置为“dev”，或者提供了可选参数但数据库名称不匹配，则此规则为 NON_COMPLIANT。

标识符：REDSHIFT_DEFAULT_DB_NAME_CHECK

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

validDatabaseNames （可选），类型：CSV

Redshift 集群的数据库名称的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-enhanced-vpc-routing-enabled

检查 Amazon Redshift 集群是否启用了 “增强版” VpcRouting。如果未启用 “增强VpcRouting” 或配置不合规。 enhancedVpcRouting 字段为 “假”。

标识符：REDSHIFT_ENHANCED_VPC_ROUTING_ENABLED

资源类型： AWS::Redshift::Cluster

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-require-tls-ssl

检查 Amazon Redshift 集群是否需要 TLS/SSL 加密才能连接到 SQL 客户端。如果任何 Amazon Redshift 集群的参数 require_SSL 未设置为 true，则此规则为 NON_COMPLIANT。

Identifier (标识符)：REDSHIFT_REQUIRE_TLS_SSL

资源类型： AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter组

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

redshift-不受限制的端口访问权限

检查与 Amazon Redshift 集群关联的安全组是否有允许不受限制的传入流量的入站规则。如果存在允许不受限制的传入流量流向 Redshift 集群端口的入站规则，则该规则不兼容。

标识符：REDSHIFT_UNRESTRIC TED_PORT_

资源类型： AWS::Redshift::Cluster

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

required-tags

检查您的资源是否具有您指定的标签。例如，可以检查您的 Amazon EC2 实例是否具有 `CostCenter` 标签，同时还可以检查您的所有 RDS 实例是否都有一组 Keys 标签。用英文逗号分隔多个值。一次最多可以查看 6 个标签。

AWS管理的 AWS Systems Manager 自动化文档`AWS-SetRequiredTags`不能作为此规则的补救措施。您需要创建自己的自定义 Systems Manager 自动化文档以进行补救。

上下文： AWS 允许您以标签的形式为 AWS 资源分配元数据。每个标签都由一个键和一个可选值组成，用于存储有关资源的信息或保留在该资源上的数据。有关更多信息，请参阅制定标记策略。

您可以使用此规则来查找账户中未使用所需配置启动的资源，方法是指定哪些资源应具有标签以及每个标签的预期值。您也可以运行修复操作来修复标记错误。但是，此规则并不能防止您创建带有错误标签的资源。

标识符：REQUIRED_TAGS

资源类型: AWS::ACM::Certificate, AWS::AutoScaling:: AutoScaling 组, AWS::CloudFormation::Stack, AWS::CodeBuild:: 项目,, AWS::DynamoDB::Table, AWS::EC2::CustomerGateway, AWS::EC2::Instance, AWS::EC2::InternetGateway, AWS::EC2::NetworkAcl,, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable AWS::EC2::SecurityGroup, AWS::EC2::Subnet, AWS::EC2::Volume, AWS::EC2::VPC, AWS::EC2::VPNConnection, AWS::EC2::VPNGateway, AWS::ElasticLoad 平衡::LoadBalancer, AWS::ElasticLoadBalancingV2::LoadBalancer, AWS::RDS::DBInstance, AWS::RDS::DBSecurityGroup, AWS::RDS::DBSnapshot, AWS::RDS::DBSubnetGroup, AWS::RDS::EventSubscription, AWS::Redshift::Cluster, AWS::Redshift::ClusterParameter 组, AWS::Redshift::ClusterSecurity 组, AWS::Redshift::ClusterSnapshot, AWS::Redshift::ClusterSubnet 组, AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

tag1Key, 类型：字符串, 默认： CostCenter

所需标签的键。

tag1Value（可选）, 类型：CSV

所需标签的可选值。用英文逗号分隔多个值。

tag2Key（可选）, 类型：字符串

第二个必需标签的键。

tag2Value（可选）, 类型：CSV

第二个所需标签的可选值。用英文逗号分隔多个值。

tag3Key（可选）, 类型：字符串

第三个所需标签的键。

tag3Value（可选），类型：CSV

第三个所需标签的可选值。用英文逗号分隔多个值。

tag4Key（可选），类型：字符串

第四个所需标签的键。

tag4Value（可选），类型：CSV

第四个所需标签的可选值。用英文逗号分隔多个值。

tag5Key（可选），类型：字符串

第五个所需标签的键。

tag5Value（可选），类型：CSV

第五个所需标签的可选值。用英文逗号分隔多个值。

tag6Key（可选），类型：字符串

第六个所需标签的键。

tag6Value（可选），类型：CSV

第六个所需标签的可选值。用英文逗号分隔多个值。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

restricted-common-ports

> **Important**
>
> 对于此规则，规则标识符 (RESTRICTED_INCOMING_TRAFFIC) 和规则名称 (restricted-common-ports) 是不同的。

检查所用安全组是否不允许不受限制的传入传输控制协议 (TCP) 流量进入指定端口。在以下情况下，此规则为 COMPLIANT：

- 禁止所有 TCP 流量访问端口。

- 端口访问通过入站规则 向 TCP 流量开放，源地址可以是单个 IPv4 地址，也可以是用 CIDR 表示的 IPv4 地址范围，但不包括所有 IPv4 地址（“0.0.0.0/0”）。
- 端口访问通过入站规则 向 TCP 流量开放，源地址可以是单个 IPv6 地址，也可以是用 CIDR 表示的 IPv6 地址范围，但不包括所有 IPv6 地址（“::/0)”）。

如果入站 TCP 连接的 IP 地址不限于指定端口，则此规则为 NON_COMPLIANT。

标识符：RESTRICTED_INCOMING_TRAFFIC

资源类型： AWS::EC2::SecurityGroup

触发器类型：配置更改和定期

AWS 区域: 所有支持的 AWS 区域

参数：

blockedPort1（可选）, 类型：int, 默认值：20

已阻止的 TCP 端口号。默认值 20 对应于文件传输协议 (FTP) 数据传输。

blockedPort2（可选）, 类型：int, 默认值：21

已阻止的 TCP 端口号。默认值 21 对应于文件传输协议 (FTP) 命令控制。

blockedPort3（可选）, 类型：int, 默认值：3389

已阻止的 TCP 端口号。默认值 3389 对应于远程桌面协议 (RDP)。

blockedPort4（可选）, 类型：int, 默认值：3306

已阻止的 TCP 端口号。默认值 3306 对应于 MySQL 协议。

blockedPort5（可选）, 类型：int, 默认值：4333

已阻止的 TCP 端口号。默认值 4333 对应于 MySQL 协议。

blockedPorts（可选）, 类型：CSV

被阻止的 TCP 端口号的逗号分隔列表。例如，20, 21, 3306, 3389 和 4333。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

root-account-hardware-mfa-enabled

检查您的 AWS 账户是否允许使用多重身份验证 (MFA) 硬件设备使用根凭证登录。如果允许任何虚拟 MFA 设备通过根凭证登录，则此规则为 NON_COMPLIANT。

> **Note**
>
> 托管规则和全球 IAM 资源类型
> 2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。
> 如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。
> 为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

标识符：ROOT_ACCOUNT_HARDWARE_MFA_ENABLED

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

root-account-mfa-enabled

检查您 AWS 账户的 root 用户是否需要多重身份验证才能登录控制台。如果 AWS 身份和访问管理 (IAM) Access Management 根账户用户未启用多重身份验证 (MFA)，则该规则不合规。

> **Note**
>
> 托管规则和全球 IAM 资源类型
>
> 2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。
>
> 如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。
>
> 为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

标识符：ROOT_ACCOUNT_MFA_ENABLED

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

route53-query-logging-enabled

检查您的 Amazon Route 53 公有托管区是否启用 DNS 查询日志记录。如果您的 Amazon Route 53 公有托管区域未启用 DNS 查询日志记录，则此规则为 NON_COMPLIANT。

标识符：ROUTE53_QUERY_LOGGING_ENABLED

资源类型： AWS::Route53::HostedZone

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-access-point-in-vpc-only

检查 Amazon S3 接入点是否不允许从互联网进行访问（NetworkOrigin 是 VPC）。如果 NetworkOrigin 是互联网，则该规则不兼容。

标识符：S3_ACCESS_POINT_IN_VPC_ONLY

资源类型： AWS::S3::AccessPoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-access-point-public-access-blocks

检查 Amazon S3 接入点是否启用了阻止公共访问设置。如果未为 S3 接入点启用阻止公共访问设置，则此规则为 NON_COMPLIANT。

标识符：S3_ACCESS_POINT_PUBLIC_ACCESS_BLOCKS

资源类型： AWS::S3::AccessPoint

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

excludedAccessPoints （可选），类型：CSV

允许的公共 Amazon S3 接入点列表（以逗号分隔）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-account-level-public-access-blocks

检查是否从账户级别配置了所需的公有访问阻止设置。仅当下面设置的字段与配置项中的相应字段不匹配时，该规则才为 NON_COMPLIANT。

> **Note**
>
> 如果您正在使用此规则，请确保已启用 S3“阻止公有访问”。此规则是更改触发型规则，因此除非启用 S3“阻止公有访问”，否则不会调用此规则。如果未启用 S3“阻止公有访问”，则此规则将返回 INSUFFICIENT_DATA。这意味着您可能仍有一些公有存储桶。有关设置 S3“阻止公有访问”的更多信息，请参阅阻止对 Amazon S3 存储的公有访问。

标识符：S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS

资源类型： AWS::S3::AccountPublicAccessBlock

触发器类型：配置更改（当前为未选中状态，仅在更改生成新事件时才会进行评估）

> **Note**
>
> 只有 S3 终端节点所在的特定区域的配置更改才会触发此规则。在所有其他区域，都会定期检查此规则。如果在其他区域进行了更改，在规则返回 NON_COMPLIANT 之前可能会有一段延迟。

AWS 区域: 所有支持的 AWS 区域

参数：

IgnorePublicAcls （可选）, 类型：字符串, 默认值：True

IgnorePublicAcls 是否强制执行，默认为 True

BlockPublicPolicy （可选）, 类型：字符串, 默认值：True

BlockPublicPolicy 是否强制执行，默认为 True

BlockPublicAcls （可选）, 类型：字符串, 默认值：True

BlockPublicAcls 是否强制执行，默认为 True

RestrictPublicBuckets （可选）, 类型：字符串, 默认值：True

RestrictPublicBuckets 是否强制执行，默认为 True

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-account-level-public-access-blocks-periodic

检查是否已在账户级别配置了所需的公有访问阻止设置。如果配置项与参数中的一个或多个设置（或默认设置）不匹配，则此规则为 NON_COMPLIANT。

标识符：S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

IgnorePublicAcls （可选）, 类型：字符串

IgnorePublicAcls 是否强制执行，默认为 True

BlockPublicPolicy （可选），类型：字符串

BlockPublicPolicy 是否强制执行，默认为 True

BlockPublicAcls （可选），类型：字符串

BlockPublicAcls 是否强制执行，默认为 True

RestrictPublicBuckets （可选），类型：字符串

RestrictPublicBuckets 是否强制执行，默认为 True

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-acl-prohibited

检查 Amazon Simple Storage Service (Amazon S3) 存储桶是否通过访问控制列表 (ACL) 允许用户访问。如果在 Amazon S3 存储桶中为用户访问配置了 ACL，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_ACL_PROHIBITED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-blacklisted-actions-prohibited

检查 Amazon Simple Storage Service (Amazon S3) 存储桶策略是否不允许其他账户的委托人对存储桶中的资源进行列入黑名单的存储桶级和对象级操作。 AWS 例如，该规则会检查 Amazon

S3 存储桶策略是否不允许其他 AWS 账户`s3:DeleteObject`对存储桶中的任何对象执行任何`s3:GetBucket*`操作。如果 Amazon S3 存储桶策略允许任何列入黑名单的操作，则此规则为 NON_COMPLIANT。

> **Note**
> 此规则只会检查 Principal 属性中的实体，不考虑策略中 Condition 属性下的任何条件

标识符：S3_BUCKET_BLACKLISTED_ACTIONS_PROHIBITED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

列入黑名单 ActionPattern, 类型：CSV

以逗号分隔的黑名单操作模式列表，例如 s3: GetBucket * 和 s3:。DeleteObject

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

已启用 s3 存储桶跨区域复制

检查您是否已为 Amazon S3 存储桶启用了 S3 跨区域复制。如果没有为跨区域复制启用复制规则，则该规则不兼容。

标识符：S3_BUCKET_CROSS_REGION_RE PLICATION_ENABLE

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-default-lock-enabled

检查默认情况下 S3 存储桶是否启用了锁定。如果锁定未启用，则规则为 NON_COMPLIANT。

Identifier (标识符)：S3_BUCKET_DEFAULT_LOCK_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

mode（可选），类型：字符串

mode（可选）：具有 GOVERNANCE 或 COMPLIANCE 有效值的模式参数。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-level-public-access-prohibited

检查 S3 存储桶是否可公开访问。如果 `excludedPublicBuckets` 参数中未列出 S3 存储桶且存储桶级别设置为公开，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_LEVEL_PUBLIC_ACCESS_PROHIBITED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

excludedPublicBuckets （可选），类型：CSV

已知允许的公有 Amazon S3 存储桶名称的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-logging-enabled

检查您的 S3 存储桶是否已启用日志记录。如果未启用日志记录，则该规则为 NON_COMPLIANT。

标识符：S3_BUCKET_LOGGING_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

targetBucket（可选），类型：字符串

用于存储服务器访问日志的目标 S3 存储桶。

targetPrefix（可选），类型：字符串

用于存储服务器访问日志的 S3 存储桶的前缀。

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
```

```
    "BucketName": "my-bucket",
    "LoggingConfiguration": {
          "DestinationBucketName": "my-log-bucket",
          "LogFilePrefix":"my-log"
    }
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-mfa-delete-enabled

检查 Amazon Simple Storage Service (Amazon S3) 存储桶版本控制配置中是否启用了 MFA 删除。如果 MFA 删除未启用，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_MFA_DELETE_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-policy-grantee-check

检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或 VPC 的限制。如果存储桶策略不存在，则此规则为 COMPLIANT。

例如，如果规则的输入参数为包含 111122223333 和 444455556666 这两个委托人的列表，并且存储桶策略指定仅 111122223333 能够访问存储桶，则此规则为 COMPLIANT。使用相同的输入参数：如果存储桶策略指定 111122223333 和 444455556666 可以访问存储桶，则它也是合规的。但是，如果存储桶策略指定 999900009999 可以访问存储桶，则规则将为 NON-COMPLIANT。

> **Note**
>
> 如果存储桶策略包含多个语句，则将根据此规则评估存储桶策略中的每条语句。

标识符：S3_BUCKET_POLICY_GRANTEE_CHECK

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

awsPrincipals（可选），类型：CSV

以逗号分隔的委托人列表，例如 IAM 用户 ARN、IAM 角色 ARN 和 AWS 账户，例如 'arn: aws: iam:: 111122223333: user/Alice，arn: aws: iam:: 4444555566666: role/bob，123456789012'。

servicePrincipals（可选），类型：CSV

逗号分隔的服务委托人列表，例如“cloudtrail.amazonaws.com, lambda.amazonaws.com”。

federatedUsers（可选），类型：CSV

Web 身份联合验证的身份提供商（如 Amazon Cognito 和 SAML 身份提供商）的逗号分隔列表。例如“cognito-identity.amazonaws.com, arn:aws:iam::111122223333:saml-provider/my-provider”。

ipAddresses（可选），类型：CSV

CIDR 格式的 IP 地址的逗号分隔列表，例如“10.0.0.1, 192.168.1.0/24, 2001:db8::/32”。

vpcIds（可选），类型：CSV

Amazon Virtual Private Cloud (Amazon VPC) ID 的逗号分隔列表，例如“vpc-1234abc0, vpc-ab1234c0”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-policy-not-more-permissive

验证您的 Amazon Simple Storage Service 存储桶策略是否不允许您提供的控制 Amazon S3 存储桶策略之外的其他账户间权限。

> **Note**
>
> 如果您提供了无效的参数值，则将看到以下错误：controlPolicy 参数的值必须是 Amazon S3 存储桶策略。

标识符：S3_BUCKET_POLICY_NOT_MORE_PERMISSIVE

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

controlPolicy, 类型：字符串

定义您的 S3 存储桶的权限上限的 Amazon S3 存储桶策略。此策略的最大长度为 1024 个字符。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-public-read-prohibited

检查您的 Amazon S3 存储桶是否不允许公有读取访问。该规则将检查“阻止公有访问”设置、存储桶策略和存储桶访问控制列表 (ACL)。

当满足以下两个条件时，该规则也合规：

- “阻止公有访问”设置限制公有策略，或者存储桶策略不允许公有读取访问。
- “阻止公有访问”设置限制公有 ACL，或者存储桶 ACL 不允许公有读取访问。

在以下情况下，该规则不合规：

- 如果 “阻止公共访问” 设置不限制公共策略，则 AWS Config 评估该策略是否允许公共读取权限。如果策略允许公有读取访问，则该规则不合规。
- 如果 “阻止公共访问” 设置不限制公共存储桶 ACL，则 AWS Config 评估存储桶 ACL 是否允许公共读取权限。如果存储桶 ACL 允许公有读取访问，则规则将不合规。

标识符：S3_BUCKET_PUBLIC_READ_PROHIBITED

资源类型： AWS::S3::Bucket

触发器类型：配置更改和定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-public-write-prohibited

检查您的 Amazon S3 存储桶是否允许公有写入访问。该规则将检查“阻止公有访问”设置、存储桶策略和存储桶访问控制列表 (ACL)。

当满足以下两个条件时，该规则也合规：

- “阻止公有访问”设置限制公有策略，或者存储桶策略不允许公有写入访问。
- “阻止公有访问”设置限制公有 ACL，或者存储桶 ACL 不允许公有写入访问。

在以下情况下，该规则不合规：

- 如果 “阻止公共访问” 设置不限制公共策略，则 AWS Config 评估该策略是否允许公共写入权限。如果策略允许公有写入访问，则该规则不合规。
- 如果 “阻止公共访问” 设置不限制公共存储桶 ACL，则 AWS Config 评估存储桶 ACL 是否允许公共写入权限。如果存储桶 ACL 允许公有写入访问，则规则将不合规。

> **Note**
>
> 此规则不评估账户级别阻止公有访问权限的更改。要检查所需的公有访问阻止设置是否是从账户级别配置的，请参阅 s3-account-level-public-access-blocks 和 s3-account-level-public-access-blocks-periodic。

标识符：S3_BUCKET_PUBLIC_WRITE_PROHIBITED

资源类型： AWS::S3::Bucket

触发器类型：配置更改和定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-replication-enabled

检查 S3 存储桶是否启用了复制规则。如果 S3 存储桶没有复制规则或复制规则未启用，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_REPLICATION_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

ReplicationType （可选），类型：字符串

接受的值：“CROSS-REGION”和“SAME-REGION”。对规则输入“CROSS-REGION”，以检查所有存储桶是否仅启用了跨区域复制。对规则输入“SAME-REGION”，以检查所有存储桶是否仅启用了同区域复制。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-server-side-encryption-enabled

检查您的 Amazon S3 存储桶是否已启用 Amazon S3 默认加密，或 Amazon S3 存储桶策略是否显式拒绝未进行服务器端加密（使用 AES-256 或 AWS Key Management Service）的 `put-object` 请求。如果您的 Amazon S3 存储桶默认未加密，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_SERVER_SIDE_ENCRYPTION_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-ssl-requests-only

检查 S3 存储桶是否具有需要请求使用 SSL/TLS 的策略。如果任何 S3 存储桶具有允许 HTTP 请求的策略，则此规则为 NON_COMPLIANT。

标识符：S3_BUCKET_SSL_REQUESTS_ONLY

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-bucket-versioning-enabled

检查您的 S3 存储桶是否已启用版本控制。(可选) 该规则检查是否为您的 S3 存储桶启用了 MFA 删除。

标识符：S3_BUCKET_VERSIONING_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

是MfaDeleteEnabled （ 可选 ）, 类型：字符串

已经为您的 S3 存储桶启用了 MFA 删除。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-default-encryption-kms

检查 S3 存储桶是否使用 AWS 密钥管理服务 (AWS KMS) 加密。如果 S3 存储桶未使用 AWS KMS 密钥加密，则该规则不合规。

Identifier (标识符)：S3_DEFAULT_ENCRYPTION_KMS

资源类型： AWS::S3::Bucket， AWS::KMS::Key

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyArns （可选）, 类型：CSV

允许加密 Amazon S3 存储桶的 AWS KMS 密钥 ARN 列表，以逗号分隔。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-event-notifications-enabled

检查 S3 存储桶上是否启用了 Amazon S3 事件通知。如果存储桶上未设置 S3 事件通知，或者事件类型或目标与 `eventTypes` 和 destinationArn 参数不匹配，则此规则为 NON_COMPLIANT。

标识符：S3_EVENT_NOTIFICATIONS_ENABLED

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

destinationArn（可选）, 类型：字符串

事件通知目标的亚马逊资源名称 (ARN)（亚马逊 SNS 主题、 AWS Lambda、亚马逊 SQS 队列）。

eventTypes（可选）, 类型：CSV

首选 Amazon S3 事件类型的逗号分隔列表

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-last-backup-recovery-point-created

检查是否为 Amazon Simple Storage Service (Amazon S3) 创建了恢复点。如果 Amazon S3 存储桶未在指定时间段内创建相应的恢复点，则此规则为 NON_COMPLIANT。

标识符：S3_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型： AWS::S3::Bucket

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Amazon S3 存储桶的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon S3 存储桶的名称。

恢复PointAgeValue （可选）, 类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit （可选）, 类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-lifecycle-policy-check

检查是否为 Amazon Simple Storage Service (Amazon S3) 存储桶配置了生命周期规则。如果没有有效的生命周期配置规则，或者配置与参数值不匹配，则此规则为 NON_COMPLIANT。

标识符：S3_LIFECYCLE_POLICY_CHECK

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

targetTransitionDays （可选）, 类型：int

对象在创建后过渡到指定存储类的天数（例如 30 天）。

targetExpirationDays （可选）, 类型：int

对象创建后删除对象的天数（例如，395 天）。

目标TransitionStorageClass （可选）, 类型：字符串

目标存储类类型（例如，Amazon S3 Standard-Infrequent Access (S3 Standard-IA）。有关更多信息，请参阅 https: //docs.aws.amazon.com/AmazonS3/latest/dev/storage-class-intro.html。

targetPrefix（可选）, 类型：字符串

用于标识一个或多个对象的 Amazon S3 对象前缀。

bucketNames（可选）, 类型：CSV

启用生命周期策略的 Amazon S3 存储桶名称的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-meets-restore-time-target

检查 Amazon Simple Storage Service (Amazon S3) 存储桶的还原时间是否符合指定的持续时间。如果 Amazon S3 存储桶 LatestRestoreExecutionTimeMinutes 的大于 maxRestoreTime 分钟，则该规则不合规。

标识符：S3_MEETS_RESTORE_TIME_TARGET

资源类型： AWS::S3::Bucket

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大 RestoreTime, 类型：int

允许的最大还原运行时间的数值。

resourceTags（可选）, 类型：字符串

此规则要检查的 Amazon S3 存储桶的标签，采用 JSON 格式 。

resourceId（可选）, 类型：字符串

此规则要检查的 Amazon S3 存储桶的名称。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-resources-protected-by-backup-plan

检查 Amazon Simple Storage Service (Amazon S3) 存储桶是否受备份计划的保护。如果备份计划不涵盖 Amazon S3 存储桶，则此规则为 NON_COMPLIANT。

标识符：S3_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型： AWS::S3::Bucket

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Amazon S3 存储桶的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选），类型：字符串

此规则要检查的 Amazon S3 存储桶的名称。

crossRegionList （可选），类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （可选），类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （可选），类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （可选），类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选），类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

s3-version-lifecycle-policy-check

检查启用了 Amazon Simple Storage Service (Amazon S3) 版本的存储桶是否配置了生命周期策略。如果未启用 Amazon S3 生命周期策略，则此规则为 NON_COMPLIANT。

标识符：S3_VERSION_LIFECYCLE_POLICY_CHECK

资源类型： AWS::S3::Bucket

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

bucketNames（可选），类型：CSV

启用生命周期策略的 Amazon S3 存储桶名称的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

sagemaker-endpoint-configuration-kms-key-configured

检查是否为亚马逊 SageMaker 终端节点配置配置了密 AWS 钥管理服务 (AWS KMS) 密钥。如果未为亚马逊 SageMaker 终端节点配置指定 “KmsKeyID”，则该规则不合规。

标识符：SAGEMAKER_ENDPOINT_CONFIGURATION_KMS_KEY_CONFIGURED

资源类型： AWS::SageMaker::EndpointConfig

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyArns （可选），类型：字符串

以逗号分隔的 Ama SageMaker zon 终端节点配置允许的特定 AWS KMS 密钥 ARN 列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

sagemaker 端点配置产品实例计数

检查 Amazon SageMaker 终端节点配置是否将生产变体 “InitialInstanceCount” 设置为大于 1 的值。如果生产变体 “InitialInstance计数” 等于 1，则该规则不合规。

标识符：SAGEMAKER_ENDPOINT_CONFIG_PROD_INSTANCE_COUN

资源类型： AWS::SageMaker::EndpointConfig

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

sagemaker-notebook-instance-inside-vpc

检查 Amazon SageMaker 笔记本实例是在 VPC 内启动的，还是在已批准的子网列表中启动。如果笔记本实例不是在 VPC 内启动，或者其子网 ID 未包含在参数列表中，则此规则为 NON_COMPLIANT。

标识符：SAGEMAKER_NOTEBOOK_INSTANCE_INSIDE_VPC

资源类型： AWS::SageMaker::NotebookInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

SubnetIds （可选），类型：CSV

笔记本实例可以在其中启动的子网 ID 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

sagemaker-notebook-instance-kms-key-configured

检查是否为 Amazon SageMaker 笔记本实例配置了密 AWS 钥管理服务 (AWS KMS) 密钥。如果未为笔记本实例指定 “KmsKeyID”，则该 SageMaker 规则不兼容。

标识符：SAGEMAKER_NOTEBOOK_INSTANCE_KMS_KEY_CONFIGURED

资源类型： AWS::SageMaker::NotebookInstance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyArns （可选），类型：字符串

以逗号分隔的 Ama SageMaker zon 笔记本实例允许的 AWS KMS 密钥 ARN 列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

sagemaker-notebook-instance-root-access-check

检查是否为亚马逊 SageMaker 笔记本实例启用了亚马逊 SageMaker RootAccess 设置。如果将 Amazon SageMaker 笔记本实例的 RootAccess 设置设置为 “已启用”，则该规则不合规。

标识符：SAGEMAKER_NOTEBOOK_INSTANCE_ROOT_ACCESS_CHECK

资源类型： AWS::SageMaker::NotebookInstance

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

sagemaker-notebook-no-direct-internet-access

检查 Amazon SageMaker 笔记本实例是否禁用了直接互联网接入。如果 SageMaker 笔记本实例支持互联网，则该规则不合规。

标识符：SAGEMAKER_NOTEBOOK_NO_DIRECT_INTERNET_ACCESS

资源类型： AWS::SageMaker::NotebookInstance

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

secretsmanager-rotation-enabled-check

检查 S AWS ecrets Manager 密钥是否启用了轮换。此外，该规则还检查可选 `maximumAllowedRotationFrequency` 参数。如果指定了参数，则密钥的轮换频率与允许的最大频率进行比较。如果密钥未计划轮换，则此规则为 NON_COMPLIANT。如果旋转频率高于 Frequency 参数中指定的数字，则该规则也是 NON_Complift。 maximumAllowedRotation

> **Note**
>
> 在首次评估后的 4 小时内重新评估此规则将不会对结果产生影响。

标识符： SECRETSMANAGER_ROTATION_ENABLED_CHECK

资源类型： AWS::SecretsManager::Secret

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

最大值AllowedRotationFrequency （可选），类型：int

密钥允许的最大轮换频率（以天为单位）。

最大值AllowedRotationFrequencyInHours （可选），类型：int

机密允许的最大轮换频率（以小时为单位）。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

secretsmanager-scheduled-rotation-success-check

检查 S AWS ecrets Manager 密钥是否根据轮换计划成功轮换。Secrets Manager 会计算应进行轮换的日期。如果日期已过但机密未轮换，则此规则为 NON_COMPLIANT。

> **Note**
>
> 对于不进行轮换的机密，此规则将返回 NOT_APPLICABLE。

标识符： SECRETSMANAGER_SCHEDULED_ROTATION_SUCCESS_CHECK

资源类型： AWS::SecretsManager::Secret

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

secretsmanager-secret-periodic-rotation

检查 S AWS ecrets Manager 的密钥是否在过去指定的天数内被轮换。如果密钥的轮换天数未超过 maxDaysSince轮换天数，则该规则为 NON_COMPLIMENT。默认值为 90 天。

标识符：SECRETSMANAGER_SECRET_PERIODIC_ROTATION

资源类型： AWS::SecretsManager::Secret

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

最大DaysSinceRotation （可选），类型：int

机密可以保持不变的最大天数。默认值为 90 天。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

secretsmanager-secret-unused

检查 S AWS ecrets Manager 密钥是否在指定的天数内被访问。如果在 “未使用ForDays” 天数内未访问密钥，则该规则不合规。默认值为 90 天。

背景：建议定期删除未使用的机密。未使用的机密可能会被不再需要访问这些机密的前用户滥用。此外，获得机密访问权的用户越多，有人滥用机密或将访问权授予未经授权实体的可能性也就越大。删除未使用的机密有助于撤消不再需要机密的用户的机密访问权限，还可以降低您使用 AWS Secrets Manager的成本。

标识符：SECRETSMANAGER_SECRET_UNUSED

资源类型： AWS::SecretsManager::Secret

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

unusedForDays （可选），类型：int

机密可以保持未使用状态的天数。默认值为 90 天。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

secretsmanager-using-cmk

检查中的 AWS Secrets Manager 所有密钥是否使用 AWS 托管式密钥 (`aws/secretsmanager`) 或在 () 中 AWS Key Management Service 创建的客户托管密钥进行加密。AWS KMS如果使用客户管理型密钥来加密机密，则此规则为 COMPLIANT。如果使用 `aws/secretsmanager` 加密机密，则此规则为 NON_COMPLIANT。

> **Note**
> 此规则无法访问跨账户客户管理型密钥，因此在使用跨账户密钥时，会将机密评估为 NON_COMPLIANT。

标识符：SECRETSMANAGER_USING_CMK

资源类型： AWS::SecretsManager::Secret

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyArns （可选），类型：CSV

KMS 密钥 Amazon Resource Names (ARN) 的逗号分隔列表，用于检查密钥是否用于加密。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

securityhub-enabled

检查 AWS 账户是否启用了 Sec AWS urity Hub。如果未启用 Sec AWS urity Hub，则该规则不合规。

Identifier (标识符)：SECURITYHUB_ENABLED

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

security-account-information-provided

检查您是否为 AWS 账户联系人提供了安全联系人信息。如果未提供账户内的安全联系人信息，则此规则为 NON_COMPLIANT。

标识符：SECURITY_ACCOUNT_INFORMATION_PROVIDED

资源类型：AWS::::Account

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

组织内共享的服务目录

在启用与 Organizations 的集成后，检查 S AWS ervice Catalog 是否与 AWS 组织共享投资组合（一组被视为单个单元的 AWS 账户）。如果股票的 “类型” 值为 “账户”，则该规则不合规。

标识符：SERVICE_CATALOG_SHARED_WITH IN_ORGAN

资源类型： AWS::ServiceCatalog::Portfolio

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

service-vpc-endpoint-enabled

检查是否已为每个 Amazon Virtual Private Cloud (Amazon VPC) 创建规则参数中提供的服务的服务终端节点。如果 Amazon VPC 没有为该服务创建 VPC 终端节点，则此规则为 NON_COMPLIANT。

标识符：SERVICE_VPC_ENDPOINT_ENABLED

资源类型：AWS:: EC2:: VPC

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

serviceName, 类型：字符串

> 服务的短名称或后缀。注意：要获取可用服务名称列表或有效后缀列表，请使用 DescribeVpcEndpointServices。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ses-malware-scanning-enabled

检查是否为 Amazon Simple Email Service (Amazon SES) 启用了接收邮件时的恶意软件和垃圾邮件扫描。如果未启用恶意软件和垃圾邮件扫描，则此规则为 NON_COMPLIANT。

标识符：SES_MALWARE_SCANNING_ENABLED

资源类型： AWS::SES::ReceiptRule

触发器类型： 定期

AWS 区域：仅适用于欧洲地区（爱尔兰）、美国东部（弗吉尼亚州北部）、美国西部（俄勒冈州）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

shield-advanced-enabled-autorenew

检查您的 AWS 账户中是否启用了 AWS Shield Advanced 以及此订阅是否设置为自动续订。如果启用了 Shield Advanced 并启用了自动续订，则此规则为 COMPLIANT。

> **Note**
>
> 的 API 终端节点 AWS Shield Advanced 仅在美国东部（弗吉尼亚北部）区域可用。此规则应仅安排在美国东部（弗吉尼亚州北部）区域中运行。

标识符：SHIELD_ADVANCED_ENABLED_AUTORENEW

触发器类型： 定期

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

shield-drt-access

检查 Shield 响应小组 (SRT) 是否可以访问您的 AWS 账户。如果已启用，但未配置 SRT 访问的角色，AWS Shield Advanced 则该规则不兼容。

标识符：SHIELD_DRT_ACCESS

触发器类型： 定期

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

sns-encrypted-kms

检查 SNS 主题是否使用 AWS 密钥管理服务 (AWS KMS) 加密。如果 SNS 主题未使用 KMS 加密，则该规则不合规。 AWS 或者，为要检查的规则指定密钥 ARN、别名 ARN、别名或密钥 ID。

Identifier (标识符)：SNS_ENCRYPTED_KMS

资源类型： AWS::SNS::Topic

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

kmsKeyIds （可选），类型：CSV

以逗号分隔的 AWS KMS 密钥 Amazon 资源名称 (ARN)、KMS 别名 ARN、KMS 别名或 KMS 密钥 ID 列表，供规则检查。

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "KmsMasterKeyId": "my-kms-key-Id"
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

sns-topic-message-delivery-notification-enabled

检查是否已启用 Amazon Simple Notification Service (SNS) 日志记录，以记录发送到端点主题的通知消息的传送状态。如果未启用消息的传送状态通知，则此规则为 NON_COMPLIANT。

标识符：SNS_TOPIC_MESSAGE_DELIVERY_NOTIFICATION_ENABLED

资源类型： AWS::SNS::Topic

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

ssm-document-not-public

检查该账户拥有的 AWS Systems Manager 文档是否公开。如果所有者为“Self”的 Systems Manager 文档是公有的，则此规则为 NON_COMPLIANT。

标识符：SSM_DOCUMENT_NOT_PUBLIC

资源类型： AWS::SSM::Document

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

step-functions-state-machine-logging-enabled

检查 Ste AWS p Functions 计算机是否启用了日志功能。如果状态机未启用日志记录，或日志记录配置未达到提供的最低级别，则此规则为 NON_COMPLIANT。

标识符：STEP_FUNCTIONS_STATE_MACHINE_LOGGING_ENABLED

资源类型： AWS::StepFunctions::StateMachine

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

云WatchLogGroupArns （可选）, 类型：CSV

以逗号分隔的 Amazon CloudWatch 日志组的亚马逊资源名称 (ARN) 列表。此规则检查是否为状态机日志配置了指定的日志组。

logLevel（可选）, 类型：字符串

状态机的最低日志级别。有效值包括：ALL、ERROR、FATAL。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

storagegateway-last-backup-recovery-point-created

检查是否为 AWS Storage Gateway 卷创建了恢复点。如果 Storage Gateway 卷没有在指定时间段内创建相应的恢复点，则此规则为 NON_COMPLIANT。

标识符：STORAGEGATEWAY_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型： AWS::StorageGateway::Volume

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选）, 类型：字符串

此规则要检查的 Storage Gateway 卷的标签，采用 JSON 格式 `{"tagkey" : "tagValue"}`。

resourceId（可选）, 类型：字符串

此规则要检查的 Storage Gateway 卷的 ID。

恢复PointAgeValue （可选）, 类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit （ 可选 ）, 类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

storagegateway-resources-protected-by-backup-plan

检查 AWS Storage Gateway 卷是否受备份计划的保护。如果 Storage Gateway 卷不在备份计划范围内，则此规则为 NON_COMPLIANT。

标识符：STORAGEGATEWAY_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型： AWS::StorageGateway::Volume

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（ 可选 ）, 类型：字符串

此规则要检查的 Storage Gateway 卷的标签，采用 JSON 格式。

resourceId（ 可选 ）, 类型：字符串

此规则要检查的 Storage Gateway 卷的 ID。

crossRegionList （ 可选 ）, 类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （ 可选 ）, 类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （ 可选 ）, 类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （ 可选 ）, 类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选），类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

subnet-auto-assign-public-ip-disabled

检查 Amazon Virtual Private Cloud (Amazon VPC) 子网是否分配了公有 IP 地址。如果 Amazon VPC 没有分配了公有 IP 地址的子网，则此规则为 COMPLIANT。如果 Amazon VPC 的子网分配了公有 IP 地址，则此规则为 NON_COMPLIANT。

标识符：SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED

资源类型： AWS::EC2::Subnet

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

主动评估

有关如何在主动模式下运行此规则的步骤，请参阅使用 AWS Config 规则评估您的资源。为了使此规则在主动模式下返回合规，StartResource评估 API 的资源配置架构需要包含以下以字符串形式编码的输入：

```
"ResourceConfiguration":
...
{
   "MapPublicIpOnLaunch": BOOLEAN
}
...
```

有关主动评估的更多信息，请参阅评估模式。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

传输家庭服务器没有 FTP

检查使用 Transfer Famil AWS y 创建的服务器是否使用 FTP 进行端点连接。如果端点连接的服务器协议启用 FTP，则该规则不兼容。

标识符：传输家庭服务器_NO_FTP

资源类型： AWS::Transfer::Server

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

virtualmachine-last-backup-recovery-point-created

检查是否为 AWS 备份 VirtualMachines网关创建了恢复点。如果 AWS 备份网关在指定时间段内没有创建相应的恢复点，则 VirtualMachines 该规则不合规。

标识符：VIRTUALMACHINE_LAST_BACKUP_RECOVERY_POINT_CREATED

资源类型： AWS::BackupGateway::VirtualMachine

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选），类型：字符串

待规则检查的 AWS 备份网关标签，采 VirtualMachines 用 JSON 格式。`{"tagkey" : "tagValue"}`

resourceId（可选），类型：字符串

要检查的规则的 AWS 备份网关 VirtualMachine 的 ID。

恢复PointAgeValue （可选），类型：int, 默认值：1

表示最长允许期限的数值。不超过 744 小时或 31 天。

恢复PointAgeUnit （可选），类型：字符串, 默认值：days

表示最长允许期限的时间单位。接受的值：“hours”、“days”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

virtualmachine-resources-protected-by-backup-plan

检查 AWS 备份网关是否 VirtualMachines 受备份计划的保护。如果备份网关不在备份 VirtualMachine 计划范围内，则该规则不合规。

标识符：VIRTUALMACHINE_RESOURCES_PROTECTED_BY_BACKUP_PLAN

资源类型： AWS::BackupGateway::VirtualMachine

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

resourceTags（可选），类型：字符串

待规则检查的 AWS 备份网关标签，采 VirtualMachines 用 JSON 格式。`{"tagkey" : "tagValue"}`

resourceId（可选），类型：字符串

要检查的规则的 AWS 备份网关 VirtualMachine 的 ID。

crossRegionList （可选），类型：字符串

逗号分隔的目标区域列表，用于保存跨区域备份副本

crossAccountList （可选），类型：字符串

逗号分隔的目标账户列表，用于保存跨账户备份副本

maxRetentionDays （可选），类型：int

备份保管库锁的最长保留期（以天为单位）

minRetentionDays （可选），类型：int

备份保管库锁的最短保留期（以天为单位）

备份VaultLockCheck （可选），类型：字符串

接受的值：“True”或“False”。输入“True”，可让规则检查资源是否已备份到锁定的保管库中

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

vpc-default-security-group-closed

检查任何 Amazon Virtual Private Cloud (Amazon VPC) 的默认安全组是否不允许入站或出站流量。如果默认安全组具有一个或多个入站或出站流量规则，则此规则为 NON_COMPLIANT。

> **Note**
>
> 在 AWS Config 记录相关资源（例如默认安全组）的删除之间可能会有一段延迟，这些资源在 Amazon VPC 删除过程中被删除。因此，即使所有默认安全组或其他相关资源都已删除或修复，此规则仍可能报告为 NON_COMPLIANT，直至下一次账户基准化流程。

标识符：VPC_DEFAULT_SECURITY_GROUP_CLOSED

资源类型： AWS::EC2::SecurityGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

vpc-flow-logs-enabled

检查是否找到并为所有 Amazon VPC 启用了 Amazon Virtual Private Cloud (Amazon VPC) 流日志。如果没有为至少一个 Amazon VPC 启用流日志，则此规则为 NON_COMPLIANT。

标识符：VPC_FLOW_LOGS_ENABLED

资源类型：AWS:: EC2:: VPC

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

trafficType（可选），类型：字符串

TrafficType 的流日志

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

vpc-network-acl-unused-check

检查是否存在未使用的网络访问控制列表（网络 ACL）。如果每个网络 ACL 都与某个子网关联，则此规则为 COMPLIANT。如果网络 ACL 未与子网关联，则此规则为 NON_COMPLIANT。

标识符：VPC_NETWORK_ACL_UNUSED_CHECK

资源类型： AWS::EC2::NetworkAcl

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

vpc-peering-dns-resolution-check

检查是否启用了从接受者/请求者 VPC 到私有 IP 的 DNS 解析。如果未启用从接受者/请求者 VPC 到私有 IP 的 DNS 解析，则此规则为 NON_COMPLIANT。

标识符：VPC_PEERING_DNS_RESOLUTION_CHECK

资源类型：AWS:: EC2:: VPC PeeringConnection

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

vpcIds（可选），类型：CSV

要检查的 VPC ID 的逗号分隔列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

vpc-sg-open-only-to-authorized-ports

检查允许无限制传入流量的安全组（“0.0.0.0/0”或“::/0”）是否只允许授权端口上的传入 TCP 或 UDP 连接。如果此类安全组的规则参数中未指定端口，则此规则为 NON_COMPLIANT。

> **Note**
>
> 此规则评估入口规则设置为 IPv4='0.0.0.0/0' 或 IPv6='::/' 的 Amazon EC2 安全组。如果安全组没有这些目的地之一，则此规则返回 `NOT_APPLICABLE`。

标识符：VPC_SG_OPEN_ONLY_TO_AUTHORIZED_PORTS

资源类型： AWS::EC2::SecurityGroup

触发器类型：配置更改和定期

AWS 区域: 所有支持的 AWS 区域

参数：

authorizedTcpPorts （可选），类型：字符串

允许向 0.0.0.0/0 或 ::/0 开放的 TCP 端口的逗号分隔列表。以短划线定义范围，例如：“443,1020-1025”。

authorizedUdpPorts （可选），类型：字符串

允许向 0.0.0.0/0 或 ::/0 开放的 UDP 端口的逗号分隔列表。以短划线定义范围，例如：“500,1020-1025”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

vpc-sg-port 限制检查

检查安全组是否明确限制从 0.0.0.0/0 或:: /0 到受限端口的传入流量。如果安全组允许通过 TCP/UDP 端口 22/3389 或参数中指定的来自 0.0.0.0/0 或:: /0 的传入流量，则该规则不合规。

标识符：VPC_SG_PORT_RESTRICTION_CHECK

资源类型： AWS::EC2::SecurityGroup

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

限制端口（可选），类型：CSV

以逗号分隔的端口列表，这些端口不应为整个 IP 范围内的传入流量开放。有效的端口号范围为 0 到 65535。如果未指定，则该规则默认为检查 22 和 3389。

协议类型（可选），类型：字符串

要检查的规则的传输协议类型。有效值包括 'TCP'、'UDP' 和 'ALL'（不区分大小写）。如果设置为 “全部”，则该规则将检查是否有使用 “TCP”、“UDP” 或 “ALL” (-1) 协议的规则。默认值为 “全部”。

排除ExternalSecurityGroups （可选），类型：布尔值

布尔值标志，用于排除对外部安全组的评估。如果设置为 “true”，则该规则在评估中将不包括外部安全组。否则，如果值设置为 “false”，则会评估所有安全组。默认值为 “真”。

IP 类型（可选），类型：字符串

要检查的规则的互联网协议 (IP) 版本。有效值包括 'IPv4'、'IPv6' 和 'ALL'（不区分大小写）。如果未指定，则该规则默认为检查 “全部”。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

vpc-vpn-2-tunnels-up

检查 AWS 站点到站点 VPN 提供的两个虚拟专用网络 (VPN) 隧道是否都处于 UP 状态。如果一个或两个隧道处于 DOWN 状态，则此规则为 NON_COMPLIANT。

标识符：VPC_VPN_2_TUNNELS_UP

资源类型：AWS::EC2::VPNConnection

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

wafv2-logging-enabled

检查 AWS Wafv2 区域和全球 Web 访问控制列表 (Web ACL) 上是否启用了日志记录。如果启用了日志记录但日志记录目标与参数值不匹配，则此规则为 NON_COMPLIANT。

标识符：WAFV2_LOGGING_ENABLED

资源类型： AWS::WAFv2::WebACL

触发器类型： 定期

AWS 区域: 所有支持的 AWS 区域

参数：

KinesisFirehoseDeliveryStreamArns （可选），类型：CSV

Kinesis Firehose 传输流 ARN 的逗号分隔列表

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

wafv2-rulegroup-logging-enabled

检查是否启用了 AWS Wafv2 规则组上的 Amazon CloudWatch 安全指标收集。如果是 '，则该规则不合规。VisibilityConfig CloudWatchMetricsEnabled'字段设置为 false。

上下文： AWS WAFV2 （Web 应用程序防火墙版本 2）允许您创建 AWS WAF 规则来保护 Web 应用程序免受常见 Web 漏洞和漏洞的侵害。 AWS WAF 规则组是可以与 Web ACL（访问控制列表）关联的 AWS WAF 规则集合，用于定义 Web 应用程序流量所需的行为。有关更多信息，请参阅AWS WAF《AWS WAF开发者指南》中的规则和规则组。

通过在 AWS WAFV2 规则组上配置 CloudWatch 安全指标收集，您可以监控安全指标，例如成功或失败的分布式拒绝服务 (DDoS)、SQL 注入和跨站点脚本 (XSS) 攻击。收集的安全指标可以帮助您简化调查。

> **Note**
>
> 如果规则组中没有可供托管 AWS WAF 规则检查的 AWS WAFV2 规则，则 AWS Config 托管规则将返回 NON_AP AWS Config PLIABLE。

标识符：WAFV2_RULEGROUP_LOGGING_ENABLED

资源类型： AWS::WAFv2::RuleGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

wafv2-rulegroup-not-empty

检查 WAFv2 规则组是否包含规则。如果 WAFv2 规则组中没有规则，则此规则为 NON_COMPLIANT。

标识符：WAFV2_RULEGROUP_NOT_EMPTY

资源类型： AWS::WAFv2::RuleGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

wafv2-webacl-not-empty

检查 WAFv2 Web ACL 是否包含任何 WAF 规则或 WAF 规则组。如果 Web ACL 不包含任何 WAF 规则或 WAF 规则组，则此规则为 NON_COMPLIANT。

标识符：WAFV2_WEBACL_NOT_EMPTY

资源类型： AWS::WAFv2::WebACL

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

waf-classic-logging-enabled

检查 AWS WAF 经典版全局 Web 访问控制列表 (Web ACL) 上是否启用了日志记录。如果全局 Web ACL 未启用日志记录，则此规则为 NON_COMPLIANT。

标识符：WAF_CLASSIC_LOGGING_ENABLED

资源类型： AWS::WAF::WebACL

触发器类型： 定期

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

KinesisFirehoseDeliveryStreamArns （可选），类型：CSV

以逗号分隔的 WAF 日志的 Amazon Kinesis 直播 AR AWS N 列表。

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

waf-global-rulegroup-not-empty

检查 AWS WAF 经典规则组是否包含任何规则。如果规则组中不存在任何规则，则此规则为 NON_COMPLIANT。

标识符：WAF_GLOBAL_RULEGROUP_NOT_EMPTY

资源类型： AWS::WAF::RuleGroup

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

waf-global-rule-not-empty

检查 AWS WAF 全局规则是否包含任何条件。如果 WAF 全局规则中不存在任何条件，则此规则为 NON_COMPLIANT。

标识符：WAF_GLOBAL_RULE_NOT_EMPTY

资源类型： AWS::WAF::Rule

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

waf-global-webacl-not-empty

检查 WAF 全局 Web ACL 是否包含任何 WAF 规则或规则组。如果 Web ACL 不包含任何 WAF 规则或规则组，则此规则为 NON_COMPLIANT。

标识符：WAF_GLOBAL_WEBACL_NOT_EMPTY

资源类型： AWS::WAF::WebACL

触发器类型： 配置更改

AWS 区域：仅适用于美国东部（弗吉尼亚州北部）区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

waf-regional-rulegroup-not-empty

检查 WAF 区域规则组是否包含任何规则。如果 WAF 区域规则组中不存在任何规则，则此规则为 NON_COMPLIANT。

标识符：WAF_REGIONAL_RULEGROUP_NOT_EMPTY

资源类型： AWS::WAFRegional::RuleGroup

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

waf-regional-rule-not-empty

检查 WAF 区域规则是否包含条件。如果区域规则至少包含一个条件，则此规则为 COMPLIANT，否则为 NON_COMPLIANT。

标识符：WAF_REGIONAL_RULE_NOT_EMPTY

资源类型： AWS::WAFRegional::Rule

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

waf-regional-webacl-not-empty

检查 WAF 区域 Web ACL 是否包含任何 WAF 规则或规则组。如果 Web ACL 中不存在任何 WAF 规则或规则组，则此规则为 NON_COMPLIANT。

标识符：WAF_REGIONAL_WEBACL_NOT_EMPTY

资源类型： AWS::WAFRegional::WebACL

触发器类型： 配置更改

AWS 区域: 所有支持的 AWS 区域

参数：

无

AWS CloudFormation 模板

要使用 AWS CloudFormation 模板创建 AWS Config 托管规则，请参阅使用 AWS CloudFormation 模板创建 AWS Config 托管规则。

按评估模式列出的 AWS Config 托管规则列表

AWS Config 目前支持以下托管规则。

注意事项

托管规则的默认值

只有在使用 AWS 控制台时，才会预先填充为托管规则指定的默认值。未提供 API、CLI 或 SDK 的默认值。

不支持目录存储桶

在评估亚马逊简单存储服务 (Amazon S3) 资源时，托管规则仅支持通用存储桶。 AWS Config 不记录目录存储桶的配置更改。有关通用存储桶和目录存储桶的更多信息，请参阅 Amazon S3 用户指南中的存储桶概述和目录存储桶。

托管规则和全球 IAM 资源类型

2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。

为避免不必要的评估，您只应定期部署规则，向支持的区域之一报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

主动评估

主动规则 是支持对尚未部署的资源采用主动评估模式的规则。这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。有关更多信息，请参阅评估模式。

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

主动评估

- api-gw-xray-enabled
- autoscaling-group-elb-healthcheck-required
- ec2-instance-multiple-eni-check
- eip-attached
- elasticsearch-node-to-node-encryption-check
- lambda-function-settings-check
- lambda-inside-vpc
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-public-access-check
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- s3-bucket-logging-enabled
- sns-encrypted-kms

- subnet-auto-assign-public-ip-disabled

侦查评估

侦查规则 是支持已部署资源的侦查评估模式的规则。这允许您评估现有资源的配置设置。

> **Note**
>
> 目前，所有 AWS Config 规则都支持侦探评估。

侦查评估

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf

- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols

- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 存储桶禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target

- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问

- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled

- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- 我启用了外部访问分析器
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam 服务器证书到期检查
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose 传送流经过加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check

- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw

- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled

- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty

- waf-regional-webacl-not-empty

按触发器类型列出的 AWS Config 托管规则列表

AWS Config 目前支持以下托管规则。

注意事项

托管规则的默认值

只有在使用 AWS 控制台时，才会预先填充为托管规则指定的默认值。未提供 API、CLI 或 SDK 的默认值。

不支持目录存储桶

在评估亚马逊简单存储服务 (Amazon S3) 资源时，托管规则仅支持通用存储桶。 AWS Config 不记录目录存储桶的配置更改。有关通用存储桶和目录存储桶的更多信息，请参阅 Amazon S3 用户指南中的存储桶概述和目录存储桶。

托管规则和全球 IAM 资源类型

2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group`、`AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。

为避免不必要的评估，您只应定期部署规则，向其中一个支持的区域报告全球 IAM 资源类型的合规性。有关哪些区域支持哪些托管规则的列表，请参阅按区域可用性列出的 AWS Config 托管规则列表。

配置更改

变更触发的规则是 AWS Config 根据配置更改进行评估的规则。

配置更改

- acm-certificate-rsa-check

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check

- clb-multiple-az
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-settings-check
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- db-instance-backup-enabled

- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- ebs-optimized-instance
- ec2-client-vpn-connection-log-enabled
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks-cluster-supported-version
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check

- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- global-endpoint-event-replication-enabled
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-user-group-membership-check
- iam-user-no-policies-check
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled

- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-using-cmk
- 组织内共享的服务目录
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

定期

定期规则是按照您指定的频率定期 AWS Config 评估的规则；例如，每 24 小时评估一次。

定期

- access-keys-rotated
- account-part-of-organizations
- acm-pca-root-ca-disabled

- alb-http-to-https-redirection-check
- api-gwv2-authorization-type-configured
- appsync-associated-with-waf
- appsync-cache-encryption-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-resource-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-resources-protected-by-backup-plan
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-last-backup-recovery-point-created
- ec2-meets-restore-time-target
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ecr-private-image-scanning-enabled
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eks-cluster-logging-enabled
- eks集群密钥已加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest

- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elbv2-acm-certificate-required
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam 外部访问分析器已启用
- iam-password-policy
- iam-policy-in-use
- iam-root-access-key-check
- iam 服务器证书到期检查
- iam-user-mfa-enabled

- iam-user-unused-credentials-check
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- kinesis-firehose-delivery-stream 加密
- kms-cmk-not-scheduled-for-deletion
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-automatic-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- mq-no-public-access
- multi-region-cloud-trail-enabled
- netfw-logging-enabled
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-resources-protected-by-backup-plan
- redshift-不受限制的端口访问权限
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-account-level-public-access-blocks-periodic
- s3-last-backup-recovery-point-created
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- securityhub-enabled
- security-account-information-provided
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-flow-logs-enabled
- vpc-sg-port 限制检查
- wafv2-logging-enabled
- waf-classic-logging-enabled

混合

混合规则是针对配置更改 AWS Config 进行评估和定期评估的规则。

混合

- acm-certificate-expiration-check
- cloudformation-stack-drift-detection-check
- incoming-ssh-disabled
- restricted-incoming-traffic
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- vpc-sg-open-only-to-authorized-ports

按区域可用性列出的 AWS Config 托管规则列表

AWS Config 目前支持以下托管规则。

注意事项

托管规则的默认值

只有在使用 AWS 控制台时，才会预先填充为托管规则指定的默认值。未提供 API、CLI 或 SDK 的默认值。

不支持目录存储桶

在评估亚马逊简单存储服务 (Amazon S3) 资源时，托管规则仅支持通用存储桶。 AWS Config 不记录目录存储桶的配置更改。有关通用存储桶和目录存储桶的更多信息，请参阅 Amazon S3 用户指南中的存储桶概述和目录存储桶。

托管规则和全球 IAM 资源类型

2022 年 2 月之前加入的全球 IAM 资源类型（`AWS::IAM::Group``AWS::IAM::Policy`、`AWS::IAM::Role`、和`AWS::IAM::User`）只能在 2022 年 2 月之前可用的 AWS AWS Config 区域 AWS Config 中进行记录。2022 年 2 月 AWS Config 之后将无法在支持的区域中记录这些资源类型。有关这些区域的列表，请参阅录制 AWS 资源 | 全球资源。

如果您在至少一个区域记录全球 IAM 资源类型，则报告全球 IAM 资源类型合规性的定期规则将在添加定期规则的所有区域进行评估，即使您尚未在添加定期规则的地区启用全球 IAM 资源类型的记录。

为避免不必要的评估，您只应定期部署规则，向支持的区域之一报告全球 IAM 资源类型的合规性。

美国东部（俄亥俄州）区域

美国东部（俄亥俄州）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled

- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check

- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target

- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check

- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions

- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check

- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw

- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled

- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

美国东部（弗吉尼亚州北部）区域

美国东部（弗吉尼亚州北部）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template

- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-accesslogs-enabled
- cloudfront-associated-with-waf
- cloudfront-custom-ssl-certificate
- cloudfront-default-root-object-configured
- cloudfront-no-deprecated-ssl-protocols
- cloudfront-origin-access-identity-enabled
- cloudfront-origin-failover-enabled
- cloudfront-s3-origin-access-control-enabled
- cloudfront-s3-origin-non-existent-bucket
- cloudfront-security-policy-check
- cloudfront-sni-enabled
- cloudfront-traffic-to-origin-encrypted
- cloudfront-viewer-policy-https
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check

- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all

- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged

- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest

- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled

- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam 服务器证书到期检查
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用

- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled

- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限

- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- route53-query-logging-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan

- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- shield-advanced-enabled-autorenew
- shield-drt-access
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-classic-logging-enabled
- waf-global-rulegroup-not-empty
- waf-global-rule-not-empty
- waf-global-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

美国西部（北加利福尼亚）区域

美国西部（加利福尼亚北部）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled

- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled

- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured

- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check

- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls

- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check

- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check

- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check

- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

美国西部（俄勒冈州）区域

美国西部（俄勒冈州）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached

- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check

- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP

- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

非洲（开普敦）区域

非洲（开普敦）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled

- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 启用 dms-redis-tls
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging

- dynamodb-autoscaling-enabled
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni

- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only

- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

亚太地区（香港）区域

亚太地区（香港）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查

- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check

- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip

- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check

- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check

- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings

- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets

- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

亚太地区（海得拉巴）区域

亚太地区（海得拉巴）

- acm-certificate-expiration-check

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted

- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs挂载目标可公开访问

- eip-attached
- eks-cluster-log-enabled
- eks集群密钥已加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-s3 保护

- iam 外部访问分析器已启用
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-firehose-delivery-stream 加密
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic

- s3-bucket-acl-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker 端点配置产品实例计数
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled

- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

亚太地区（雅加达）区域

亚太地区（雅加达）

- access-keys-rotated
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- approved-amis-by-id
- approved-amis-by-tag
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-multiple-az
- clb-multiple-az
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled

- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-stopped-instance

- ec2-volume-inuse-check
- ecs-task-definition-user-for-host-mode-check
- efs挂载目标可公开访问
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks集群密钥已加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-supported-engine-version
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured

- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- kinesis-firehose-delivery-stream 加密
- lambda-function-public-access-prohibited

- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-rabbit-deployment-mode
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted

- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-default-admin-check
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-version-lifecycle-policy-check

- sagemaker 端点配置产品实例计数
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled

亚太地区（墨尔本）区域

亚太地区（墨尔本）

- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check

- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled

- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets

- ecs-task-definition-pid-mode-check
- efs挂载目标可公开访问
- eip-attached
- eks集群密钥已加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-s3 保护
- iam 外部访问分析器已启用
- iam-password-policy
- iam-root-access-key-check
- incoming-ssh-disabled

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled

- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker 端点配置产品实例计数
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

亚太地区（孟买）区域

亚太地区（孟买）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled

- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target

- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached

- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check

- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled

- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest

- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled

- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled

- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan

- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

亚太地区（大阪）区域

亚太地区（大阪）

- access-keys-rotated
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled

- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-envvar-awscred-check
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 启用 dms-redis-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-launch-template-public-ip-disabled
- ec2-no-amazon-key-pair
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecs-containers-readonly-access
- efs-access-point-enforce-root-directory

- efs-access-point-enforce-user-identity
- efs挂载目标可公开访问
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks集群密钥已加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-supported-engine-version
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elbv2-multiple-az
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时

- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-function-public-access-prohibited
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode

- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-cluster-default-admin-check
- rds-cluster-encrypted-at-rest
- rds-instance-default-admin-check
- rds-instance-public-access-check
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check

- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 组织内共享的服务目录
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- 传输家庭服务器没有 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-peering-dns-resolution-check
- vpc-sg-port 限制检查
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

亚太地区（首尔）区域

亚太地区（首尔）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 存储桶禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled

- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target

- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan

- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled

- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy

- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled

- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance

- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled

- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled

- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created

- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

亚太地区（新加坡）区域

亚太地区（新加坡）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled

- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check

- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 存储桶禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target

- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target

- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问

- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled

- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check

- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access

- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled

- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited

- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled

- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

亚太地区（悉尼）区域

亚太地区（悉尼）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled

- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 存储桶禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled

- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan

- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check

- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created

- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled

- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check

- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查

- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled

- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Asia Pacific（Tokyo）Region

Asia Pacific (Tokyo)

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check

- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled

- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 存储桶禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check

- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check

- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az

- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions

- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc

- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated

- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled

- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

加拿大（中部）区域

加拿大（中部）

- access-keys-rotated

- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 存储桶禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled

- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited

- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan

- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required

- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用

- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- inspector-ec2-scan 已启用
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查

- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled

- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan

- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms

- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

Canada West (Calgary) Region

加拿大西部（卡尔加里）

- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- approved-amis-by-id

- approved-amis-by-tag
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-encryption-enabled
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- eip-attached
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- encrypted-volumes
- incoming-ssh-disabled
- instances-in-vpc

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- required-tags
- restricted-incoming-traffic
- s3-account-level-public-access-blocks-periodic
- s3-bucket-blacklisted-actions-prohibited
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-vpn-2-tunnels-up

中国（北京）区域

中国（北京）

- access-keys-rotated
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2

- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudfront-s3-origin-non-existent-bucket
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 存储桶禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check

- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-paravirtual-instance-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest

- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled

- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled

- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports

- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

中国（宁夏）区域

中国（宁夏）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-authorization-check
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit

- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check

- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-launch-template-public-ip-disabled

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-encrypted-check
- efs-in-backup-plan
- eip-attached
- eks-cluster-log-enabled
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest

- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- guardduty-enabled-centralized
- guardduty-non-archived-findings
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted

- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks

- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- security-account-information-provided
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled

- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- subnet-auto-assign-public-ip-disabled
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- wafv2-rulegroup-logging-enabled
- wafv2-webacl-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧洲地区（法兰克福）区域

欧洲地区（法兰克福）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check

- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check

- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created

- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled

- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access

- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check

- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled

- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力

- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check

- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created

- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed

- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧洲地区（爱尔兰）区域

欧洲地区（爱尔兰）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check

- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check

- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached

- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan

- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check

- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version

- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes

- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check

- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode

- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check

- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check

- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- ses-malware-scanning-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP

- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧洲地区（伦敦）区域

欧洲地区（伦敦）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured

- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled

- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check

- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms

- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic

- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version

- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled

- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access

- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志

- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only

- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled

- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled

- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP

- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧洲地区（米兰）

欧洲地区（米兰）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled

- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查

- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证

- 启用 dms-redis-tls
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled

- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问

- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access

- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled

- iam-user-no-policies-check
- iam-user-unused-credentials-check
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-deletion-protection-enabled

- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-last-backup-recovery-point-created
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-cluster-configuration-check

- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms

- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-root-access-check
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check

- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧洲地区（巴黎）区域

欧洲地区（巴黎）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled

- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-mysql-backtracking-enabled
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问

- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check

- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target

- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan

- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled

- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest

- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled

- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc

- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧洲地区（西班牙）区域

欧洲（西班牙）

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志

- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- ebs-optimized-instance
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version

- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs挂载目标可公开访问
- eip-attached
- eks-cluster-log-enabled
- eks集群密钥已加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-s3 保护

- iam 外部访问分析器已启用
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- kinesis-firehose-delivery-stream 加密
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- rds-instance-default-admin-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-mfa-delete-enabled
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-versioning-enabled
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker 端点配置产品实例计数
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation

- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

欧洲地区（斯德哥尔摩）区域

欧洲地区（斯德哥尔摩）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf

- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az

- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy

- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm

- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration

- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-openzfs-copy-tags-enabled
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时

- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 代码扫描功能
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密

- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted

- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-default-admin-check
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check

- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks

- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check

- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty

- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

欧洲（苏黎世）

欧洲（苏黎世）

- account-part-of-organizations
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-mysql-backtracking-enabled
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志

- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check

- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs挂载目标可公开访问
- eip-attached
- eks-cluster-log-enabled
- eks集群密钥已加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elbv2-multiple-az
- elb-deletion-protection-enabled
- elb-logging-enabled
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check

- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-s3 保护
- iam 外部访问分析器已启用
- iam-password-policy
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled

- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-snapshot-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker 端点配置产品实例计数
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up

- wafv2-rulegroup-logging-enabled

以色列（特拉维夫）区域

以色列（特拉维夫）

- account-part-of-organizations
- alb-desync-mode-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check

- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-security-group-attached-to-eni
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- eip-attached
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elb-cross-zone-load-balancing-enabled
- elb-logging-enabled
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- 已启用 guardduty-s3 保护
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc

- macie自动敏感数据发现检查
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-automatic-minor-version-upgrade-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-storage-encrypted
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker 端点配置产品实例计数
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- vpc-default-security-group-closed
- vpc-network-acl-unused-check
- vpc-sg-port 限制检查
- wafv2-webacl-not-empty

中东（巴林）区域

中东（巴林）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan
- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted

- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- custom-eventbus-policy-attached
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance

- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user
- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled

- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan

- fsx-windows-audit-log-configured
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only

- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled

- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled
- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check

- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited

- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided

- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

中东（阿联酋）区域

中东（阿联酋）

- account-part-of-organizations
- acm-certificate-expiration-check

- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- clb-multiple-az
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- codebuild-project-envvar-awscred-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dynamodb-autoscaling-enabled
- dynamodb-pitr-enabled
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-optimized-instance
- ebs-snapshot-public-restorable-check
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-volume-inuse-check
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled

- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-pid-mode-check
- efs挂载目标可公开访问
- eks-cluster-log-enabled
- eks集群密钥已加密
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- emr-block-public-access
- emr-kerberos-enabled
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-lustre-copy-tags-to-backups
- fsx-windows-audit-log-configured
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时

- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护
- guardduty-non-archived-findings
- 已启用 guardduty-s3 保护
- iam 外部访问分析器已启用
- iam-password-policy
- incoming-ssh-disabled
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mq-active-deployment-mode
- mq-auto-minor-version-upgrade-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-rabbit-deployment-mode
- nacl-no-unrestricted-ssh-rdp
- no-unrestricted-route-to-igw
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-cluster-encrypted-at-rest
- rds-cluster-iam-authentication-enabled
- rds-cluster-multi-az-enabled
- rds-enhanced-monitoring-enabled

- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-logging-enabled
- rds-multi-az-support
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check

- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-lifecycle-policy-check
- s3-version-lifecycle-policy-check
- sagemaker 端点配置产品实例计数
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- security-account-information-provided
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- ssm-document-not-public
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-rulegroup-logging-enabled

南美洲（圣保罗）区域

南美洲（圣保罗）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- acm-certificate-rsa-check
- acm-pca-root-ca-disabled
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gwv2-access-logs-enabled
- api-gwv2-authorization-type-configured
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- appsync-associated-with-waf
- appsync-authorization-check
- appsync-cache-encryption-at-rest
- appsync-logging-enabled
- athena-workgroup-encrypted-at-rest
- aurora-last-backup-recovery-point-created
- aurora-meets-restore-time-target
- aurora-resources-protected-by-backup-plan

- autoscaling-capacity-rebalancing
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-hop-limit
- autoscaling-launch-config-public-ip-disabled
- autoscaling-launch-template
- autoscaling-multiple-az
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- clb-multiple-az
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-action-enabled-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled

- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-artifact-encryption
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- codedeploy-auto-rollback-monitor-enabled
- codedeploy-ec2-minimum-healthy-hosts-configured
- codedeploy-lambda-allatonce-traffic-shift-disabled
- codepipeline-deployment-count-check
- codepipeline-region-fanout-check
- custom-eventbus-policy-attached
- custom-schema-registry-policy-attached
- cw-loggroup-retention-period-check
- dax-encryption-enabled
- dax-tls-端点加密
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- dms-auto-minor-version-upgrade-check
- dms-endpoint-ssl-configured
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dms-replication-task-sourcedb-logging
- dms-replication-task-targetdb-logging

- docdb-cluster-audit-logging-enabled
- docdb-cluster-backup-retention-check
- docdb-cluster-deletion-protection-enabled
- docdb-cluster-encrypted
- docdb-cluster-snapshot-public-prohibited
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-meets-restore-time-target
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-meets-restore-time-target
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-client-vpn-not-authorize-all
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-multiple-eni-check
- ec2-instance-no-public-ip
- ec2-instance-profile-attached

- ec2-last-backup-recovery-point-created
- ec2-launch-template-public-ip-disabled
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-meets-restore-time-target
- ec2-no-amazon-key-pair
- ec2-paravirtual-instance-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-security-group-attached-to-eni-periodic
- ec2-stopped-instance
- ec2-token-hop-limit-check
- ec2-transit-gateway-auto-vpc-attach-disabled
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-awsvpc-networking-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-no-environment-secrets
- ecs-task-definition-log-configuration
- ecs-task-definition-memory-hard-limit
- ecs-task-definition-nonroot-user

- ecs-task-definition-pid-mode-check
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-root-directory
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs-meets-restore-time-target
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks-cluster-logging-enabled
- eks-cluster-log-enabled
- eks-cluster-oldest-supported-version
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-auto-minor-version-upgrade-check
- elasticache-rbac-auth-enabled
- elasticache-redis-cluster-automatic-backup-check
- elasticache-repl-grp-auto-failover-enabled
- elasticache-repl-grp-encrypted-at-rest
- elasticache-repl-grp-encrypted-in-transit
- elasticache-repl-grp-redis-auth-enabled
- elasticache-subnet-group-check
- elasticache-supported-engine-version
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch

- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-logs-to-cloudwatch
- elastic-beanstalk-managed-updates-enabled
- elbv2-acm-certificate-required
- elbv2-multiple-az
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-block-public-access
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-lustre-copy-tags-to-backups
- fsx-meets-restore-time-target
- fsx-resources-protected-by-backup-plan
- fsx-windows-audit-log-configured
- global-endpoint-event-replication-enabled
- 已启用 guardduty-eks 保护审计
- 启用 guardduty-eks 保护运行时
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- 已启用 guardduty 恶意软件防护

- guardduty-non-archived-findings
- 启用 guardduty-rds 保护
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam 外部访问分析器已启用
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check

- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- lambda-vpc-multi-az-check
- macie自动敏感数据发现检查
- macie-status-check
- mfa-enabled-for-iam-console-access
- mq-active-deployment-mode
- mq-automatic-minor-version-upgrade-enabled
- mq-auto-minor-version-upgrade-enabled
- mq-cloudwatch-audit-logging-enabled
- 已启用 mq-cloudwatch 审计日志
- mq-no-public-access
- mq-rabbit-deployment-mode
- msk-enhanced-monitoring-enabled
- msk-in-cluster-node-require-tls
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- neptune-cluster-backup-retention-check
- neptune-cluster-cloudwatch-log-export-enabled
- neptune-cluster-copy-tags-to-snapshot-enabled
- neptune-cluster-deletion-protection-enabled
- neptune-cluster-encrypted
- neptune-cluster-iam-database-authentication
- neptune-cluster-multi-az-enabled
- neptune-cluster-snapshot-encrypted
- neptune-cluster-snapshot-public-prohibited
- netfw-deletion-protection-enabled
- netfw-logging-enabled
- netfw-multi-az-enabled

- netfw-policy-default-action-fragment-packets
- netfw-policy-default-action-full-packets
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- nlb-cross-zone-load-balancing-enabled
- no-unrestricted-route-to-igw
- opensearch-access-control-enabled
- opensearch-audit-logging-enabled
- opensearch-data-node-fault-tolerance
- opensearch-encrypted-at-rest
- opensearch-https-required
- opensearch-in-vpc-only
- opensearch-logs-to-cloudwatch
- opensearch-node-to-node-encryption-check
- opensearch 主节点容错能力
- opensearch-update-check
- rds-aurora-mysql-audit-logging-enabled
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-auto-minor-version-upgrade-enable
- rds-cluster-encrypted-at-rest
- rds-db-security-group-not-allowed
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-meets-restore-time-target

- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-audit-logging-enabled
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-default-db-name-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- root-account-hardware-mfa-enabled
- root-account-mfa-enabled
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled

- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-meets-restore-time-target
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-inside-vpc
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-instance-root-access-check
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- security-account-information-provided
- 组织内共享的服务目录

- service-vpc-endpoint-enabled
- sns-encrypted-kms
- sns-topic-message-delivery-notification-enabled
- ssm-document-not-public
- step-functions-state-machine-logging-enabled
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-peering-dns-resolution-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled
- wafv2-rulegroup-logging-enabled
- wafv2-rulegroup-not-empty
- wafv2-webacl-not-empty
- waf-regional-rulegroup-not-empty
- waf-regional-rule-not-empty
- waf-regional-webacl-not-empty

AWS GovCloud（美国东部）区域

AWS GovCloud（美国东部）

- access-keys-rotated
- account-part-of-organizations

- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled
- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志

- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check
- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan

- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted
- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled

- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest
- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip

- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-resources-protected-by-backup-plan
- 已启用 guardduty-eks 保护审计
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- guardduty-non-archived-findings
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check
- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能

- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- 已启用 mq-cloudwatch 审计日志
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty
- no-unrestricted-route-to-igw
- opensearch 主节点容错能力
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support

- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only
- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited

- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check
- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan

- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

AWS GovCloud（美国西部）区域

AWS GovCloud（美国西部）

- access-keys-rotated
- account-part-of-organizations
- acm-certificate-expiration-check
- alb-desync-mode-check
- alb-http-drop-invalid-header-enabled
- alb-http-to-https-redirection-check
- alb-waf-enabled
- api-gw-associated-with-waf
- api-gw-cache-enabled-and-encrypted
- api-gw-endpoint-type-check
- api-gw-execution-logging-enabled
- api-gw-ssl-enabled
- api-gw-xray-enabled
- approved-amis-by-id
- approved-amis-by-tag
- aurora-last-backup-recovery-point-created
- aurora-resources-protected-by-backup-plan
- autoscaling-group-elb-healthcheck-required
- autoscaling-launchconfig-requires-imdsv2
- autoscaling-launch-config-public-ip-disabled

- autoscaling-multiple-instance-types
- backup-plan-min-frequency-and-min-retention-check
- backup-recovery-point-encrypted
- backup-recovery-point-manual-deletion-disabled
- backup-recovery-point-minimum-retention-check
- beanstalk-enhanced-health-reporting-enabled
- clb-desync-mode-check
- cloudformation-stack-drift-detection-check
- cloudformation-stack-notification-check
- cloudtrail-all-read-s3 数据事件检查
- cloudtrail-all-write-s3 数据事件检查
- cloudtrail-s3 存储桶访问日志
- cloudtrail-s3 bucket-bucket-禁止公共访问
- cloudtrail-s3-dataevents-enabled
- cloudtrail-security-trail-enabled
- cloudwatch-alarm-action-check
- cloudwatch-alarm-resource-check
- cloudwatch-alarm-settings-check
- cloudwatch-log-group-encrypted
- cloud-trail-cloud-watch-logs-enabled
- cloud-trail-enabled
- cloud-trail-encryption-enabled
- cloud-trail-log-file-validation-enabled
- cmk-backing-key-rotation-enabled
- codebuild-project-environment-privileged-check
- codebuild-project-envvar-awscred-check
- codebuild-project-logging-enabled
- codebuild-project-s3-logs-encrypted
- codebuild-project-source-repo-url-check
- cw-loggroup-retention-period-check

- db-instance-backup-enabled
- desired-instance-tenancy
- desired-instance-type
- 已启用 dms-mongo-db 身份验证
- 已启用 dms-neptune-iam 授权
- 启用 dms-redis-tls
- dms-replication-not-public
- dynamodb-autoscaling-enabled
- dynamodb-in-backup-plan
- dynamodb-last-backup-recovery-point-created
- dynamodb-pitr-enabled
- dynamodb-resources-protected-by-backup-plan
- dynamodb-table-deletion-protection-enabled
- dynamodb-table-encrypted-kms
- dynamodb-table-encryption-enabled
- dynamodb-throughput-limit-check
- ebs-in-backup-plan
- ebs-last-backup-recovery-point-created
- ebs-optimized-instance
- ebs-resources-protected-by-backup-plan
- ebs-snapshot-public-restorable-check
- ec2-client-vpn-connection-log-enabled
- ec2-ebs-encryption-by-default
- ec2-imdsv2-check
- ec2-instance-detailed-monitoring-enabled
- ec2-instance-managed-by-ssm
- ec2-instance-no-public-ip
- ec2-instance-profile-attached
- ec2-last-backup-recovery-point-created
- ec2-managedinstance-applications-blacklisted

- ec2-managedinstance-applications-required
- ec2-managedinstance-association-compliance-status-check
- ec2-managedinstance-inventory-blacklisted
- ec2-managedinstance-patch-compliance-status-check
- ec2-managedinstance-platform-check
- ec2-resources-protected-by-backup-plan
- ec2-security-group-attached-to-eni
- ec2-stopped-instance
- ec2-volume-inuse-check
- ecr-private-image-scanning-enabled
- ecr-private-lifecycle-policy-configured
- ecr-private-tag-immutability-enabled
- ecs-containers-nonprivileged
- ecs-containers-readonly-access
- ecs-container-insights-enabled
- ecs-fargate-latest-platform-version
- ecs-task-definition-user-for-host-mode-check
- efs-access-point-enforce-user-identity
- efs-encrypted-check
- efs-in-backup-plan
- efs-last-backup-recovery-point-created
- efs挂载目标可公开访问
- efs-resources-protected-by-backup-plan
- eip-attached
- eks集群密钥已加密
- eks-cluster-supported-version
- eks-endpoint-no-public-access
- eks-secrets-encrypted
- elasticache-redis-cluster-automatic-backup-check
- elasticsearch-encrypted-at-rest

- elasticsearch-in-vpc-only
- elasticsearch-logs-to-cloudwatch
- elasticsearch-node-to-node-encryption-check
- elastic-beanstalk-managed-updates-enabled
- elb-acm-certificate-required
- elb-cross-zone-load-balancing-enabled
- elb-custom-security-policy-ssl-check
- elb-deletion-protection-enabled
- elb-logging-enabled
- elb-predefined-security-policy-ssl-check
- elb-tls-https-listeners-only
- emr-kerberos-enabled
- emr-master-no-public-ip
- encrypted-volumes
- fms-shield-resource-policy-check
- fms-webacl-resource-policy-check
- fms-webacl-rulegroup-association-check
- fsx-last-backup-recovery-point-created
- fsx-resources-protected-by-backup-plan
- 已启用 guardduty-eks 保护审计
- guardduty-enabled-centralized
- 启用 guardduty-lambda 保护
- guardduty-non-archived-findings
- 已启用 guardduty-s3 保护
- iam-customer-policy-blocked-kms-actions
- iam-group-has-users-check
- iam-inline-policy-blocked-kms-actions
- iam-no-inline-policy-check
- iam-password-policy
- iam-policy-blacklisted-check

- iam-policy-in-use
- iam-policy-no-statements-with-admin-access
- iam-policy-no-statements-with-full-access
- iam-role-managed-policy-check
- iam-root-access-key-check
- iam 服务器证书到期检查
- iam-user-group-membership-check
- iam-user-mfa-enabled
- iam-user-no-policies-check
- iam-user-unused-credentials-check
- incoming-ssh-disabled
- 已启用 inspector-ec2-scan
- 支持 inspector-ecr-scan
- 已启用 inspector-lambda 标准扫描功能
- instances-in-vpc
- internet-gateway-authorized-vpc-only
- kinesis-firehose-delivery-stream 加密
- kinesis-stream-encrypted
- kms-cmk-not-scheduled-for-deletion
- lambda-concurrency-check
- lambda-dlq-check
- lambda-function-public-access-prohibited
- lambda-function-settings-check
- lambda-inside-vpc
- mfa-enabled-for-iam-console-access
- 已启用 mq-cloudwatch 审计日志
- multi-region-cloud-trail-enabled
- nacl-no-unrestricted-ssh-rdp
- netfw-policy-rule-group-associated
- netfw-stateless-rule-group-not-empty

- no-unrestricted-route-to-igw
- opensearch 主节点容错能力
- opensearch-update-check
- rds-automatic-minor-version-upgrade-enabled
- rds-cluster-deletion-protection-enabled
- rds-enhanced-monitoring-enabled
- rds-instance-default-admin-check
- rds-instance-deletion-protection-enabled
- rds-instance-iam-authentication-enabled
- rds-instance-public-access-check
- rds-in-backup-plan
- rds-last-backup-recovery-point-created
- rds-logging-enabled
- rds-multi-az-support
- rds-resources-protected-by-backup-plan
- rds-snapshots-public-prohibited
- rds-snapshot-encrypted
- rds-storage-encrypted
- redshift-backup-enabled
- redshift-cluster-configuration-check
- redshift-cluster-kms-enabled
- redshift-cluster-maintenancesettings-check
- redshift-cluster-public-access-check
- redshift-default-admin-check
- redshift-enhanced-vpc-routing-enabled
- redshift-require-tls-ssl
- redshift-不受限制的端口访问权限
- required-tags
- restricted-incoming-traffic
- s3-access-point-in-vpc-only

- s3-access-point-public-access-blocks
- s3-account-level-public-access-blocks
- s3-account-level-public-access-blocks-periodic
- s3-bucket-acl-prohibited
- s3-bucket-blacklisted-actions-prohibited
- 已启用 s3 存储桶跨区域复制
- s3-bucket-default-lock-enabled
- s3-bucket-level-public-access-prohibited
- s3-bucket-logging-enabled
- s3-bucket-mfa-delete-enabled
- s3-bucket-policy-grantee-check
- s3-bucket-policy-not-more-permissive
- s3-bucket-public-read-prohibited
- s3-bucket-public-write-prohibited
- s3-bucket-replication-enabled
- s3-bucket-server-side-encryption-enabled
- s3-bucket-ssl-requests-only
- s3-bucket-versioning-enabled
- s3-default-encryption-kms
- s3-event-notifications-enabled
- s3-last-backup-recovery-point-created
- s3-lifecycle-policy-check
- s3-resources-protected-by-backup-plan
- s3-version-lifecycle-policy-check
- sagemaker-endpoint-configuration-kms-key-configured
- sagemaker 端点配置产品实例计数
- sagemaker-notebook-instance-kms-key-configured
- sagemaker-notebook-no-direct-internet-access
- secretsmanager-rotation-enabled-check
- secretsmanager-scheduled-rotation-success-check

- secretsmanager-secret-periodic-rotation
- secretsmanager-secret-unused
- secretsmanager-using-cmk
- securityhub-enabled
- 组织内共享的服务目录
- service-vpc-endpoint-enabled
- sns-encrypted-kms
- ssm-document-not-public
- storagegateway-last-backup-recovery-point-created
- storagegateway-resources-protected-by-backup-plan
- subnet-auto-assign-public-ip-disabled
- 传输家庭服务器没有 FTP
- virtualmachine-last-backup-recovery-point-created
- virtualmachine-resources-protected-by-backup-plan
- vpc-default-security-group-closed
- vpc-flow-logs-enabled
- vpc-network-acl-unused-check
- vpc-sg-open-only-to-authorized-ports
- vpc-sg-port 限制检查
- vpc-vpn-2-tunnels-up
- wafv2-logging-enabled

服务相关规则 AWS Config

服务相关 AWS Config 规则是一种独特的 AWS Config 托管规则，它支持其他 AWS 服务在您的账户中创建 AWS Config 规则。服务相关规则经过预定义，包括代表您调用其他 AWS 服务所需的所有权限。这些规则与 AWS 服务在您的合规性验证中推荐 AWS 账户 的标准类似。

这些与服务相关的 AWS Config 规则归 AWS 服务团队所有。 AWS 服务团队会在您的中创建这些规则 AWS 账户。您具有对这些规则的只读访问权限。如果您订阅了与这些规则关联的 AWS 服务，则无法编辑或删除这些规则。

与服务相关的规则和 AWS Command Line Interface

使用时 AWS CLI，PutConfig规则、DeleteConfig规则和DeleteEvaluation结果 API 返回访问被拒绝，并显示以下错误消息：

```
INSUFFICIENT_SLCR_PERMISSIONS = "An AWS service owns
ServiceLinkedConfigRule. You do not have permissions to take action on this
rule."
```

服务相关规则和控制台 AWS Config

在 AWS Config 控制台中，服务相关 AWS Config 规则显示在 “规则” 页面中。控制台中的编辑和删除结果按钮显示为灰色，以限制您编辑规则。您可以通过选择规则来查看规则的详细信息。

与服务相关的规则、补救措施和一致性包

要向一致性包中的服务相关规则添加补救操作，您需要将修正操作添加到一致性包模板本身，然后使用更新的模板更新一致性包。有关更新一致性包的信息，请参阅部署一致性包（控制台）、部署一致性包（AWS CLI）和管理组织一致性包。

编辑和删除服务相关规则

要编辑或删除服务相关规则，请联系创建该规则的 AWS 服务。例如，对于由创建的服务相关规则 AWS Security Hub，您可以按照《AWS Security Hub 用户指南：禁用安全标准》中的以下步骤删除服务相关规则。

使用 AWS CloudFormation 模板创建 AWS Config 托管规则

> **Important**
>
> 必须先创建并启动 AWS Config 配置记录器，才能使用 AWS CloudFormation 创建 AWS Config 托管规则。有关更多信息，请参阅管理配置记录器。

对于支持的 AWS Config 托管规则，您可以使用 AWS CloudFormation 模板为账户创建规则或更新现有 AWS CloudFormation 堆栈。堆栈是您作为单个单元配置和更新的相关资源的集合。在使用模板启动堆栈时，将为您创建 AWS Config 托管规则。模板仅创建规则，而不创建其他 AWS 资源。

> **Note**
>
> 在更新 AWS Config 托管规则时，将针对最新更改来更新模板。要为规则保存特定版本的模板，请下载该模板并将其上传到您的 S3 存储桶。

有关使用 AWS CloudFormation 模板的更多信息，请参阅《AWS CloudFormation 用户指南》中的 AWS CloudFormation 入门。

为 AWS Config 托管规则启动 AWS CloudFormation 堆栈

1. 转至 CloudFormation 控制台并创建新堆栈。
2. 对于 Specify template (指定模板)：
   - 如果您已下载模板，请选择 Upload a template file (上传模板文件)，然后选择 Choose file (选择文件) 以上传模板。
   - 您也可以选择 Amazon S3 URL，然后输入模板 URL `http://s3.amazonaws.com/aws-configservice-us-east-1/cloudformation-templates-for-managed-rules/THE_RULE_IDENTIFIER.template`。

   > **Note**
   > 规则标识符应写在 ALL_CAPS_WITH_UNDERSCORES 中。例如，应为 CLOUDWATCH_LOG_GROUP_ENCRYPTED 而不是 cloudwatch-log-group-encrypted。对于某些规则，规则标识符与规则名称不同。确保使用规则标识符。例如，restricted-ssh 的规则标识符为 INCOMING_SSH_DISABLED。

3. 选择 Next（下一步）。
4. 对于 Specify stack details (指定堆栈详细信息)，键入堆栈名并输入 AWS Config 规则的参数值。例如，如果您使用的是 `DESIRED_INSTANCE_TYPE` 托管规则模板，则可以指定实例类型，例如“m4.large”。
5. 选择 Next（下一步）。
6. 对于 Options，您可以创建标签或配置其他高级选项。这些操作不是必需的。
7. 选择 Next（下一步）。
8. 对于 Review，验证模板、参数和其他选项是否正确。
9. 选择 Create（创建）。将在几分钟内创建堆栈。您可以在 AWS Config 控制台中查看创建的规则。

您可以使用模板为 AWS Config 托管规则创建单个堆栈或更新您的账户中的现有堆栈。如果您删除堆栈，也将删除从该堆栈创建的托管规则。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的使用堆栈。

AWS Config 自定义规则

AWS Config 自定义规则是您从头开始创建的规则。有两种方法可以创建 AWS Config 自定义规则：使用 Lambda 函数（AWS Lambda 开发者指南）和使用 Guard（Guard GitHub存储库）（一种 policy-as-code 语言）。

AWS Config 使用 Lambda 创建的自定义规则称为自定义 AWS Config Lambda 规则，使用 Guard 创建的 AWS Config 自定义规则称为AWS Config 自定义策略规则。

AWS Config 自定义策略规则

使用 Guard 编写的规则可以从 AWS Config 控制台创建，也可以使用 AWS Config 规则 API 创建。AWS Config 自定义策略规则允许您创建 AWS Config 自定义规则，而无需使用 Java 或 Python 开发 Lambda 函数来管理您的自定义规则。 AWS Config 自定义策略规则由配置更改启动。有关 Guard 的更多信息，请参阅 Guard GitHub 存储库。

AWS Config 自定义 Lambda 规则

自定义 Lambda 规则为您提供了使用 Java 或 Python 为自定义规则创建 Lambda 函数的选项。 AWS Config Lambda 函数是您上传到的自定义代码 AWS Lambda，由事件源向其发布的事件调用该函数。如果 Lambda 函数与规则关联， AWS Config 则在规则启动时 AWS Config 调用该函数。然后，Lambda 函数评估发送的配置信息 AWS Config，并返回评估结果。有关 Lambda 函数的更多信息，请参阅《AWS Lambda 开发人员指南》中的函数和事件源。

与成本相关的注意事项

有关资源记录相关费用的详细信息，请参阅AWS Config 定价。

建议：添加逻辑以处理自定义 lambda 规则对已删除资源的评估

在创建 AWS Config 自定义 lambda 规则时，强烈建议您添加逻辑来处理已删除资源的评估。

当评估结果被标记为 `NOT_APPLICABLE` 时，这些资源将被标记为已删除并被清理。如果资源未被标记为 `NOT_APPLICABLE`，则在删除规则之前，评估结果将保持不变，这可能会导致删除规则后创建 `AWS::Config::ResourceCompliance` 配置项目 (CI) 出现意外激增。

有关如何设置 AWS Config 自定义 lambda 规则以返回`NOT_APPLICABLE`已删除资源的信息，请参阅使用 AWS Config 自定义 lambda 规则管理已删除的资源。

建议：为自定义 lambda 规则提供范围内的资源

AWS Config 如果自定义 Lambda 规则的范围不限于一种或多种资源类型，则该规则可能会导致大量的 Lambda 函数调用。为避免与您的账户相关的活动增加，强烈建议您在自定义 Lambda 规则的范围内提供资源。如果未选择任何资源类型，该规则将为账户中的所有资源调用 Lambda 函数。

建议：在删除规则之前停止记录资源合规性

强烈建议您在删除账户中的规则之前，停止记录该`AWS::Config::ResourceCompliance`资源类型。删除规则会为配置记录器创建 CI，`AWS::Config::ResourceCompliance`并可能影响您的 AWS Config 配置记录器成本。如果您要删除评估大量资源类型的规则，则可能会导致记录的 CI 数量激增。

最佳实践：

1. 停止录制 `AWS::Config::ResourceCompliance`
2. 删除规则
3. 开启录制 `AWS::Config::ResourceCompliance`

触发器类型

向账户添加规则后， AWS Config 将您的资源与规则的条件进行比较。在这次初始评估之后，每次触发评估时都会 AWS Config 继续运行评估。评估触发器被定义为规则的一部分，它们可以包括以下类型。

触发器类型	描述
配置更改	AWS Config 当存在与规则范围匹配的资源并且资源的配置发生变化时，会对规则进行评估。评估将在 AWS Config 发送配置项目变更通知后运行。 通过定义规则的范围来选择哪些资源启动评估。范围可以包括： • 一个或多个资源类型 • 资源类型和资源 ID 的组合 • 标签键和值的组合

触发器类型	描述
	• 当创建、更新或删除任何记录的资源时 AWS Config 当它检测到与规则范围相匹配的资源发生变化时，就会运行评估。您可以使用范围来定义哪些资源启动评估。
定期	AWS Config 按您选择的频率对规则进行评估；例如，每 24 小时运行一次。
混合	有些规则既有配置更改也有定期触发器。对于这些规则，它 AWS Config 会在检测到配置更改时以及按照您指定的频率评估您的资源。

评估模式

AWS Config 规则有两种评估模式。

评估模式	描述
主动	使用主动评估在资源部署之前对其进行评估。这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。 有关更多信息，请参阅评估模式。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。
侦查	使用侦查评估来评估已部署的资源。这允许您评估现有资源的配置设置。

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

使用 AWS Config 自定义 lambda 规则管理已删除的资源

报告已删除资源的规则应返回 NOT_APPLICABLE 的评估结果，以避免不必要的规则评估。

当您删除资源时， AWS Config 会ResourceDeleted为创建一个 configurationItem with configurationItemStatus。您可以使用此元数据检查规则是否报告了已删除的资源。有关配置项的更多信息，请参阅概念 | 配置项。

包括以下代码片段以检查是否有已删除的资源，并将 AWS Config 自定义 lambda 规则的评估结果设置为（NOT_APPLICABLE如果它报告了已删除的资源）：

Custom Lambda Rules (Node.js)

```
// Check whether the resource has been deleted. If the resource was deleted, then
 the evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope
 === false;
}
```

Custom Lambda Rules (Python)

```
# Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope
```

> **Note**
>
> AWS Config 默认情况下，托管规则和 AWS Config 自定义策略规则会处理此行为。如果您使用开发套件 (RDK) 和 AWS Config AWS Config 开发套件库 (rdkLib) 使用 Python 创建 AWS Config 自定义 lambd 规则，则导入的评估器类将检查此行为。有关如何使用 RDK 和 RDKlib 编写规则的信息，请参阅使用 RDK 和 RDKlib 编写规则。

主题

- 创建 AWS Config 自定义策略规则
- 创建 AWS Config 自定义 Lambda 规则

创建 AWS Config 自定义策略规则

您可以通过 AWS Management Console AWS CLI、或 AWS Config API 创建 AWS Config 自定义策略规则。有关如何使用 Guard 编写规则的更多信息，请参阅 Guard 用户指南中的编写 AWS CloudFormation 防护规则。有关 AWS Config 可以评估的受支持资源类型的架构的更多信息，请参阅资源架构存储库中的 AWS Config 资源类型。 GitHub

> **Important**
>
> 用于评估配置项目的 AWS Config 资源架构与用于评估 AWS CloudFormation 模板的 CFN 架构不同。如果将 CFN 架构用于 AWS Config 自定义策略规则，评估结果将返回 `NOT_APPLICABLE`。创建 AWS Config 自定义策略规则时使用 AWS Config 资源架构，并根据配置项目结构编写策略。有关 AWS Config 资源架构的列表，请参阅资源架构存储库中的 AWS Config 资源类型。 GitHub

创建 AWS Config 自定义策略规则（控制台）

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的 AWS 区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 在左侧导航窗格中，选择 Rules。

4. 在 Rules 页面，选择 Add rule。
5. 在指定规则类型页面上，选择使用 Guard 创建自定义规则。
6. 在配置规则页面上，通过完成以下步骤创建规则：
   a. 对于规则名称，键入一个唯一的规则名称。
   b. 对于描述，键入规则的描述。
   c. 对于 Guard 运行时版本，请为您的 AWS Config 自定义策略规则选择运行时系统。
   d. 对于规则内容，可以为其填充规则的 Guard 自定义策略。有关 Guard Custom 策略的结构和功能的更多信息，请参阅 AWS CloudFormation Guard 2.0 在 Guard GitHub 存储库中的操作模式。

> **Note**
>
> 用于评估配置项目的 AWS Config 资源架构与用于评估 AWS CloudFormation 模板的 CFN 架构不同。如果将 CFN 架构用于 AWS Config 自定义策略规则，评估结果将返回 NOT_APPLICABLE。创建 AWS Config 自定义策略规则时使用 AWS Config 资源架构，并根据配置项目结构编写策略。有关 AWS Config 资源架构的列表，请参阅资源架构存储库中的 AWS Config 资源类型。 GitHub

以下示例显示了 AWS Config 托管规则的 AWS Config 自定义策略规则版本的策略定义 dynamodb-pitr-enabled

```
# This rule checks if point in time recovery (PITR) is enabled on active Amazon
 DynamoDB tables
let status = ['ACTIVE']

rule tableisactive when
    resourceType == "AWS::DynamoDB::Table" {
    configuration.tableStatus == %status
}

rule checkcompliance when
    resourceType == "AWS::DynamoDB::Table"
    tableisactive {
        let pitr =
 supplementaryConfiguration.ContinuousBackupsDescription.pointInTimeRecoveryDescription
        %pitr == "ENABLED"
}
```

e. 对于评估模式，请选择在资源创建和管理过程中何 AWS Config 时评估您的资源。根据规则，AWS Config 可以在置备资源之前、资源调配之后或两者兼而有之地评估您的资源配置。

   i. 选择开启主动评估，以允许您在部署资源之前对资源的配置设置进行评估。

      开启主动评估后，您可以使用StartResource评估 API 和 GetResourceEvaluationSummaryAPI 来检查您在这些命令中指定的资源是否会被您所在地区的账户中的主动规则标记为 “不合规”。

      有关使用此命令的更多信息，请参阅使用 AWS Config 规则评估您的资源。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。

   ii. 选择开启侦查评估以评估您的现有资源的配置设置。

      对于侦探评估， AWS Config 自定义策略规则由配置更改启动。将预先选择以下选项。

      - 资源 – 在创建、更改或删除与指定资源类型（或类型和标识符）匹配的资源时。
      - 标签 – 在创建、更改或删除包含指定标签的资源时。
      - 所有更改-创建、更改或删除记录的资源时。 AWS Config

      AWS Config 当它检测到与规则范围相匹配的资源发生变化时，就会运行评估。您可以使用范围来限制哪些资源启动评估。否则，当配置后的资源发生变化时，就会启动评估。

f. 对于参数，如果您的规则包含参数，可以自定义所提供的键的值。参数是资源在被视为符合规则之前必须遵守的属性。

7. 在 “查看并创建” 页面上，查看您的所有选择，然后再将规则添加到您的中 AWS 账户。
8. 查看完规则后，选择添加规则。

创建 AWS Config 自定义策略规则 (AWS CLI)

使用 `put-config-rule` 命令。

`Owner` 字段应为 `CUSTOM_POLICY`。 AWS Config 自定义策略规则需要以下附加字段：

- `Runtime`：您的 AWS Config 自定义策略规则的运行时系统。
- `PolicyText`：包含 AWS Config 自定义策略规则逻辑的策略定义。

- `EnableDebugLogDelivery`：用于为 AWS Config 自定义策略规则启用调试日志记录的布尔表达式。默认值为 `false`。

创建 AWS Config 自定义策略规则 (API)

使用 “PutConfig规则” 操作。

`Owner` 字段应为 `CUSTOM_POLICY`。 AWS Config 自定义策略规则需要以下附加字段：

- `Runtime`：您的 AWS Config 自定义策略规则的运行时系统。
- `PolicyText`：定义 AWS Config 自定义策略规则逻辑的策略。
- `EnableDebugLogDelivery`：用于为 AWS Config 自定义策略规则启用调试日志记录的布尔表达式。默认值为 `false`。

创建 AWS Config 自定义 Lambda 规则

您可以开发自定义规则，并使用 AWS Lambda 函数将其添加至 AWS Config。您可以将每个自定义规则与一个 Lambda 函数关联，其中包含用于评估您的 AWS 资源是否符合规则的逻辑。将此函数与您的规则关联后，该规则会定期或因响应配置更改而调用该函数。然后，该函数评估您的资源是否符合您的规则，并将评估结果发送给 AWS Config。

自定义 Lambda 规则（Amazon EC2 示例）中的示例将指导您首次创建自定义 Lambda 规则，该规则用于评估您的每个 EC2 实例是否都是 t2.micro 类型。其中包括不加修改就可以添加至 AWS Lambda 的示例 Lambda 函数。自定义 Lambda 规则（一般示例）中的示例提供了创建自定义 Lambda 规则的更通用示例。

要了解 AWS Lambda 函数的工作原理以及如何编写这些函数，请参阅《AWS Lambda 开发人员指南》。

主题

- 自定义 Lambda 规则（Amazon EC2 示例）
- 自定义 Lambda 规则（一般示例）
- 针对 AWS Config 规则的 AWS Lambda 函数和事件示例

自定义 Lambda 规则（Amazon EC2 示例）

此过程将指导您完成创建自定义 Lambda 规则的过程，该规则用于评估您的每个 EC2 实例是否都是 t2.micro 类型。 AWS Config 将对此规则运行基于事件的评估，这意味着每次 AWS Config 检测到实例中的配置更改时，它都会检查您的实例配置。 AWS Config 会将 t2.micro 实例标记为合规，将所有其他实例标记为不合规。合规性状态将显示在 AWS Config 控制台中。

为了使此过程获得最佳结果，您应该在中拥有一个或多个 EC2 实例 AWS 账户。您的实例中应包含至少一个 t2.micro 实例和其他类型的实例。

要创建此规则，首先，您需要通过在 AWS Lambda 控制台中自定义蓝图来创建 AWS Lambda 函数。然后，您将在中创建自定义 Lambda 规则 AWS Config，并将该规则与该函数关联。

主题

- 为自定义 Config 规则创建 AWS Lambda 函数
- 创建用于评估 Amazon EC2 实例的自定义 Lambda 规则

为自定义 Config 规则创建 AWS Lambda 函数

1. 登录 AWS Management Console 并打开 AWS Lambda 控制台，网址为 https://console.aws.amazon.com/lambda/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 在 AWS Lambda 控制台中，选择创建 Lambda 函数。
4. 选择使用蓝图。在搜索栏中，键入 config-rule-change-triggered。选择筛选结果中的蓝图，然后选择配置。
5. 在 Configure triggers 页面上，选择 Next。
6. 在基本信息页面上，完成以下步骤：
   a. 对于函数名称，请键入 **`InstanceTypeCheck`**。
   b. 对于执行角色，选择从 AWS 策略模板创建新角色。
   c. 对于 Runtime，请保留 Node.js。
   d. 对于角色名称，键入名称。
   e. 对于策略模板，选择 AWS Config 规则权限。

f. 对于 Lambda 函数代码函数，保留预配置的代码。代码编辑器中带有用于您的函数的 Node.js 代码。在本程序中，您无需更改代码。

g. 验证详细信息，然后选择创建函数。 AWS Lambda 控制台显示您的函数。

7. 要验证您的函数是否设置正确，请通过以下步骤进行测试：

   a. 从函数概述下方的菜单中选择测试，然后选择配置测试事件。

   b. 对于模板，选择 AWS Config 配置项更改通知。

   c. 对于名称，键入名称。

   d. 选择 “测试”。 AWS Lambda 使用示例事件测试您的函数。如果您的函数按预期运行，Execution result 下会出现与下面类似的错误消息：

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

   之所以`InvalidResultTokenException`是预料之中的，是因为您的函数只有在收到来自的结果令牌时才能成功运行 AWS Config。结果令牌可以识别 AWS Config 规则和引起评估的事件，并将评估与规则相关联。这一异常表示您的函数具备将结果发送至 AWS Config所需的权限。否则，将出现这种错误消息：`not authorized to perform: config:PutEvaluations`。如果发生这一错误，请更新您分配给函数的角色以便支持 `config:PutEvaluations` 操作，然后再次测试您的函数。

创建用于评估 Amazon EC2 实例的自定义 Lambda 规则

1. 打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为与您为自定义 Lambda 规则创建 AWS Lambda 函数的区域相同。
3. 在 Rules 页面，选择 Add rule。
4. 在指定规则类型页面上，选择创建自定义规则。
5. 在 Configure rule 页面，完成以下步骤：

   a. 对于名称，键入 **`InstanceTypesAreT2micro`**。

   b. 对于描述，键入 **`Evaluates whether EC2 instances are the t2.micro type`**。

   c. 对于 AWS Lambda 函数 ARN，指定 AWS Lambda 分配给您的函数的 ARN。

> **Note**
>
> 您在此步骤中指定的 ARN 不能包含 `$LATEST` 限定词。您可以指定不带版本限定符的 ARN，也可以使用其他任何限定符指定。`$LATEST` AWS Lambda 支持函数版本控制，并且每个版本都分配了一个带有限定符的 ARN。 AWS Lambda 使用最新版本的`$LATEST`限定符。

d. 对于触发器类型，选择在配置发生更改时。

e. 对于 Scope of changes，请选择 Resources。

f. 对于资源，从资源类型下拉列表中选择 AWS EC2 实例。

g. 在参数部分，您必须指定 AWS Lambda 函数评估的规则参数和所需的值。本程序中的函数会评估 `desiredInstanceType` 参数。

   对于 Key (键)，键入 **`desiredInstanceType`**。对于 Value，键入 **`t2.micro`**。

6. 选择下一步。在审核并创建页面上，验证您的规则的详细信息，然后选择添加规则函数。您的新规则将显示在 Rules 页面中。

   合规性将显示正在评估... 直到 AWS Config 收到您的 AWS Lambda 职能的评估结果。如果规则和函数按预期运行，关于结果的汇总将在几分钟后显示。例如，2 noncompliant resource(s) 结果表示您的实例中有两个不是 t2.micro 实例，Compliant 结果表示所有实例均为 t2.micro 实例。您可以使用刷新按钮更新结果。

   如果规则或函数没有按预期运行，您可能会在 Compliance 中看到以下一项内容：

   - 未报告任何结果- AWS Config 根据规则评估了您的资源。规则不适用于其范围内的 AWS 资源，指定的资源已删除，或者评估规则已删除。要获取评估结果，请更新规则、更改其范围或者选择 Re-evaluate。

     验证范围是否包括资源的 AWS EC2 实例，然后重试。

   - 范围内没有资源- AWS Config 无法根据此规则评估您记录的 AWS 资源，因为您的所有资源都不在该规则的范围内。要获得评估结果，请编辑规则并更改其范围，或者使用 “设置” 页面添加 AWS Config 要记录的资源。

     验证 AWS Config 是否在记录 EC2 实例。

   - Evaluations failed (评估失败) - 有关可帮助您确定问题的信息，请选择规则名称以打开其详细信息页面并查看错误消息。

如果您的规则正常运行并 AWS Config 提供了评估结果，则可以了解哪些条件会影响规则的合规状态。您可以了解哪些资源不合规 (如果有) 及其原因。有关更多信息，请参阅 查看合规信息和评估结果。

自定义 Lambda 规则（一般示例）

完成以下过程以创建自定义 Lambda 规则。要创建自定义 Lambda 规则，您需要先创建一个 AWS Lambda 函数，其中包含该规则的评估逻辑。然后，将该函数与您在 AWS Config中创建的自定义 Lambda 规则关联。

> **Important**
>
> 作为允许调用您的 Lambda 函数的 AWS Config 权限的最佳安全实践，我们强烈建议您在调用请求中限制对基于资源的 Lambda 策略的访问`sourceARN`。`sourceAccountId`有关更多信息，请参阅 基于 AWS Lambda 资源的策略的安全最佳实践。

目录

- 为自定义 Config 规则创建 AWS Lambda 函数
- 在中创建自定义规则 AWS Config
- 基于 AWS Lambda 资源的策略的安全最佳实践
- 评估其他资源类型

为自定义 Config 规则创建 AWS Lambda 函数

Lambda 函数是您上传到的自定义代码 AWS Lambda，由事件源向其发布的事件调用该函数。如果 Lambda 函数与 Config 规则关联，则在规则触发时 AWS Config 调用该函数。之后，Lambda 函数会评估由 AWS Config发送的配置信息并返回评估结果。有关 Lambda 函数的更多信息，请参阅《AWS Lambda 开发人员指南》中的函数和事件源。

您可以使用支持的编程语言为自定义 Lambda 规则创建 Lambda 函数。 AWS Lambda 为了简化此任务，您可以自定义 AWS Lambda 蓝图或重复使用 AWS Config 规则 GitHub存储库中的示例函数。

AWS Lambda 蓝图

AWS Lambda 控制台提供示例函数或蓝图，您可以通过添加自己的评估逻辑对其进行自定义。当您创建函数时，您可以选择以下蓝图之一：

- config-rule-change-triggered— 当您的 AWS 资源配置发生变化时触发。

- config-rule-periodic— 按您选择的频率触发（例如，每 24 小时一次）。

AWS Config 规则 GitHub 存储库

自定义 Lambda 规则示例函数的公共存储库位于基于 Web 的代码托管和共享服务上 GitHub。示例函数是由 AWS 社区开发和贡献的。如果要使用示例，可以将其代码复制到新 AWS Lambda 函数中。要查看存储库，请访问 https://github.com/awslabs/aws-config-rules/。

为您的自定义规则创建函数

1. 登录 AWS Management Console 并打开 AWS Lambda 控制台，网址为 https://console.aws.amazon.com/lambda/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 选择 Create a Lambda function (创建 Lambda 函数)。
4. 在 “使用蓝图” 页面上，您可以选择 AWS Config 规则的蓝图函数之一作为起点，也可以通过选择 “跳过” 在没有蓝图的情况下继续操作。
5. 在 Configure triggers 页面上，选择 Next。
6. 在基本信息页面上，键入名称和描述。
7. 对于 Runtime，请选择您编写函数时使用的编程语言。
8. 对于 Code entry type，请选择您偏好的条目类型。如果使用蓝图，请保留预先配置的代码。
9. 用您选择的代码条目类型要求的方法提供您的代码。如果您正在使用蓝图，那么函数代码由代码编辑器提供，且您可以自定义代码，以使其包含您自己的评估逻辑。您的代码可以评估在调用您的函数时 AWS Config 提供的事件数据：
   - 对于基于config-rule-change-triggered蓝图的函数，或者对于由配置更改触发的函数，事件数据是已更改 AWS 资源的配置项目或超大配置项目对象。
   - 对于基于config-rule-periodic蓝图的函数，或者对于以您选择的频率触发的函数，事件数据是一个 JSON 对象，其中包含有关何时触发评估的信息。
   - 对于这两种类型的函数，都以 JSON 格式 AWS Config 传递规则参数。您在 AWS Config中创建自定义 Lambda 规则时，可以定义传递哪些规则参数。
   - 有关在调用您的函数时 AWS Config 发布的事件示例，请参阅。AWS Config 规则的示例事件
10. 对于执行角色，选择从 AWS 策略模板创建新角色。
11. 对于 Role name，请输入名称。

12. 对于策略模板，选择 AWS Config 规则权限。
13. 验证详细信息，然后选择创建函数。

在中创建自定义规则 AWS Config

AWS Config 用于创建自定义 Lambda 规则并将该规则与 Lambda 函数关联。

创建自定义规则

1. 打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为与您为自定义 Lambda 规则创建 AWS Lambda 函数的区域相同。
3. 在 Rules 页面，选择 Add rule。
4. 在指定规则类型页面上，选择创建自定义规则。
5. 在 Configure rule 页面，键入一个名称和描述。
6. 对于 AWS Lambda 函数 ARN，指定 AWS Lambda 分配给您的函数的 ARN。

> **Note**
>
> 您在此步骤中指定的 ARN 不能包含 `$LATEST` 限定词。您可以指定不带版本限定符的 ARN，也可以使用其他任何限定符来指定 ARN。`$LATEST` AWS Lambda 支持函数版本控制，并且每个版本都分配了一个带有限定符的 ARN。 AWS Lambda 使用最新版本的`$LATEST`限定符。

7. 对于 Trigger type，请选择下列一个或两个选项：
   - 配置更改-在检测到配置更改时 AWS Config 调用您的 Lambda 函数。
   - 定期 — 按您选择的频率 AWS Config 调用 Lambda 函数（例如，每 24 小时一次）。
8. 如果您的规则的触发器类型包括配置更改，请为 AWS Config 调用您的 Lambda 函数的更改范围指定以下选项之一：
   - 所有更改-创建、更改或删除记录的任何资源时。 AWS Config
   - 资源 – 在创建、更改或删除任何与指定类型（或类型和标识符）匹配的资源时。
   - 标签 – 在创建、更改或删除任何包含指定标签的资源时。
9. 如果您的规则的触发器类型包括定期，请指定 AWS Config 调用 Lambda 函数的频率。
10. 在参数部分中，指定您的 AWS Lambda 函数评估的所有规则参数和所需的值。

11. 选择下一步。在审核并创建页面上，验证您的规则的详细信息，然后选择添加规则函数。您的新规则将显示在规则页面中。

    合规性将显示正在评估... 直到 AWS Config 收到您的 AWS Lambda 职能的评估结果。如果规则和函数按预期运行，结果汇总将在几分钟后显示。您可以使用刷新按钮更新结果。

    如果规则或函数没有按预期运行，您可能会在 Compliance 中看到以下一项内容：

    - 未报告任何结果- AWS Config 根据规则评估了您的资源。规则不适用于其范围内的 AWS 资源，指定的资源已删除，或者评估规则已删除。要获取评估结果，请更新规则、更改其范围或者选择 Re-evaluate。

      如果规则不报告评估结果，该消息可能也会出现。
    - 范围内没有资源- AWS Config 无法根据此规则评估您记录的 AWS 资源，因为您的所有资源都不在该规则的范围内。您可以在设置页面上选择 AWS Config 记录哪些资源。
    - Evaluations failed (评估失败) - 有关可帮助您确定问题的信息，请选择规则名称以打开其详细信息页面并查看错误消息。

> **Note**
>
> 当您使用 AWS Config 控制台创建自定义 Lambda 规则时，系统会自动为您创建相应的权限。如果您使用创建自定义 Lambda 规则 AWS CLI，则需要授予使用命令调用 Lambda 函数的 AWS Config 权限。`aws lambda add-permission`有关更多信息，请参阅开发人员指南中的使用基于资源的策略 AWS Lambda （Lambda 函数策略）AWS Lambda 。
> 在 AWS Config 授予调用 Lambda 函数的权限之前，请参阅以下部分。基于 AWS Lambda 资源的策略的安全最佳实践

基于 AWS Lambda 资源的策略的安全最佳实践

作为安全性最佳实践，为了避免为整个服务主体名称 (SPN) 授予调用 Lambda 函数的调用权限，我们强烈建议您在基于 Lambda 资源的策略中使用调用请求中的 `sourceARN` 和/或 `sourceAccountId` 限制访问权限。

`sourceARN`是调用 Lambda 函数的 AWS Config 规则的 ARN。

`sourceAccountId` 是创建规则的用户的账户 ID。

在 Lambda 基于资源的策略中限制访问有助于确保 AWS Lambda 仅代表预期的用户和场景访问您的资源。

要添加基于 SPN 的权限，您需要使用以下 CLI

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com
```

添加 SourceAccountId 基于权限的权限

在创建规则之前，可以使用以下 CLI 向基于资源的策略添加基于 `sourceAccountId` 的权限

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID
```

同时添加 SourceAccountId 基于 SourceArn 和的权限

在创建规则之后，可以使用以下 CLI 向基于资源的策略添加基于 `sourceARN` 的权限。这仅允许特定规则 ARN 调用 Lambda 函数。

```
aws lambda add-permission --function-name rule lambda function name --action
 lambda:InvokeFunction --statement-id config --principal config.amazonaws.com --source-
account your account ID --source-arn ARN of the created config rule
```

评估其他资源类型

您可以创建自定义 Lambda 规则，对尚未记录的资源类型进行评估。 AWS Config如果您想评估当前 AWS Config 未记录的其他资源类型的合规性，这将非常有用。有关您可以使用自定义 Lambda 规则评估的其他资源类型的列表，请参阅《AWS 资源类型参考》。

> **Note**
>
> 为未记录的资源类型创建自定义 Lambda 时 AWS Config，该规则必须具有定期触发类型。不支持配置更改触发器类型。有关更多信息，请参阅 AWS Config 规则的评估模式和触发器类型。

示例

1. 您想评估自己账户中的 Amazon S3 Glacier 文件库。 AWS Config目前未记录 Amazon S3 Glacier 文件库资源。
2. 您可以创建一个 AWS Lambda 函数来评估您的 Amazon S3 Glacier 文件库是否符合您的账户要求。
3. 您创建名为的自定义 Lambda 规则 evaluate-glacier-vaults，然后将您的 AWS Lambda 函数分配给该规则。
4. AWS Config 调用你的 Lambda 函数，然后根据你的规则评估 Amazon S3 Glacier 文件库。
5. AWS Config 返回评估结果，您可以查看规则的合规性结果。

> **Note**
>
> 您可以在 AWS Config 时间轴中查看配置详细信息，也可以在 AWS Config 控制台中查找资源以获取 AWS Config 支持的资源。如果您配置 AWS Config 为记录所有资源类型，则将自动记录新支持的资源。有关更多信息，请参阅 支持的资源类型。

针对 AWS Config 规则的 AWS Lambda 函数和事件示例

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

有关 AWS Lambda 中的函数和事件的更多信息，请参阅《AWS Lambda 开发人员指南》中的函数和事件源。

主题

- AWS Config 规则的示例 AWS Lambda 函数 (Node.js)
- 用于 AWS Config 规则 (Python) 的示例 AWS Lambda 函数
- AWS Config 规则的示例事件

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

AWS Lambda 执行函数以响应 AWS 服务发布的事件。 AWS Config 自定义 Lambda 规则的函数接收由发布的事件 AWS Config，然后该函数使用从该事件中接收的数据以及从 AWS Config API 检索的数据来评估规则的合规性。用于 Config 规则的函数的运作方式会因其执行的评估是由配置更改触发还是定期触发而有所不同。

有关 AWS Lambda 函数中常见模式的信息，请参阅《AWS Lambda 开发人员指南》中的编程模型。

目录

- 评估由配置更改触发时的示例函数
- 定期评估时的示例函数

评估由配置更改触发时的示例函数

AWS Config 当它检测到自定义规则范围内的资源的配置更改时，将调用如下例所示的函数。

如果您使用 AWS Config 控制台创建与函数相关联的规则（例如此示例），请选择配置更改作为触发器类型。如果您使用 AWS Config API 或创建规则， AWS CLI 请将`MessageType`属性设置为`ConfigurationItemChangeNotification`和`OversizedConfigurationItemChangeNotificati`通过这些设置，无论何时由于资源更改而 AWS Config 生成配置项目或超大配置项目，都可触发您的规则。

此示例评估您的资源并检查实例是否匹配资源类型 `AWS::EC2::Instance`。此规则在 AWS Config 生成配置项或过大配置项通知时触发。

```
'use strict';

import { ConfigServiceClient, GetResourceConfigHistoryCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Helper function used to validate input
function checkDefined(reference, referenceName) {
    if (!reference) {
        throw new Error(`Error: ${referenceName} is not defined`);
    }
    return reference;
}
```

```
// Check whether the message type is OversizedConfigurationItemChangeNotification,
function isOverSizedChangeNotification(messageType) {
    checkDefined(messageType, 'messageType');
    return messageType === 'OversizedConfigurationItemChangeNotification';
}

// Get the configurationItem for the resource using the getResourceConfigHistory API.
async function getConfiguration(resourceType, resourceId, configurationCaptureTime,
 callback) {
    const input = { resourceType, resourceId, laterTime: new
 Date(configurationCaptureTime), limit: 1 };
    const command = new GetResourceConfigHistoryCommand(input);
    await configClient.send(command).then(
        (data) => {
            callback(null, data.configurationItems[0]);
        },
        (error) => {
            callback(error, null);
        }
    );

}

// Convert the oversized configuration item from the API model to the original
 invocation model.
function convertApiConfiguration(apiConfiguration) {
    apiConfiguration.awsAccountId = apiConfiguration.accountId;
    apiConfiguration.ARN = apiConfiguration.arn;
    apiConfiguration.configurationStateMd5Hash =
 apiConfiguration.configurationItemMD5Hash;
    apiConfiguration.configurationItemVersion = apiConfiguration.version;
    apiConfiguration.configuration = JSON.parse(apiConfiguration.configuration);
    if ({}.hasOwnProperty.call(apiConfiguration, 'relationships')) {
        for (let i = 0; i < apiConfiguration.relationships.length; i++) {
            apiConfiguration.relationships[i].name =
 apiConfiguration.relationships[i].relationshipName;
        }
    }
    return apiConfiguration;
}

// Based on the message type, get the configuration item either from the
 configurationItem object in the invoking event or with the getResourceConfigHistory
 API in the getConfiguration function.
```

```
async function getConfigurationItem(invokingEvent, callback) {
    checkDefined(invokingEvent, 'invokingEvent');
    if (isOverSizedChangeNotification(invokingEvent.messageType)) {
        const configurationItemSummary =
 checkDefined(invokingEvent.configurationItemSummary, 'configurationItemSummary');
        await getConfiguration(configurationItemSummary.resourceType,
 configurationItemSummary.resourceId,
 configurationItemSummary.configurationItemCaptureTime, (err, apiConfigurationItem) =>
 {
            if (err) {
                callback(err);
            }
            const configurationItem = convertApiConfiguration(apiConfigurationItem);
            callback(null, configurationItem);
        });
    } else {
        checkDefined(invokingEvent.configurationItem, 'configurationItem');
        callback(null, invokingEvent.configurationItem);
    }
}

// Check whether the resource has been deleted. If the resource was deleted, then the
 evaluation returns not applicable.
function isApplicable(configurationItem, event) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(event, 'event');
    const status = configurationItem.configurationItemStatus;
    const eventLeftScope = event.eventLeftScope;
    return (status === 'OK' || status === 'ResourceDiscovered') && eventLeftScope ===
 false;
}

// In this example, the resource is compliant if it is an instance and its type matches
 the type specified as the desired type.
// If the resource is not an instance, then this resource is not applicable.
function evaluateChangeNotificationCompliance(configurationItem, ruleParameters) {
    checkDefined(configurationItem, 'configurationItem');
    checkDefined(configurationItem.configuration, 'configurationItem.configuration');
    checkDefined(ruleParameters, 'ruleParameters');

    if (configurationItem.resourceType !== 'AWS::EC2::Instance') {
        return 'NOT_APPLICABLE';
    } else if (ruleParameters.desiredInstanceType ===
 configurationItem.configuration.instanceType) {
```

```
        return 'COMPLIANT';
    }
    return 'NON_COMPLIANT';
}

// Receives the event and context from AWS Lambda.
export const handler = async (event, context) => {
    checkDefined(event, 'event');
    const invokingEvent = JSON.parse(event.invokingEvent);
    const ruleParameters = JSON.parse(event.ruleParameters);
    await getConfigurationItem(invokingEvent, async (err, configurationItem) => {

        let compliance = 'NOT_APPLICABLE';
        let annotation = '';
        const putEvaluationsRequest = {};
        if (isApplicable(configurationItem, event)) {
            // Invoke the compliance checking function.
            compliance = evaluateChangeNotificationCompliance(configurationItem,
 ruleParameters);
            if (compliance === "NON_COMPLIANT") {
                annotation = "This is an annotation describing why the resource is not
 compliant.";
            }
        }
        // Initializes the request that contains the evaluation results.
        if (annotation) {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
                    Annotation: annotation
                },
            ];
        } else {
            putEvaluationsRequest.Evaluations = [
                {
                    ComplianceResourceType: configurationItem.resourceType,
                    ComplianceResourceId: configurationItem.resourceId,
                    ComplianceType: compliance,
                    OrderingTimestamp: new
 Date(configurationItem.configurationItemCaptureTime),
```

```
                },
            ];
        }
        putEvaluationsRequest.ResultToken = event.resultToken;

        // Sends the evaluation results to AWS Config.
        await configClient.send(new PutEvaluationsCommand(putEvaluationsRequest));
    });
};
```

函数运作

本函数在运行时执行以下操作：

1. 该函数在将event对象 AWS Lambda 传递给handler函数时运行。在此示例中，该函数接受可选callback参数，该参数用于向调用者返回信息。 AWS Lambda 还传递一个context对象，其中包含函数在运行时可以使用的信息和方法。请注意，在新版本的 Lambda 中，不再使用上下文。
2. 此函数检查事件的 messageType 是配置项还是过大配置项，然后返回配置项。
3. 处理程序调用 isApplicable 函数来确定资源是否已删除。

   > **Note**
   >
   > 报告已删除资源的规则应返回 NOT_APPLICABLE 的评估结果，以避免不必要的规则评估。

4. 处理程序调用该evaluateChangeNotificationCompliance函数并传递在事件中 AWS Config 发布的configurationItem和ruleParameters对象。

   函数首先评估资源是否为 EC2 实例。如果资源不是 EC2 实例，函数会返回 NOT_APPLICABLE 这一合规性值。

   然后，函数评估配置项中的 instanceType 属性是否与 desiredInstanceType 参数值一致。如果值相等，该函数将返回 COMPLIANT。如果值不相等，该函数将返回 NON_COMPLIANT。
5. 处理程序准备 AWS Config 通过初始化putEvaluationsRequest对象将评估结果发送到。该对象包含 Evaluations 参数，这一参数用于识别受评估资源的合规性结果、资源类型和 ID。该putEvaluationsRequest对象还包括事件的结果标记，用于标识规则和事件 AWS Config。
6. AWS Config 通过将对象传递给config客户端putEvaluations的方法，处理程序将评估结果发送到。

定期评估时的示例函数

AWS Config 将调用如下例所示的函数进行定期评估。定期评估按您在 AWS Config中定义规则时指定的频率进行。

如果您使用 AWS Config 控制台创建与函数关联的规则（例如此示例），请选择周期作为触发器类型。如果您使用 AWS Config API 或创建规则， AWS CLI 请将`MessageType`属性设置为`ScheduledNotification`。

本示例会检查指定资源的总数是否超出指定的最大值。

```
'use strict';
import { ConfigServiceClient, ListDiscoveredResourcesCommand, PutEvaluationsCommand }
 from "@aws-sdk/client-config-service";

const configClient = new ConfigServiceClient({});

// Receives the event and context from AWS Lambda.
export const handler = async (event, context, callback) => {
    // Parses the invokingEvent and ruleParameters values, which contain JSON objects
 passed as strings.
    var invokingEvent = JSON.parse(event.invokingEvent),
        ruleParameters = JSON.parse(event.ruleParameters),
        numberOfResources = 0;

    if (isScheduledNotification(invokingEvent) &&
 hasValidRuleParameters(ruleParameters, callback)) {
        await countResourceTypes(ruleParameters.applicableResourceType, "",
 numberOfResources, async function (err, count) {
            if (err === null) {
                var putEvaluationsRequest;
                const compliance = evaluateCompliance(ruleParameters.maxCount, count);
                var annotation = '';
                if (compliance === "NON_COMPLIANT") {
                    annotation = "Description of why the resource is not compliant.";
                }
                // Initializes the request that contains the evaluation results.
                if (annotation) {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
```

```
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date(),
                            Annotation: annotation
                        }],
                        ResultToken: event.resultToken
                    };
                } else {
                    putEvaluationsRequest = {
                        Evaluations: [{
                            // Applies the evaluation result to the AWS account
 published in the event.
                            ComplianceResourceType: 'AWS::::Account',
                            ComplianceResourceId: event.accountId,
                            ComplianceType: compliance,
                            OrderingTimestamp: new Date()
                        }],
                        ResultToken: event.resultToken
                    };
                }

                // Sends the evaluation results to AWS Config.
                try {
                    await configClient.send(new
 PutEvaluationsCommand(putEvaluationsRequest));
                }
                catch (e) {
                    callback(e, null);
                }
            } else {
                callback(err, null);
            }
        });
    } else {
        console.log("Invoked for a notification other than Scheduled Notification...
 Ignoring.");
    }
};

// Checks whether the invoking event is ScheduledNotification.
function isScheduledNotification(invokingEvent) {
    return (invokingEvent.messageType === 'ScheduledNotification');
}
```

```
// Checks the rule parameters to see if they are valid
function hasValidRuleParameters(ruleParameters, callback) {
    // Regular express to verify that applicable resource given is a resource type
    const awsResourcePattern = /^AWS::(\w*)::(\w*)$/;
    const isApplicableResourceType =
 awsResourcePattern.test(ruleParameters.applicableResourceType);
    // Check to make sure the maxCount in the parameters is an integer
    const maxCountIsInt = !isNaN(ruleParameters.maxCount) &&
 parseInt(Number(ruleParameters.maxCount)) == ruleParameters.maxCount && !
isNaN(parseInt(ruleParameters.maxCount, 10));
    if (!isApplicableResourceType) {
        callback("The applicableResourceType parameter is not a valid resource type.",
 null);
    }
    if (!maxCountIsInt) {
        callback("The maxCount parameter is not a valid integer.", null);
    }
    return isApplicableResourceType && maxCountIsInt;
}

// Checks whether the compliance conditions for the rule are violated.
function evaluateCompliance(maxCount, actualCount) {
    if (actualCount > maxCount) {
        return "NON_COMPLIANT";
    } else {
        return "COMPLIANT";
    }
}

// Counts the applicable resources that belong to the AWS account.
async function countResourceTypes(applicableResourceType, nextToken, count, callback) {
    const input = { resourceType: applicableResourceType, nextToken: nextToken };
    const command = new ListDiscoveredResourcesCommand(input);
    try {
        const response = await configClient.send(command);
        count = count + response.resourceIdentifiers.length;
        if (response.nextToken !== undefined && response.nextToken != null) {
            countResourceTypes(applicableResourceType, response.nextToken, count,
 callback);
        }
        callback(null, count);
    } catch (e) {
        callback(e, null);
    }
```

```
    return count;
}
```

函数运作

本函数在运行时执行以下操作：

1. 该函数在将event对象 AWS Lambda 传递给handler函数时运行。在此示例中，该函数接受可选callback参数，该参数用于向调用者返回信息。 AWS Lambda 还传递一个context对象，其中包含函数在运行时可以使用的信息和方法。请注意，在新版本的 Lambda 中，不再使用上下文。
2. 为计数指定类型的资源，处理程序会调用 countResourceTypes 函数，而且它传递其从事件收到的 applicableResourceType 参数。countResourceTypes 函数调用 listDiscoveredResources 客户端的 config 方法，该方法返回适用资源的标识符列表。该函数使用此列表的长度来确定适用资源的数量，而且它将此计数返回到处理程序。
3. 处理程序准备 AWS Config 通过初始化putEvaluationsRequest对象将评估结果发送到。此对象包括Evaluations参数，该参数标识合规性结果和 AWS 账户 在事件中发布的结果。您可以使用 Evaluations 参数将结果应用于 AWS Config支持的任何资源类型。该putEvaluationsRequest对象还包括事件的结果标记，用于标识规则和事件 AWS Config。
4. 在 putEvaluationsRequest 对象中，处理程序调用 evaluateCompliance 函数。此函数测试适用资源的数量是否超出分配给事件所提供的 maxCount 参数的最大值。如果资源的数量超出最大值，函数将返回 NON_COMPLIANT。如果资源的数量没有超出最大值，函数将返回 COMPLIANT。
5. AWS Config 通过将对象传递给config客户端putEvaluations的方法，处理程序将评估结果发送到。

用于 AWS Config 规则 (Python) 的示例 AWS Lambda 函数

AWS Lambda 将执行函数来响应由 AWS 服务发布的事件。用于 AWS Config 自定义 Lambda 规则的函数收到一个由 AWS Config 发布的事件，然后该函数使用从该事件接收以及它通过 AWS Config API 检索的数据，来评估是否符合规则。用于 Config 规则的函数的运作方式会因其执行的评估是由配置更改触发还是定期触发而有所不同。

有关 AWS Lambda 函数中常见模式的信息，请参阅《AWS Lambda 开发人员指南》中的编程模型。

目录

- 评估由配置更改触发时的示例函数
- 定期评估时的示例函数

评估由配置更改触发时的示例函数

AWS Config 检测到自定义规则范围内的资源发生配置更改时，会调用函数示例如下。

如果您使用 AWS Config 控制台创建与类似此示例的函数关联的规则，请选择 Configuration changes (配置更改) 作为触发器类型。如果您使用 AWS Config API 或 AWS CLI 创建规则，请将 `MessageType` 属性设置为 `ConfigurationItemChangeNotification` 和 `OversizedConfigurationItemChangeNotification`。这些设置可使您的规则在每次 AWS Config 生成配置项或资源更改导致过大配置项时触发。

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

# Helper function used to validate input
def check_defined(reference, reference_name):
    if not reference:
        raise Exception('Error: ', reference_name, 'is not defined')
    return reference

# Check whether the message is OversizedConfigurationItemChangeNotification or not
```

```
def is_oversized_changed_notification(message_type):
    check_defined(message_type, 'messageType')
    return message_type == 'OversizedConfigurationItemChangeNotification'

# Get configurationItem using getResourceConfigHistory API
# in case of OversizedConfigurationItemChangeNotification
def get_configuration(resource_type, resource_id, configuration_capture_time):
    result = AWS_CONFIG_CLIENT.get_resource_config_history(
        resourceType=resource_type,
        resourceId=resource_id,
        laterTime=configuration_capture_time,
        limit=1)
    configurationItem = result['configurationItems'][0]
    return convert_api_configuration(configurationItem)

# Convert from the API model to the original invocation model
def convert_api_configuration(configurationItem):
    for k, v in configurationItem.items():
        if isinstance(v, datetime.datetime):
            configurationItem[k] = str(v)
    configurationItem['awsAccountId'] = configurationItem['accountId']
    configurationItem['ARN'] = configurationItem['arn']
    configurationItem['configurationStateMd5Hash'] =
 configurationItem['configurationItemMD5Hash']
    configurationItem['configurationItemVersion'] = configurationItem['version']
    configurationItem['configuration'] = json.loads(configurationItem['configuration'])
    if 'relationships' in configurationItem:
        for i in range(len(configurationItem['relationships'])):
            configurationItem['relationships'][i]['name'] =
 configurationItem['relationships'][i]['relationshipName']
    return configurationItem

# Based on the type of message get the configuration item
# either from configurationItem in the invoking event
# or using the getResourceConfigHistory API in getConfiguration function.
def get_configuration_item(invokingEvent):
    check_defined(invokingEvent, 'invokingEvent')
    if is_oversized_changed_notification(invokingEvent['messageType']):
        configurationItemSummary =
 check_defined(invokingEvent['configurationItemSummary'], 'configurationItemSummary')
        return get_configuration(configurationItemSummary['resourceType'],
 configurationItemSummary['resourceId'],
 configurationItemSummary['configurationItemCaptureTime'])
    return check_defined(invokingEvent['configurationItem'], 'configurationItem')
```

```
# Check whether the resource has been deleted. If it has, then the evaluation is
 unnecessary.
def is_applicable(configurationItem, event):
    try:
        check_defined(configurationItem, 'configurationItem')
        check_defined(event, 'event')
    except:
        return True
    status = configurationItem['configurationItemStatus']
    eventLeftScope = event['eventLeftScope']
    if status == 'ResourceDeleted':
        print("Resource Deleted, setting Compliance Status to NOT_APPLICABLE.")
    return (status == 'OK' or status == 'ResourceDiscovered') and not eventLeftScope

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

def evaluate_change_notification_compliance(configuration_item, rule_parameters):
    check_defined(configuration_item, 'configuration_item')
    check_defined(configuration_item['configuration'],
 'configuration_item[\'configuration\']')
    if rule_parameters:
        check_defined(rule_parameters, 'rule_parameters')

    if (configuration_item['resourceType'] != 'AWS::EC2::Instance'):
        return 'NOT_APPLICABLE'

    elif rule_parameters.get('desiredInstanceType'):
        if (configuration_item['configuration']['instanceType'] in
 rule_parameters['desiredInstanceType']):
```

```
            return 'COMPLIANT'
    return 'NON_COMPLIANT'

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    check_defined(event, 'event')
    invoking_event = json.loads(event['invokingEvent'])
    rule_parameters = {}
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    configuration_item = get_configuration_item(invoking_event)
    if is_applicable(configuration_item, event):
        compliance_value = evaluate_change_notification_compliance(
                configuration_item, rule_parameters)

    response = AWS_CONFIG_CLIENT.put_evaluations(
       Evaluations=[
           {
               'ComplianceResourceType': invoking_event['configurationItem']
['resourceType'],
               'ComplianceResourceId': invoking_event['configurationItem']
['resourceId'],
               'ComplianceType': compliance_value,
               'OrderingTimestamp': invoking_event['configurationItem']
['configurationItemCaptureTime']
           },
       ],
       ResultToken=event['resultToken'])
```

函数运作

本函数在运行时执行以下操作：

1. 此函数在 AWS Lambda 将 `event` 对象传递给 `handler` 函数时运行。在此示例中，该函数接受可选 `callback` 参数，该参数用于向调用方返回信息。AWS Lambda 还会传递一个 `context` 对象，其中包含函数在运行时可以使用的信息和方法。请注意，在新版本的 Lambda 中，不再使用上下文。

2. 此函数检查事件的 messageType 是配置项还是过大配置项，然后返回配置项。
3. 处理程序调用 isApplicable 函数来确定资源是否已删除。

> **Note**
>
> 报告已删除资源的规则应返回 NOT_APPLICABLE 的评估结果，以避免不必要的规则评估。

4. 处理程序调用 evaluateChangeNotificationCompliance 函数并传递 AWS Config 在事件中发布的 configurationItem 和 ruleParameters 对象。

   函数首先评估资源是否为 EC2 实例。如果资源不是 EC2 实例，函数会返回 NOT_APPLICABLE 这一合规性值。

   然后，函数评估配置项中的 instanceType 属性是否与 desiredInstanceType 参数值一致。如果值相等，该函数将返回 COMPLIANT。如果值不相等，该函数将返回 NON_COMPLIANT。
5. 处理程序通过初始化 putEvaluationsRequest 对象来做好向 AWS Config 发送评估结果的准备。该对象包含 Evaluations 参数，这一参数用于识别受评估资源的合规性结果、资源类型和 ID。putEvaluationsRequest 对象还包含来自事件的结果令牌，该令牌可标识 AWS Config 的规则和事件。
6. 处理程序通过向 config 客户端的 putEvaluations 方法传递对象来向 AWS Config 发送评估结果。

定期评估时的示例函数

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

如果您使用 AWS Config 控制台创建与类似此示例的函数关联的规则，请选择 Periodic (定期) 作为触发器类型。如果您使用 AWS Config API 或 AWS CLI 创建规则，请将 MessageType 属性设置为 ScheduledNotification。

```
import botocore
import boto3
import json
import datetime

# Set to True to get the lambda to assume the Role attached on the Config Service
 (useful for cross-account).
ASSUME_ROLE_MODE = False
```

```
DEFAULT_RESOURCE_TYPE = 'AWS::::Account'

# This gets the client after assuming the Config service role
# either in the same AWS account or cross-account.
def get_client(service, event):
    """Return the service boto client. It should be used instead of directly calling
 the client.
    Keyword arguments:
    service -- the service name used for calling the boto.client()
    event -- the event variable given in the lambda handler
    """
    if not ASSUME_ROLE_MODE:
        return boto3.client(service)
    credentials = get_assume_role_credentials(event["executionRoleArn"])
    return boto3.client(service, aws_access_key_id=credentials['AccessKeyId'],
                        aws_secret_access_key=credentials['SecretAccessKey'],
                        aws_session_token=credentials['SessionToken']
                       )

def get_assume_role_credentials(role_arn):
    sts_client = boto3.client('sts')
    try:
        assume_role_response = sts_client.assume_role(RoleArn=role_arn,
 RoleSessionName="configLambdaExecution")
        return assume_role_response['Credentials']
    except botocore.exceptions.ClientError as ex:
        # Scrub error message for any internal account info leaks
        if 'AccessDenied' in ex.response['Error']['Code']:
            ex.response['Error']['Message'] = "AWS Config does not have permission to
 assume the IAM role."
        else:
            ex.response['Error']['Message'] = "InternalError"
            ex.response['Error']['Code'] = "InternalError"
        raise ex

# Check whether the message is a ScheduledNotification or not.
def is_scheduled_notification(message_type):
    return message_type == 'ScheduledNotification'

def count_resource_types(applicable_resource_type, next_token, count):
    resource_identifier =
 AWS_CONFIG_CLIENT.list_discovered_resources(resourceType=applicable_resource_type,
 nextToken=next_token)
    updated = count + len(resource_identifier['resourceIdentifiers']);
```

```
    return updated

# Evaluates the configuration items in the snapshot and returns the compliance value to
 the handler.
def evaluate_compliance(max_count, actual_count):
    return 'NON_COMPLIANT' if int(actual_count) > int(max_count) else 'COMPLIANT'

def evaluate_parameters(rule_parameters):
    if 'applicableResourceType' not in rule_parameters:
        raise ValueError('The parameter with "applicableResourceType" as key must be
 defined.')
    if not rule_parameters['applicableResourceType']:
        raise ValueError('The parameter "applicableResourceType" must have a defined
 value.')
    return rule_parameters

# This generate an evaluation for config
def build_evaluation(resource_id, compliance_type, event,
 resource_type=DEFAULT_RESOURCE_TYPE, annotation=None):
    """Form an evaluation as a dictionary. Usually suited to report on scheduled rules.
    Keyword arguments:
    resource_id -- the unique id of the resource to report
    compliance_type -- either COMPLIANT, NON_COMPLIANT or NOT_APPLICABLE
    event -- the event variable given in the lambda handler
    resource_type -- the CloudFormation resource type (or AWS::::Account) to report on
 the rule (default DEFAULT_RESOURCE_TYPE)
    annotation -- an annotation to be added to the evaluation (default None)
    """
    eval_cc = {}
    if annotation:
        eval_cc['Annotation'] = annotation
    eval_cc['ComplianceResourceType'] = resource_type
    eval_cc['ComplianceResourceId'] = resource_id
    eval_cc['ComplianceType'] = compliance_type
    eval_cc['OrderingTimestamp'] = str(json.loads(event['invokingEvent'])
['notificationCreationTime'])
    return eval_cc

def lambda_handler(event, context):

    global AWS_CONFIG_CLIENT

    evaluations = []
    rule_parameters = {}
```

```
    resource_count = 0
    max_count = 0

    invoking_event = json.loads(event['invokingEvent'])
    if 'ruleParameters' in event:
        rule_parameters = json.loads(event['ruleParameters'])

    valid_rule_parameters = evaluate_parameters(rule_parameters)

    compliance_value = 'NOT_APPLICABLE'

    AWS_CONFIG_CLIENT = get_client('config', event)
    if is_scheduled_notification(invoking_event['messageType']):
        result_resource_count =
 count_resource_types(valid_rule_parameters['applicableResourceType'], '',
 resource_count)

    if valid_rule_parameters.get('maxCount'):
        max_count = valid_rule_parameters['maxCount']

    compliance_value = evaluate_compliance(max_count, result_resource_count)
    evaluations.append(build_evaluation(event['accountId'], compliance_value, event,
 resource_type=DEFAULT_RESOURCE_TYPE))
    response = AWS_CONFIG_CLIENT.put_evaluations(Evaluations=evaluations,
 ResultToken=event['resultToken'])
```

函数运作

本函数在运行时执行以下操作：

1. 此函数在 AWS Lambda 将 `event` 对象传递给 `handler` 函数时运行。在此示例中，该函数接受可选 `callback` 参数，该参数用于向调用方返回信息。AWS Lambda 还会传递一个 `context` 对象，其中包含函数在运行时可以使用的信息和方法。请注意，在新版本的 Lambda 中，不再使用上下文。
2. 为计数指定类型的资源，处理程序会调用 `countResourceTypes` 函数，而且它传递其从事件收到的 `applicableResourceType` 参数。`countResourceTypes` 函数调用 `listDiscoveredResources` 客户端的 `config` 方法，该方法返回适用资源的标识符列表。该函数使用此列表的长度来确定适用资源的数量，而且它将此计数返回到处理程序。
3. 处理程序通过初始化 `putEvaluationsRequest` 对象来做好向 AWS Config 发送评估结果的准备。该对象包含 `Evaluations` 参数，该参数可以识别合规性结果和在事件中发布的 AWS 账户。您可以使用 `Evaluations` 参数将结果应用于 AWS Config 支持的任何资源类

型。putEvaluationsRequest 对象还包含来自事件的结果令牌，该令牌可标识 AWS Config 的规则和事件。

4. 在 putEvaluationsRequest 对象中，处理程序调用 evaluateCompliance 函数。此函数测试适用资源的数量是否超出分配给事件所提供的 maxCount 参数的最大值。如果资源的数量超出最大值，函数将返回 NON_COMPLIANT。如果资源的数量没有超出最大值，函数将返回 COMPLIANT。
5. 处理程序通过向 config 客户端的 putEvaluations 方法传递对象来向 AWS Config 发送评估结果。

AWS Config 规则的示例事件

当规则的触发器发生时，通过发布事件来 AWS Config 调用规则的 AWS Lambda 函数。然后通过将事件传递给函数的处理程序来 AWS Lambda 执行该函数。

由配置更改触发的评估的示例事件

AWS Config 当它检测到规则范围内的资源的配置更改时会发布事件。下面的示例事件演示规则被某个 EC2 实例的配置更改所触发。

```
{
    "invokingEvent": "{\"configurationItem\":{\"configurationItemCaptureTime
\":\"2016-02-17T01:36:34.043Z\",\"awsAccountId\":\"123456789012\",
\"configurationItemStatus\":\"OK\",\"resourceId\":\"i-00000000\",\"ARN
\":\"arn:aws:ec2:us-east-2:123456789012:instance/i-00000000\",\"awsRegion
\":\"us-east-2\",\"availabilityZone\":\"us-east-2a\",\"resourceType\":
\"AWS::EC2::Instance\",\"tags\":{\"Foo\":\"Bar\"},\"relationships\":[{\"resourceId
\":\"eipalloc-00000000\",\"resourceType\":\"AWS::EC2::EIP\",\"name\":\"Is
 attached to ElasticIp\"}],\"configuration\":{\"foo\":\"bar\"}},\"messageType\":
\"ConfigurationItemChangeNotification\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "change-triggered-config-rule",
    "configRuleId": "config-rule-0123456",
    "accountId": "123456789012",
    "version": "1.0"
}
```

由过大配置更改触发的评估的示例事件

某些资源更改会生成过大配置项。下面的示例事件演示规则被某个 EC2 实例的过大配置更改所触发。

```
{
        "invokingEvent": "{\"configurationItemSummary\": {\"changeType\":
 \"UPDATE\",\"configurationItemVersion\": \"1.2\",\"configurationItemCaptureTime
\":\"2016-10-06T16:46:16.261Z\",\"configurationStateId\": 0,\"awsAccountId
\":\"123456789012\",\"configurationItemStatus\": \"OK\",\"resourceType
\": \"AWS::EC2::Instance\",\"resourceId\":\"i-00000000\",\"resourceName
\":null,\"ARN\":\"arn:aws:ec2:us-west-2:123456789012:instance/i-00000000\",
\"awsRegion\": \"us-west-2\",\"availabilityZone\":\"us-west-2a\",
\"configurationStateMd5Hash\":\"8f1ee69b287895a0f8bc5753eca68e96\",
\"resourceCreationTime\":\"2016-10-06T16:46:10.489Z\"},\"messageType\":
\"OversizedConfigurationItemChangeNotification\"}",
        "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
        "resultToken": "myResultToken",
        "eventLeftScope": false,
        "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
        "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-ec2-managed-instance-inventory",
        "configRuleName": "change-triggered-config-rule",
        "configRuleId": "config-rule-0123456",
        "accountId": "123456789012",
        "version": "1.0"
    }
```

由定期频率触发的评估的示例事件

AWS Config 当它以您指定的频率（例如每 24 小时）评估您的资源时发布一个事件。下面的示例事件演示规则被定期频率触发。

```
{
    "invokingEvent": "{\"awsAccountId\":\"123456789012\",\"notificationCreationTime\":
\"2016-07-13T21:50:00.373Z\",\"messageType\":\"ScheduledNotification\",\"recordVersion
\":\"1.0\"}",
    "ruleParameters": "{\"myParameterKey\":\"myParameterValue\"}",
    "resultToken": "myResultToken",
    "eventLeftScope": false,
    "executionRoleArn": "arn:aws:iam::123456789012:role/config-role",
    "configRuleArn": "arn:aws:config:us-east-2:123456789012:config-rule/config-
rule-0123456",
    "configRuleName": "periodic-config-rule",
```

```
    "configRuleId": "config-rule-6543210",
    "accountId": "123456789012",
    "version": "1.0"
}
```

事件属性

AWS Config 事件的 JSON 对象包含以下属性：

`invokingEvent`

触发规则评估的事件。如果事件是为了响应资源配置更改而发布的，则此属性的值是一个包含 JSON `configurationItem` 或 `configurationItemSummary` (对于过大配置项) 的字符串。配置项目表示 AWS Config 检测到更改时资源的状态。有关配置项目的示例，请参阅中的`get-resource-config-history` AWS CLI 命令生成的输出查看配置历史记录。

如果事件是针对定期评估而发布的，则值是一个包含 JSON 对象的字符串。该对象包含关于已触发的评估的信息。

对于每种类型的事件，函数必须通过 JSON 解析程序解析字符串，以便能够评估其内容，如下面的 Node.js 示例中所示：

```
var invokingEvent = JSON.parse(event.invokingEvent);
```

`ruleParameters`

函数会将其作为评估逻辑的一部分来处理的键/值对。您可以在使用 AWS Config 控制台创建自定义 Lambda 规则时定义参数。您也可以在 `PutConfigRule` AWS Config API 请求或`put-config-rule` AWS CLI 命令中使用`InputParameters`属性定义参数。

参数的 JSON 代码包含在字符串中，因此，函数必须通过 JSON 解析程序解析字符串，以便能够评估其内容，如下面的 Node.js 示例中所示：

```
var ruleParameters = JSON.parse(event.ruleParameters);
```

`resultToken`

函数在调用时必须传递给 AWS Config 的标`PutEvaluations`记。

`eventLeftScope`

一个布尔值，表示要评估的 AWS 资源是否已从规则的作用域中移除。如果值为 `true`，则该函数表示可通过传递 `NOT_APPLICABLE` 作为 `ComplianceType` 调用中的 `PutEvaluations` 属性值来忽略评估。

`executionRoleArn`

分配给的 IAM 角色的 ARN。 AWS Config

`configRuleArn`

AWS Config 分配给规则的 ARN。

`configRuleName`

您为导致 AWS Config 发布事件和调用函数的规则分配的名称。

`configRuleId`

AWS Config 分配给规则的 ID。

`accountId`

拥有 AWS 账户 该规则的 ID。

`version`

由分配的版本号 AWS。如果向 AWS Config 事件 AWS 添加属性，则版本将增加。如果函数需要仅在匹配或超过特定版本的事件中的属性，则该函数可以检查此属性的值。

AWS Config 事件的当前版本是 1.0。

添加、更新和删除 AWS Config 规则

您可以使用 AWS Config 控制台或 AWS SDK 查看、添加和删除您的规则。

添加、查看、更新和删除规则（控制台）

规则页面在一个表中显示您的规则及其当前的合规性结果。每条规则的结果都是 “正在评估...” 直到根据规则 AWS Config 完成对您的资源进行评估。您可以使用刷新按钮更新结果。 AWS Config 完成评估后，您可以看到合规或不合规的规则和资源类型。有关更多信息，请参阅 查看合规信息和评估结果。

> **Note**
>
> AWS Config 仅评估其记录的资源类型。例如，如果您添加了启用 cloudtra il 的规则，但未记录 CloudTrail 跟踪资源类型，则 AWS Config 无法评估您账户中的跟踪是合规还是不合规。有关更多信息，请参阅 录制 AWS 资源。

添加规则

添加一项规则

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 在左侧导航窗格中，选择 Rules。
4. 在 Rules 页面，选择 Add rule。
5. 在指定规则类型页面上，通过完成以下步骤指定规则类型：
   a. 在搜索字段中键入内容，以便按规则名称、描述和标签筛选托管规则列表。例如，键入 EC2 可返回评估 EC2 资源类型的规则，或者键入 periodic 可返回定期触发的规则。
   b. 您还可以创建自己的自定义规则。选择使用 Lambda 创建自定义规则或使用 Guard 创建自定义规则，然后按照创建自定义 AWS Config Lambda 规则或创建 AWS Config自定义策略规则中的步骤进行操作。
6. 在创建规则页面上，通过完成以下步骤来配置规则：
   a. 对于 Name，请输入一个唯一的规则名称。
   b. 对于描述，键入规则的描述。
   c. 对于评估模式，请选择在资源创建和管理过程中何 AWS Config 时评估您的资源。根据规则，AWS Config 可以在部署资源之前、部署资源之后或两者兼而有之地评估您的资源配置。
      i. 选择开启主动评估，以允许您在部署资源之前对资源的配置设置进行评估。

         开启主动评估后，您可以使用StartResource评估 API 和 GetResourceEvaluationSummaryAPI 来检查您在这些命令中指定的资源是否会被您所在地区的账户中的主动规则标记为 “不合规”。

有关使用此命令的更多信息，请参阅使用 AWS Config 规则评估您的资源。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。

ii. 选择开启侦查评估以评估您的现有资源的配置设置。

对于侦查评估，有两种类型的触发器：在配置发生更改时和定期。

A. 如果您的规则的触发器类型包括配置更改，请为 AWS Config 调用您的 Lambda 函数的更改范围指定以下选项之一：

- 资源 – 在创建、更改或删除与指定资源类型（或类型和标识符）匹配的资源时。
- 标签 – 在创建、更改或删除包含指定标签的资源时。
- 所有更改-创建、更改或删除记录的资源时。 AWS Config

AWS Config 当它检测到与规则范围相匹配的资源发生变化时，就会运行评估。您可以使用范围来定义哪些资源启动评估。

B. 如果您的规则的触发器类型包括定期，请指定 AWS Config 调用 Lambda 函数的频率。

d. 对于参数，如果您的规则包含参数，可以自定义所提供的键的值。参数是资源在被视为符合规则之前必须遵守的属性。

7. 在 “查看并创建” 页面上，查看您的所有选择，然后再将规则添加到您的 AWS 账户。如果规则没有按预期运行，您可能会在合规性中看到以下内容之一：

- 未报告任何结果- AWS Config 根据规则评估了您的资源。该规则不适用于其范围内的 AWS 资源，指定的资源已被删除，或者评估结果被删除。要获取评估结果，请更新规则、更改其范围或者选择 Re-evaluate。

  如果规则不报告评估结果，该消息可能也会出现。

- 范围内没有资源- AWS Config 无法根据此规则评估您记录的 AWS 资源，因为您的所有资源都不在该规则的范围内。要获得评估结果，请编辑规则并更改其范围，或者使用 “设置” 页面添加 AWS Config 要记录的资源。
- Evaluations failed (评估失败) - 有关可帮助您确定问题的信息，请选择规则名称以打开其详细信息页面并查看错误消息。

查看规则

查看您的规则

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 在左侧导航窗格中，选择 Rules。
4. “规则” 页面显示您当前存在的所有规则 AWS 账户。其中列出每条规则的名称、关联的修正操作和合规性状态。
   - 选择 Add rule 以开始创建规则。
   - 选择规则可查看其设置，或者选择规则，然后选择查看详细信息。
   - 当规则评估资源时，请查看规则的合规性状态。
   - 选择规则，然后选择编辑规则以更改该规则的配置设置，并为不合规的规则设置修正操作。

更新规则

更新规则

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 在左侧导航窗格中，选择 Rules。
4. 选择规则，然后为要更新的规则选择编辑规则。
5. 在编辑规则页面上修改设置，以根据需要更改您的规则。
6. 选择保存。

删除规则

删除一项规则

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 在左侧导航窗格中，选择 Rules。
4. 从表中选择要删除的规则。
5. 从操作下拉列表中，选择删除规则。
6. 出现提示时，键入“Delete”（此条目区分大小写），然后选择删除。

开启主动评估

可以使用主动评估在资源部署之前对其进行评估。这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。

资源类型架构说明了资源的属性。您可以在 AWS CloudFormation 注册表的 “AWS 公共扩展” 中找到资源类型架构，也可以使用以下 CLI 命令找到：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

有关更多信息，请参阅《 AWS CloudFormation 用户指南》中参考的通过 AWS CloudFormation 注册表管理扩展以及AWS 资源和属性类型。

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

开启主动评估

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。

2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的区域。有关支持的 AWS 区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和端点。
3. 在左侧导航窗格中，选择 Rules。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。
4. 选择规则，然后为要更新的规则选择编辑规则。
5. 对于评估模式，选择开启主动评估，以允许您在部署资源之前对资源的配置设置进行评估。
6. 选择保存。

开启主动评估后，您可以使用StartResource评估 API 和 GetResourceEvaluationSummaryAPI 来检查您在这些命令中指定的资源是否会被您所在地区的账户中的主动规则标记为 “不合规”。

例如，从 StartResourceEvaluation API 开始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您应该会在输出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然后，使用`ResourceEvaluationId`带有 GetResourceEvaluationSummary API 的来检查评估结果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您应收到类似以下内容的输出：

```
{
```

```
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

要查看有关评估结果的其他信息，例如哪条规则将资源标记为 “不合规”，请使用资源 API。GetCompliance DetailsBy

查看、更新或添加和删除规则 (AWS SDK)

查看规则

以下代码示例演示如何使用 `DescribeConfigRules`。

CLI

AWS CLI

获取 AWS Config 规则的详细信息

以下命令返回名为的 AWS Config 规则的详细信息`InstanceTypesAreT2micro`：

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

输出：

```
{
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
```

```
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅DescribeConfig《AWS CLI 命令参考》中的规则。

PowerShell

用于 PowerShell

示例 1：此示例列出了账户的配置规则以及选定的属性。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

输出：

```
ConfigRuleName                                      ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
```

```
--------------                                    ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                             config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                               config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required        config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考中的DescribeConfig规则。

Python

SDK for Python (Boto3)

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

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.
```

```
        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- 有关 API 的详细信息，请参阅适用于 Python 的AWS SDK (Boto3) API 参考中的DescribeConfig规则。

更新或添加规则

以下代码示例演示如何使用 `PutConfigRule`。

CLI

AWS CLI

添加 AWS 托管 Config 规则

以下命令提供用于添加 AWS 托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` 是一个包含规则配置的 JSON 文件：

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
```

```
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

对于该`ComplianceResourceTypes`属性，此 JSON 代码将范围限制为该`AWS::EC2::Instance`类型的资源，因此 AWS Config 将仅根据规则评估 EC2 实例。由于该规则是托管规则，因此 `Owner` 属性设置为 `AWS`，`SourceIdentifier` 属性设置为规则标识符 `REQUIRED_TAGS`。对于 `InputParameters` 属性，指定了规则所需的标签键 `CostCenter` 和 `Owner`。

如果命令成功， AWS Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules 命令并指定规则名称。

添加客户托管的 Config 规则

以下命令将提供用于添加客户托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` 是一个包含规则配置的 JSON 文件：

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
```

```
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

对于该`ComplianceResourceTypes`属性，此 JSON 代码将范围限制为该`AWS::EC2::Instance`类型的资源，因此 AWS Config 将仅根据规则评估 EC2 实例。由于此规则是客户托管规则，因此该`Owner`属性设置为`CUSTOM_LAMBDA`，并且该`SourceIdentifier`属性设置为 Lambda 函数 AWS 的 ARN。`SourceDetails`对象为必填项。当 Confi AWS g 调用 AWS Lambda 函数来根据规则评估资源时，为该`InputParameters`属性指定的参数将传递给 Lambda 函数。

如果命令成功， AWS Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules 命令并指定规则名称。

- 有关 API 的详细信息，请参阅《AWS CLI 命令参考》中的PutConfig规则。

Python

SDK for Python (Boto3)

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

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
```

```
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- 有关 API 的详细信息，请参阅 Python AWS SDK 中的PutConfig规则 (Boto3) API 参考。

删除规则

以下代码示例演示如何使用 `DeleteConfigRule`。

CLI

AWS CLI

删除 C AWS onfig 规则

以下命令删除名为的 AWS Config 规则`MyConfigRule`：

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- 有关 API 的详细信息，请参阅《AWS CLI 命令参考》中的DeleteConfig规则。

Python

SDK for Python (Boto3)

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

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
```

```
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- 有关 API 的详细信息，请参阅 Python AWS SDK 中的DeleteConfig规则 (Boto3) API 参考。

开启主动评估 (AWS CLI)

可以使用主动评估在资源部署之前对其进行评估。这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。

资源类型架构说明了资源的属性。您可以在 AWS CloudFormation 注册表的 “AWS 公共扩展” 中找到资源类型架构，也可以使用以下 CLI 命令找到：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

有关更多信息，请参阅《 AWS CloudFormation 用户指南》中参考的通过 AWS CloudFormation 注册表管理扩展以及AWS 资源和属性类型。

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

开启主动评估

使用 `put-config-rule` 命令并为 `EvaluationModes` 启用 `PROACTIVE`。

开启主动评估后，您可以使用 start-resource-evaluation CLI 命令和 get- resource-evaluation-summary CLI 命令来检查您在这些命令中指定的资源是否会被您所在地区的账户中的主动规则标记为 “不合规”。

例如，先使用 start-resource-evaluation 命令：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
```

```
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您应该会在输出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然后，将 `ResourceEvaluationId` 和 get-resource-evaluation-summary 结合使用来检查评估结果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您应收到类似以下内容的输出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

要查看有关评估结果的更多信息，例如哪条规则将资源标记为 NON_COMPLIANT，请使用 get-compliance-details-by-resource CLI 命令。

> **Note**
>
> 有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。

开启主动评估 (API)

可以使用主动评估在资源部署之前对其进行评估。这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。

资源类型架构说明了资源的属性。您可以在 AWS CloudFormation 注册表的 “AWS 公共扩展” 中找到资源类型架构，也可以使用以下 CLI 命令找到：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

有关更多信息，请参阅《 AWS CloudFormation 用户指南》中参考的通过 AWS CloudFormation 注册表管理扩展以及AWS 资源和属性类型。

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

为规则开启主动评估

使用 “PutConfig规则” 操作并启`PROACTIVE`用`EvaluationModes`。

开启主动评估后，您可以使用StartResource评估 API 和 GetResourceEvaluationSummaryAPI 来检查您在这些命令中指定的资源是否会被您所在地区的账户中的主动规则标记为 “不合规”。例如，从 StartResourceEvaluation API 开始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",

 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您应该会在输出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然后，使用`ResourceEvaluationId`带有 GetResourceEvaluationSummary API 的来检查评估结果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您应收到类似以下内容的输出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

要查看有关评估结果的其他信息，例如哪条规则将资源标记为“不合规”，请使用资源 API。GetCompliance DetailsBy

> **Note**
>
> 有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。

将规则评估发送到 Security Hub

添加 AWS Config 规则后，您还可以将规则评估发送到 AWS Security Hub。与 Security Hub AWS Config 之间的集成允许您对规则评估以及其他错误配置和安全问题进行分类和修复。

将规则评估发送到 Security Hub

要向 Security Hub 发送规则评估，必须先设置 AWS Security Hub 和 AWS Config，然后再添加至少一条 AWS Config 托管或自定义规则。之后， AWS Config 立即开始向 Security Hub 发送规则评估。Security Hub 可以丰富规则评估，并将其转化为 Security Hub 调查结果。

有关此集成的更多信息，请参阅《 AWS Security Hub 用户指南》中的可用 AWS 服务集成。

使用 AWS Config 规则评估您的资源

创建自定义规则或使用托管规则时，会根据这些规则 AWS Config 评估您的资源。您可以按照您的规则对资源进行按需评估。例如，当您创建自定义规则并希望检查该规则 AWS Config 是否正确评估您的资源或确定 AWS Lambda 函数的评估逻辑是否存在问题时，这会很有帮助。

示例

1. 您创建一个自定义规则，用以评估您的 IAM 用户是否具有有效的访问密钥。
2. AWS Config 根据您的自定义规则评估您的资源。
3. 在您的账户中存在一个没有有效访问密钥的 IAM 用户。您的规则不能正确将此资源标记为 NON_COMPLIANT。
4. 您修复规则并重新开始评估。
5. 由于您修复了规则，规则正确评估您的资源，并将 IAM 用户资源标记为 NON_COMPLIANT。

向账户添加规则时，您可以指定在资源创建和管理过程中何 AWS Config 时评估您的资源。资源创建和管理过程称为资源预置。您可以选择评估模式来指定在此过程中何 AWS Config 时评估您的资源。

根据规则， AWS Config 可以在部署资源之前、部署资源之后或两者兼而有之地评估您的资源配置。在资源部署之前对其进行评估是主动评估。在资源部署之后对其进行评估是侦查评估。

主动模式

使用主动评估在资源部署之前对其进行评估。这使您可以评估一组资源属性（如果用于定义 AWS 资源）是合规还是不合规，因为您所在地区的账户中有一组主动规则。

资源类型架构说明了资源的属性。您可以在 AWS CloudFormation 注册表的 “AWS 公共扩展” 中找到资源类型架构，也可以使用以下 CLI 命令找到：

```
aws cloudformation describe-type --type-name "AWS::S3::Bucket" --type RESOURCE
```

有关更多信息，请参阅通过 AWS CloudFormation 注册表管理扩展以及 AWS CloudFormation 用户指南中的AWS 资源和属性类型参考。

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

评估您的资源

开启主动评估

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，确认区域选择器设置为支持 AWS Config 规则的区域。有关支持的 AWS 区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和端点。
3. 在左侧导航窗格中，选择 Rules。有关支持主动评估的托管规则列表，请参阅按评估模式列出的 AWS Config 托管规则列表。
4. 选择规则，然后为要更新的规则选择编辑规则。
5. 对于评估模式，选择开启主动评估，以允许您在部署资源之前对资源的配置设置进行评估。
6. 选择保存。

> **Note**
>
> 您也可以使用put-config-rule命令和启用PROACTIVE开启主动评估，EvaluationModes或者使用PutConfigRule操作和启PROACTIVE用EvaluationModes。

开启主动评估后，您可以使用 StartResourceEvaluationAPI 和 GetResourceEvaluationSummaryAPI 来检查您在这些命令中指定的资源是否会被您所在地区的账户中的主动规则标记为 “不合规”。

例如，从 StartResourceEvaluation API 开始：

```
aws configservice start-resource-evaluation --evaluation-mode PROACTIVE
                --resource-details '{"ResourceId":"MY_RESOURCE_ID",
                                     "ResourceType":"AWS::RESOURCE::TYPE",
```

```
 "ResourceConfiguration":"RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA",

 "ResourceConfigurationSchemaType":"CFN_RESOURCE_SCHEMA"}'
```

您应该会在输出中收到 `ResourceEvaluationId`：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID"
}
```

然后，使用`ResourceEvaluationId`带有 GetResourceEvaluationSummary API 的来检查评估结果：

```
aws configservice get-resource-evaluation-summary
    --resource-evaluation-id MY_RESOURCE_EVALUATION_ID
```

您应收到类似以下内容的输出：

```
{
    "ResourceEvaluationId": "MY_RESOURCE_EVALUATION_ID",
    "EvaluationMode": "PROACTIVE",
    "EvaluationStatus": {
        "Status": "SUCCEEDED"
    },
    "EvaluationStartTimestamp": "2022-11-15T19:13:46.029000+00:00",
    "Compliance": "COMPLIANT",
    "ResourceDetails": {
        "ResourceId": "MY_RESOURCE_ID",
        "ResourceType": "AWS::RESOURCE::TYPE",
        "ResourceConfiguration":
 "RESOURCE_DEFINITION_AS_PER_THE_RESOURCE_CONFIGURATION_SCHEMA"
    }
}
```

要查看有关评估结果的更多信息，例如哪条规则将资源标记为 “不合规”，请使用 API。GetComplianceDetailsByResource

侦查模式

使用侦查评估来评估已部署的资源。这允许您评估现有资源的配置设置。

评估您的资源（控制台）

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在 AWS Management Console 菜单中，检查区域选择器是否设置为支持 AWS Config 规则的区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 在导航窗格中，选择规则。规则页面显示每条规则的名称、关联的修正操作和合规性状态。
4. 从表中选择规则。
5. 从操作下拉列表中，选择重新评估。
6. AWS Config 开始根据您的规则评估资源。

> **Note**
>
> 您可以每分钟重新评估一次规则。您必须等待 AWS Config 规则的评估完成后才能开始另一次评估。如果规则同时被更新或同时被删除，您将无法运行评估。

评估您的资源 (CLI)

- 使用 start-config-rules-evaluation 命令：

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

AWS Config 开始根据您的规则评估记录的资源配置。您还可以在请求中指定多个规则：

```
$ aws configservice start-config-rules-evaluation --config-rule-
names ConfigRuleName1 ConfigRuleName2 ConfigRuleName3
```

评估您的资源 (API)

使用 StartConfigRulesEvaluation 操作。

从 AWS Config 规则中删除评估结果

在 AWS Config 评估您的规则后，您可以在该规则的 Rules (规则) 页或 Rules details (规则详细信息) 页上查看评估结果。如果评估结果不正确，或者您要重新评估，您可以删除该规则的当前评估结果。例如，如果您的规则错误地评估您的资源或从您最近已从账户中删除资源，您可以删除评估结果，然后运行新的评估。

删除评估结果（控制台）

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Config 控制台：https://console.aws.amazon.com/config/。
2. 在 AWS Management Console菜单上，验证区域选择器是否设置为支持 AWS Config 规则的 AWS 区域。有关支持的区域的列表，请参阅《Amazon Web Services 一般参考》中的 AWS Config 区域和终端节点。
3. 在导航窗格中，选择 Rules (规则)。规则页面显示每条规则的名称、关联的修正操作和合规性状态。
4. 从表中选择规则。
5. 从操作下拉列表中，选择删除结果。
6. 出现提示时，键入 Delete（此条目区分大小写），然后选择删除。删除评估后，您将无法对其进行检索。
7. 在评估结果被删除后，您可以手动开始新的评估。

删除评估结果 (CLI)

- 使用 delete-evaluation-results 命令。

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

  AWS Config 删除规则的评估结果。

删除评估结果 (API)

使用 DeleteEvaluationResults 操作。

管理组织中所有账户的 AWS Config 规则

> **Important**
>
> 只能使用 API 或 CLI 创建组织规则。 AWS Config 控制台不支持此操作。

AWS Config 允许您管理组织 AWS 账户 内所有部门的 AWS Config 规则。您可以：

- 集中创建、更新和删除组织中所有账户的 AWS Config 规则。
- 在所有账户中部署一组通用的 AWS Config 规则，并指定不应在其中创建 AWS Config 规则的账户。
- 通过确保组织的成员账户无法修改基础 AWS Config 规则，使用中 AWS Organizations 管理账户中的 API 来实施治理。

注意事项

对于跨不同区域的部署

跨账户部署规则和一致性包的 API 调用因 AWS 区域而异。在组织级别，如果您想在其他区域部署规则，需要将 API 调用的上下文更改为其他区域。例如，要在美国东部（弗吉尼亚州北部）部署规则，应将区域更改为美国东部（弗吉尼亚州北部），然后调用 `PutOrganizationConfigRule`。

对用于组织内的账户

如果有新账户加入组织，会将相关的规则或合规包部署到该账户中。当账户离开组织时，相关的规则或合规包将被删除。

如果您在组织管理员账户中部署组织规则或合规包，然后建立委派管理员，并在委派管理员账户中部署组织规则或合规包，您将无法通过委派管理员账户在组织管理员账户中查看组织规则或合规包，也无法通过组织管理员账户查看委派管理员账户中的组织规则或合规包。DescribeOrganizationConfigRules和 DescribeOrganizationConformancePacksAPI 只能查看从调用这些 API 的账户内部部署的组织相关资源并与之交互。

添加到组织的新账户的重试机制

如果没有记录器，则只有在向组织添加账户后，才会重试部署现有组织规则和合规包 7 小时。如果在向组织添加账户后的 7 小时内没有记录器，则需要创建一个记录器。

组织管理账户、委派管理员和服务相关角色

如果您使用的是组织管理帐户并打算使用委派管理员进行组织部署，请注意这 AWS Config 不会自动创建服务相关角色 (SLR)。您必须使用 IAM 单独手动创建服务相关角色 (SLR)。

如果您的管理账户没有 SLR，则无法从委托管理员账户向该账户部署资源。您仍然可以将管理账户和委派管理员账户中的 AWS Config 规则部署到成员账户。有关更多信息，请参阅 AWS Identity and Access Management (IAM) 用户指南中的使用服务相关角色。

部署

有关如何 AWS Config 与集成的信息 AWS Organizations，请参阅AWS Organizations 用户指南 AWS Organizations中的AWS Config 和。在使用以下 API 管理组织 AWS 账户 内所有 AWS Config 规则之前，请确保 AWS Config 录制已开启：

- PutOrganizationConfigRule，为整个组织添加或更新组织配置规则，以评估您的 AWS 资源是否符合所需的配置。
- DescribeOrganizationConfigRules，返回组织配置规则列表。
- GetOrganizationConfigRuleDetailedStatus，返回给定组织配置规则下组织内每个成员账户的详细状态。
- GetOrganizationCustomRulePolicy，返回包含组织配置自定义策略规则逻辑的策略定义。
- DescribeOrganizationConfigRule状态，提供组织的组织配置规则部署状态。
- DeleteOrganizationConfigRule，从该组织的所有成员账户中删除指定的组织配置规则及其所有评估结果。

区域支持

以下区域支持跨 AWS 组织成员账户部署 AWS Config 规则。

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

区域名称	区域	端点	协议
美国西部（加利福尼亚北部）	us-west-1	config.us-west-1.amazonaws.com	HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

使用规则修复不合规的资源 AWS Config

AWS Config 允许您修复由评估的不合规资源。 AWS Config 规则 AWS Config 使用AWS Systems Manager 自动化文档应用补救。这些文档定义了要对由 AWS Config 规则评估的不合规 AWS 资源执行的操作。您可以使用 AWS Management Console 或 API 来关联 SSM 文档。

AWS Config 提供了一组包含补救操作的托管自动化文档。您还可以创建自定义自动化文档并将其与 AWS Config 规则关联。

要对不合规的资源应用补救，您可以从预先填充的列表中选择要关联的修正操作，也可以使用 SSM 文档创建自己的自定义修复操作。 AWS Config 中提供了建议的补救措施列表 AWS Management Console。

在中 AWS Management Console，您可以通过将修复操作与规则关联来选择手动或自动修复不合规的资源。 AWS Config 借助所有修正操作，您可以选择手动或自动修正。

主题

- 先决条件
- 设置手动修正（控制台）
- 设置自动修正（控制台）
- 删除修正操作（控制台）
- 管理修正 (API)
- 区域支持

先决条件

在开始对不合规资源应用修正之前，您必须选择一条规则并针对该规则设置修正（手动或自动）。

设置手动修正（控制台）

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 选择左侧的规则，然后在规则页面上，选择添加规则以向规则列表中添加新规则。

   对于现有规则，从规则列表中选择不合规规则，然后选择操作下拉列表。
3. 从操作下拉列表中，选择管理修正。选择“手动修正”，然后从建议列表中选择相应的修正操作。

> **Note**
> 您只能管理非服务关联 AWS Config 规则的修正。有关更多信息，请参阅服务相关的 AWS 规则。

根据所选的修正操作，您将会看到特定参数，或者看不到任何参数。

4. （可选）如果要将不合规资源的资源 ID 传递给修正操作，请选择 Resource ID parameter (资源 ID 参数)。如果选中，则在运行时会将该参数替换为要修正的资源的 ID。

   每个参数都具有静态值或动态值。如果未从下拉列表中选择特定资源 ID 参数，可以为每个键输入值。如果从下拉列表中选择资源 ID 参数，可以为除所选资源 ID 参数之外的所有其他键输入值。

5. 选择保存。此时将显示 Rules (规则) 页面。

要对失败的修复操作进行故障排除，您可以运行 AWS 命令行界面命令`describe-remediation-execution-status`来获取一组资源的修复执行的详细视图。详细信息包括修正执行步骤的状态、时间戳，以及失败步骤的任何错误消息。

设置自动修正（控制台）

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 选择左侧的规则，然后在规则页面上，选择添加规则以向规则列表中添加新规则。

   对于现有规则，从规则列表中选择不合规规则，然后选择操作下拉列表。

3. 从操作下拉列表中，选择管理修正。选择“自动修正”，然后从建议列表中选择相应的修正操作。

> **Note**
> 您只能管理非服务关联 AWS Config 规则的修正。有关更多信息，请参阅服务相关的 AWS 规则。

根据所选的修正操作，您将会看到特定参数，或者看不到任何参数。

4. 选择 Auto remediation (自动修正) 以自动修正不合规的资源。

如果资源在自动修复后仍然不合规，则可以将规则设置为再次尝试自动修复。输入所需的重试次数和秒数。

> **Note**
>
> 多次运行修正脚本会有关联的成本。只有当修正失败，并且在指定时间段内有效时才会重试；例如，在 300 秒内重试 5 次。

5. （可选）如果要将不合规资源的资源 ID 传递给修正操作，请选择 Resource ID parameter (资源 ID 参数)。如果选中，则在运行时会将该参数替换为要修正的资源的 ID。

   每个参数都具有静态值或动态值。如果未从下拉列表中选择特定资源 ID 参数，可以为每个键输入值。如果从下拉列表中选择资源 ID 参数，可以为除所选资源 ID 参数之外的所有其他键输入值。
6. 选择保存。此时将显示 Rules (规则) 页面。

用于故障排除失败的补救措施

要对失败的修复操作进行故障排除，您可以运行 AWS 命令行界面命令`describe-remediation-execution-status`来获取一组资源的修复执行的详细视图。详细信息包括修正执行步骤的状态、时间戳，以及失败步骤的任何错误消息。

即使是合规资源也可以启动自动修复

如果您使用PutRemediation配置 API 或 AWS Config 控制台为特定 AWS Config 规则启用自动修复，则它会启动针对该特定规则的所有不合规资源的修复过程。auto 修复过程依赖于定期捕获的合规性数据快照。对于在快照计划之间更新的任何不合规资源，都将继续根据上次已知的合规性数据快照进行修复。

这意味着，在某些情况下，即使是合规资源也可以启动自动修复，因为引导处理器使用的数据库可能基于上次已知的合规性数据快照得出陈旧的评估结果。

删除修正操作（控制台）

要删除规则，必须首先删除与该规则关联的修正操作。

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 选择左侧的规则，然后在规则页面上，从规则列表中选择规则，再选择查看详细信息。

3. 在####页面上，转到修正操作部分。展开这部分以查看更多详细信息。
4. 在修正操作部分中，选择删除并确认您的删除操作。

> **Note**
>
> 如果正在进行修正，修正操作不会被删除。如果选择删除修正操作，您将无法检索修正操作。删除修正操作不会删除关联的规则。

如果删除了修正操作，则资源 ID 参数将为空并显示“不适用”。在规则页面上，修正操作列将显示未设置关联规则。

管理修正 (API)

手动修正

使用以下 AWS Config API 操作来管理补救措施：

- DeleteRemediation配置，删除修正配置。
- DescribeRemediation配置，返回一个或多个修复配置的详细信息。
- DescribeRemediationExecutionStatus，提供了一组资源的修正执行的详细视图，包括状态、执行修正步骤的时间戳以及失败步骤的任何错误消息。
- PutRemediation使用具有所选目标或操作的特定 AWS Config 规则@@ 配置、添加或更新修复配置。
- StartRemediation执行，根据上次已知的修正配置对指定 AWS Config 规则运行按需修复。

自动修正

使用以下 AWS Config API 操作来管理自动修复：

- PutRemediation异常、添加新异常或使用特定规则更新特定资源的现有异常。 AWS Config
- DescribeRemediation异常，返回一个或多个修正异常的详细信息。
- DeleteRemediation异常，删除资源密钥中提及的一个或多个修正异常。

区域支持

目前，以下区域支持 AWS Config 规则的修正操作：

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS
美国西部（加利福尼亚北部）	us-west-1	config.us-west-1.amazonaws.com	HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

故障排除

如果您无法删除 AWS Config 规则或收到类似于以下内容的错误，请检查以下问题进行故障排除：“出现错误” AWS Config。

AWS Identity and Access Management (IAM) 实体拥有 DeleteConfigRule 该 API 的权限

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择用户或角色。
3. 选择您用来删除 AWS Config 规则的用户或角色，然后展开权限策略。
4. 在 “权限” 选项卡中，选择 JSON。
5. 在 JSON 预览窗格中，确认 IAM 策略是否允许使用DeleteConfig规则 API 的权限。

IAM 实体权限边界允许 DeleteConfigRule API

如果 IAM 实体有权限边界，请确保它允许 DeleteConfigRule API 的权限。

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择用户或角色。
3. 选择您用来删除 AWS Config 规则的用户或角色，展开权限边界，然后选择 JSON。
4. 在 JSON 预览窗格中，确认 IAM 策略是否允许使用DeleteConfig规则 API 的权限。

> **Warning**
>
> IAM 用户拥有长期证书，这会带来安全风险。为帮助减轻这种风险，我们建议仅向这些用户提供执行任务所需的权限，并在不再需要这些用户时将其移除。

服务控制策略 (SCP) 允许 API DeleteConfigRule

1. 使用组织的管理账户打开 AWS Organizations 控制台，网址为 https://console.aws.amazon.com/organizations/。
2. 在账户名中，选择 AWS 账户。
3. 在策略中，展开服务控制策略并记下附加的 SCP 策略。
4. 在页面顶部，选择策略。
5. 选择策略，然后选择 “查看详细信息”。
6. 在 JSON 预览窗格中，确认策略允许使用DeleteConfig规则 API。

该规则不是服务相关规则

启用安全标准后， AWS Security Hub 会为您创建与服务相关的规则。您无法使用删除这些与服务相关的规则 AWS Config，并且删除按钮显示为灰色。要删除服务相关规则，请参阅 Securit y Hub 用户指南中的禁用安全标准。

未进行任何补救措施

您无法删除正在执行修正操作的 AWS Config 规则。按照步骤删除与该规则关联的修正操作。然后，再次尝试删除该规则。

> **Important**
>
> 仅删除处于失败或成功状态的修复操作。

合规包

一致性包是 AWS Config 规则和补救措施的集合，可以轻松地将其作为单个实体部署到一个账户和一个区域或整个组织中 AWS Organizations。

通过编写一个包含 AWS Config 规则（托管或自定义）和修复操作列表的 YAML 模板，可以创建一致性包。您还可以使用 AWS Systems Manager 文档（SSM 文档）将合规包模板存储在上面， AWS 并使用 SSM 文档名称直接部署一致性包。您可以使用 AWS Config 控制台或 AWS CLI部署模板。

要快速入门并评估您的 AWS 环境，请使用其中一个样本一致性包模板。您也可以基于自定义合规包，从头开始创建合规包 YAML 文件。

主题

- 先决条件
- 区域支持
- AWS Config 在一致性包中进行流程检查
- 一致性包示例模板
- 自定义合规包
- 在“合规包”控制面板中查看合规性数据
- 查看合规包的合规性历史记录时间线
- 使用 AWS Config 控制台部署一致性包
- 使用 AWS Command Line Interface部署一致性包
- 管理合规包 (API)
- 跨组织中的所有账户管理一致性包
- 故障排除

先决条件

在部署一致性包之前，请开启 AWS Config 录制。

开始 AWS Config 录制

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。

2. 在导航窗格中，选择设置。
3. 要开始记录，请选择 Recording is off (记录已关闭) 下的 Turn on (开启)。系统提示时，请选择继续。

将一致性包与修正结合使用的先决条件

在使用带有修复功能的示例模板部署一致性包之前，必须根据修复目标创建相应的 AWS 资源，例如自动代入角色和其他资源。

如果您已有 Automation 角色并使用该角色通过 SSM 文档进行修复，则可以直接提供该角色的 ARN。如果您有任何资源，可以在模板中提供这些资源。

> **Note**
>
> 向组织部署具有修正功能的合规包时，需要指定该组织的管理账户 ID。否则，在部署组织合规包期间， AWS Config 会自动将管理账户 ID 替换为成员账户 ID。

AWS Config 不支持自动化执行角色的 AWS CloudFormation 内部函数。您必须以字符串形式提供角色的准确 ARN。

有关如何传递准确 ARN 的更多信息，请参阅一致性包示例模板。使用示例模板时，请更新您的账户 ID 和组织的管理账户 ID。

使用带有一条或多 AWS Config 条规则的一致性包的先决条件

在部署包含一个或多个自定义 AWS Config 规则的一致性包之前，请创建相应的资源，例如 AWS Lambda 函数和相应的执行角色。

如果您已有自定义 AWS Config 规则，则可以直接提供 of AWS Lambda 函数来创建该ARN自定义规则的另一个实例，作为包的一部分。

如果您没有现有的自定义 AWS Config 规则，则可以创建一个 AWS Lambda 函数并使用 Lambda 函数的 ARN。有关更多信息，请参阅 AWS Config 自定义规则。

如果您的 AWS Lambda 函数存在于不同的中 AWS 账户，则可以使用适当的跨账户 AWS Lambda 功能授权来创建 AWS Config 规则。有关更多信息，请参阅如何集中管理多个 AWS Config 规则 AWS 账户博客文章。

Same account bucket policy

AWS Config 为了能够存储合规包项目，您需要提供一个 Amazon S3 存储桶并添加以下权限。有关命名存储桶的更多信息，请参阅存储桶命名规则。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::delivery-bucket-name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::AccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::delivery-bucket-name/[optional] prefix/
AWSLogs/AccountId/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    }
  ]
}
```

Cross-account bucket policy

AWS Config 为了能够存储合规包项目，您需要提供一个 Amazon S3 存储桶并添加以下权限。有关命名存储桶的更多信息，请参阅存储桶命名规则。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigConformsBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms",
            "PutConformancePack API caller user principal like
 arn:aws:iam::SourceAccountId:user/userName "
        ]
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name"
    },
    {
      "Sid": "AWSConfigConformsBucketDelivery",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control"
        }
      }
    },
    {
      "Sid": " AWSConfigConformsBucketReadAccess",
      "Effect": "Allow",
      "Principal": {
```

```
        "AWS": [
            "arn:aws:iam::SourceAccountId:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
        ]
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/[optional]
 prefix/AWSLogs/AccountID/Config/*"
    }
  ]
}
```

> **Note**
>
> 部署跨账户合规包时，传输 Amazon S3 存储桶的名称应以 `awsconfigconforms` 开头。

Organization 一致性包的先决条件

如果输入模板具有自动修正配置，则在模板中为该修正指定 Automation 执行角色 ARN。确保组织的所有账户（管理账户和成员账户）中都有具有指定名称的角色。您必须先在所有账户中创建此角色，然后再调用 `PutOrganizationConformancePack`。您可以手动创建此角色，也可以使用 AWS CloudFormation 堆栈集在每个账户中创建此角色。

如果您的模板使用 AWS CloudFormation 内部函数`Fn::ImportValue`来导入特定变量，则该变量必须在该组织的所有成员账户`Export Value`中定义为。

有关自定义 AWS Config 规则，请参阅如何集中管理多个 AWS Config 规则 AWS 账户博客以设置适当的权限。

组织存储桶策略：

AWS Config 为了能够存储合规包项目，您需要提供一个 Amazon S3 存储桶并添加以下权限。有关命名存储桶的更多信息，请参阅存储桶命名规则。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGetObject",
            "Effect": "Allow",
            "Principal": "*",
```

```
            "Action": [
                 "s3:GetObject",
                 "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        },
        {
            "Sid": "AllowGetBucketAcl",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::awsconfigconforms-suffix in bucket name",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "customer_org_id"
                },
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::*:role/aws-service-role/config-
conforms.amazonaws.com/AWSServiceRoleForConfigConforms"
                }
            }
        }
    ]
}
```

> **Note**
>
> 在组织中部署合规包时，传输 Amazon S3 存储桶的名称应以 `awsconfigconforms` 开头。

区域支持

以下区域支持一致性包。

区域名称	区域	端点	协议	
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS	
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS	
美国西部（加利福尼亚北部）	us-west-1	config.us-west-1.amazonaws.com	HTTPS	
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS	
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS	
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS	
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS	
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS	
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS	

区域名称	区域	端点	协议
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

以下区域支持跨 AWS 组织成员账户部署合规包。

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS
美国西部（加利福尼亚北部）	us-west-1	config.us-west-1.amazonaws.com	HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

AWS Config 在一致性包中进行流程检查

流程检查是一种 AWS Config 规则，允许您跟踪需要作为一致性包一部分进行验证的外部和内部任务。可以将这些检查添加到现有合规包或新的合规包中。您可以在一个位置跟踪所有合规性，包括 AWS Config持续时间和手动检查。

通过流程检查，您可以在单个位置列出要求和操作的合规性。这些流程检查有助于扩大基于合规制度的合规包的覆盖范围。您可以通过添加新的流程检查来进一步扩展合规包，以跟踪需要手动验证和跟踪的流程和操作。这使合规包能够成为提供有关 AWS Config合规制度持续时间和手动流程的详细信息的模板。

您可以将合规包中与资源配置更改无关的流程的合规性作为流程检查进行跟踪和管理。例如，您可以添加流程检查来跟踪将媒体备份存储在异地位置的 PCI-DSS 合规性要求。您将根据 PCI-DSS 指南或贵组织的指导手动评估其合规性。

地区可用性：在所有提供一致性包 AWS 区域 的地方，都可以使用 AWS Config 一致性包进行流程检查。有关更多信息，请参阅 区域支持。

主题

- 用于创建流程检查的样本合规包模板
- 在合规包中包括流程检查
- 更改流程检查的合规性状态
- 查看和编辑流程检查（控制台）

用于创建流程检查的样本合规包模板

```
################################################################################
#
#  Conformance Pack template for process check
#
################################################################################
Resources:
  AWSConfigProcessCheck:
    Properties:
      ConfigRuleName: RuleName
      Description: Description of Rule
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

查看两个示例模板，即 CIS AWS 基金会运营最佳实践基准 v1.4 第 1 级 模板和 CIS AWS 基金会运营最佳实践基准 v1.4 第 2 级 模板。

在合规包中包括流程检查

1. 在合规包模板中添加流程检查。请参阅前面的示例模板。

```
Resources:
  ConfigEnabledAllRegions:
```

```
    Properties:
      ConfigRuleName: Config-Enabled-All-Regions
      Description: Ensure AWS Config is enabled in all Regions.
      Source:
        Owner: AWS
        SourceIdentifier: AWS_CONFIG_PROCESS_CHECK
    Type: AWS::Config::ConfigRule
```

2. 输入流程检查的名称。
3. 输入流程检查的描述。
4. 从 AWS 管理控制台部署合规包。有关更多信息，请参阅 使用 AWS Config 控制台部署一致性包。

> **Note**
>
> 您可以使用命令行界面 (AWS CLI) 部署合规包。有关更多信息，请参阅 使用 AWS Command Line Interface部署一致性包。

更改流程检查的合规性状态

更改流程检查的合规性状态（控制台）

要更改流程的合规性状态，请检查（控制台）

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 导航到 “ AWS Config 规则” 页面。
3. 选择您在模板中指定的流程检查的名称，以及合规包中的标识符。

> **Note**
>
> 来自同一个合规包的所有流程检查都有相同的后缀。

4. 在规则详细信息页面上，您无法编辑规则，但可以编辑规则的合规性。在“手动合规性”部分中，选择编辑合规性。
5. 从下拉列表中选择相应的合规性。
6. （可选）输入合规性状态的描述。

7. 选择保存。

更改流程检查的合规性状态 (CLI)

更改流程检查的合规状态 (CLI)

您可以使用 AWS 命令行界面 (AWS CLI) 更新合规包中的流程检查的合规性。

要在本地计算机 AWS CLI 上安装，请参阅AWS CLI 用户指南中的安装 AWS CLI。

如有必要`AWS Config ure`，键入 AWS CLI 将配置为使用提供 AWS Config 一致性包的 AWS 区域。

1. 打开命令提示符或终端窗口。
2. 输入以下命令以更新流程的合规性`ComplianceResourceId`，检查您的位置`Account ID`，并包括您的规则名称。

```
aws configservice put-external-evaluation --config-rule-
name process-check-rule-name  --external-evaluation
 ComplianceResourceType=AWS::::Account,ComplianceResourceId=Account
 ID,ComplianceType=NON_COMPLIANT,OrderingTimestamp=2020-12-17T00:10:00.000Z
```

3. 按 Enter 键运行命令。

更改流程检查的合规性状态 (API)

更改流程检查的合规性状态 (API)

部署完成后，要更新流程检查的评估和合规性，请使用 `PutExternalEvaluation` API。有关更多信息，请参阅PutExternal评估。

查看和编辑流程检查（控制台）

只有在流程检查中添加了合规性状态后，您才能查看流程检查。选择具体的合规包以查看该合规包中的所有流程检查。在这里，您可以看到处于合规和不合规状态的流程检查列表。

由于这是一项服务相关规则，因此您无法通过规则详细信息页面编辑流程检查。

> **Note**
>
> 但是，您可以通过选择 “编辑合规性”，然后从 “合规”、“不合规” 或 “不适用” 中选择相应的值来更新流程检查的合规性。

您可以在添加流程检查的合规包中编辑或从中删除流程检查。

一致性包示例模板

在 AWS Config 控制台中可以看到以下几个合规包 YAML 模板。在每个一致性包模板中，您可以使用一个或多个 AWS Config 规则和修正操作。一致性包中列出的 AWS Config 规则可以是 AWS Config 托管规则和/或 AWS Config 自定义规则。您可以从 GitHub 下载所有合规包模板。

> **Important**
>
> 一致性包提供了一个通用的合规性框架，可帮助您使用托管或自定义 AWS Config 规则和 AWS Config 修正操作来创建安全性、运营或成本优化监管检查。AWS 一致性包示例模板旨在帮助您创建您自己的一致性包，其中包含适合您的环境的不同或附加规则、输入参数和修正操作。示例模板（包括与合规性标准和行业基准相关的模板）的设计目的不是为了确保您符合特定的监管标准。它们既不能替代您的内部工作，也无法保证您会通过合规性评估。

> **Note**
>
> 建议您在部署合规包之前查看部署合规包的区域中可用的规则（按区域可用性列出的 AWS Config 托管规则列表），并修改该区域尚不可用的规则模板。

主题

- AWS Control Tower 探测防护机制合规包
- ABS CCIG 2.0 重要工作负载操作最佳实践
- ABS CCIG 2.0 标准工作负载操作最佳实践
- ACSC Essential 8 操作最佳实践
- ACSC ISM 操作最佳实践
- 人工智能和机器学习操作最佳实践

- Amazon API Gateway 操作最佳实践
- Amazon 最佳运营实践 CloudWatch
- Amazon DynamoDB 操作最佳实践
- Amazon S3 操作最佳实践
- APRA CPG 234 操作最佳实践
- 资产管理操作最佳实践
- AWS Backup操作最佳实践
- AWS Identity And Access Management 操作最佳实践
- Well-Architecte AWS d 框架可靠性支柱的运营最佳实践
- Well-Architecte AWS d Framework 安全支柱的运营最佳实践
- BCP 和 DR 操作最佳实践
- BNM RMiT 操作最佳实践
- 加拿大网络安全中心 (CCCS) Medium Cloud Control Profile 操作最佳实践
- CIS AWS 基金会运营最佳实践基准 v1.4 第 1 级
- CIS AWS 基金会运营最佳实践基准 v1.4 第 2 级
- CIS 关键安全控制 v8 IG1 操作最佳实践
- CIS 关键安全控制 v8 IG2 操作最佳实践
- CIS 关键安全控制 v8 IG3 操作最佳实践
- CIS Top 20 操作最佳实践
- CISA 网络基本要素操作最佳实践
- 刑事司法信息服务 (CJIS) 操作最佳实践
- CMMC Level 1 操作最佳实践
- CMMC Level 2 操作最佳实践
- CMMC Level 3 操作最佳实践
- CMMC Level 4 操作最佳实践
- CMMC Level 5 操作最佳实践
- CMMC 2.0 Level 1 操作最佳实践
- CMMC 2.0 Level 2 操作最佳实践
- 计算服务操作最佳实践
- 数据弹性操作最佳实践

- 数据库服务操作最佳实践
- 数据湖和分析服务操作最佳实践
- DevOps 操作最佳实践
- EC2 操作最佳实践
- 加密和密钥管理操作最佳实践
- 适用于 SME 的 ENISA 网络安全指南操作最佳实践
- Esquema Nacional de Seguridad (ENS) Low 操作最佳实践
- Esquema Nacional de Seguridad (ENS) Medium 操作最佳实践
- Esquema Nacional de Seguridad (ENS) High 操作最佳实践
- FDA 联邦法规第 21 篇第 11 部分操作最佳实践
- FedRAMP(Low) 操作最佳实践
- FedRAMP(Moderate) 操作最佳实践
- FFIEC 操作最佳实践
- 德国云计算合规性条件目录 (C5) 操作最佳实践
- 《格雷姆-里奇-布里利法案》(GLBA) 操作最佳实践
- GxP 欧盟附件 11 操作最佳实践
- HIPAA 安全操作最佳实践
- IRS 1075 操作最佳实践
- K-ISMS 操作最佳实践
- 负载平衡操作最佳实践
- 日志记录操作最佳实践
- 管理和治理服务操作最佳实践
- MAS 第 655 号通知操作最佳实践
- MAS TRMG 操作最佳实践
- 监控操作最佳实践
- NBC TRMG 操作最佳实践
- NERC CIP BCSI 操作最佳实践
- NCSC 云安全原则操作最佳实践
- NCSC 网络评估框架操作最佳实践
- 联网和内容交付服务操作最佳实践

- NIST 800-53 rev 4 操作最佳实践
- NIST 800-53 rev 5 操作最佳实践
- NIST 800 171 操作最佳实践
- NIST 800 172 操作最佳实践
- NIST 800 181 操作最佳实践
- NIST 1800 25 操作最佳实践
- NIST CSF 操作最佳实践
- NIST 隐私框架 v1.0 操作最佳实践
- NYDFS 23 操作最佳实践
- NZISM 操作最佳实践
- PCI DSS 3.2.1 操作最佳实践
- 可公开访问资源操作最佳实践
- 印度储备银行 UCB 网络安全框架操作最佳实践
- RBI MD-ITF 操作最佳实践
- 安全性、身份和合规性操作最佳实践
- 无服务器操作最佳实践
- 存储服务操作最佳实践
- SWIFT CSP 操作最佳实践
- Amazon Elastic Container Service (Amazon ECS) 安全最佳实践
- Amazon Elastic File System (Amazon EFS) 安全最佳实践
- Amazon Elastic Kubernetes Service (Amazon EKS) 安全最佳实践
- Amazon 安全最佳实践 CloudFront
- Amazon OpenSearch 服务安全最佳实践
- Amazon Redshift 安全最佳实践
- Amazon Relational Database Service (Amazon RDS) 安全最佳实践
- AWS Auto Scaling安全最佳实践
- AWS CloudTrail安全最佳实践
- AWS CodeBuild安全最佳实践
- Amazon ECR 安全最佳实践
- AWS Lambda安全最佳实践

- AWS Network Firewall安全最佳实践
- Amazon 安全最佳实践 SageMaker
- AWS Secrets Manager安全最佳实践
- AWS WAF安全最佳实践
- 具有修正操作的示例模板

AWS Control Tower 探测防护机制合规包

该模板可在 GitHub 上找到：AWS Control Tower 探测防护机制合规包。

ABS CCIG 2.0 重要工作负载操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了澳大利亚统计局云计算实施指南 2.0-材料工作负载与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 ABS 云计算实施指南控件相关。一个 ABS 云计算实施指南控制可以与多个 Config 规则相关。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	AWS Config 规则	指南
section4a-govern-the-cloud-2-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4a-govern-the-cloud-2-material-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其

控制 ID	AWS Config 规则	指南
		进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector 、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	AWS Config 规则	指南
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
section4a-govern-the-cloud-3-material-workloads	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
section4a-govern-the-cloud-3-material-workloads	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
section4a-govern-the-cloud-3-standard-workloads	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-3-material-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
section4b-design-and-secure-the-cloud-3-material-workloads	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-3-material-workloads	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
section4b-design-and-secure-the-cloud-3-material-workloads	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
section4b-design-and-secure-the-cloud-3-material-workloads	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-3-material-workloads	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
section4b-design-and-secure-the-cloud-4-material-workloads	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
section4b-design-and-secure-the-cloud-4-material-workloads	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
section4b-design-and-secure-the-cloud-4-material-workloads	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-material-workloads	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
section4b-design-and-secure-the-cloud-4-material-workloads	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-material-workloads	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
section4b-design-and-secure-the-cloud-4-material-workloads	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
section4b-design-and-secure-the-cloud-4-material-workloads	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-material-workloads	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-4-material-workloads	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-4-material-workloads	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-material-workloads	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-4-material-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-4-material-workloads	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-material-workloads	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-material-workloads	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
section4b-design-and-secure-the-cloud-4-material-workloads	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
section4b-design-and-secure-the-cloud-4-material-workloads	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
section4b-design-and-secure-the-cloud-5-material-workloads	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-5-material-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-5-material-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-5-material-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-5-material-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
section4b-design-and-secure-the-cloud-6-material-workloads	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-material-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
section4b-design-and-secure-the-cloud-6-material-workloads	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-6-material-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-6-material-workloads	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-material-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-8-material-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-8-material-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-material-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-9-material-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4b-design-and-secure-the-cloud-9-material-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-9-material-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-9-material-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-9-material-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4b-design-and-secure-the-cloud-10-material-workloads	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-material-workloads	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
section4b-design-and-secure-the-cloud-10-material-workloads	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Manager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-material-workloads	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-10-material-workloads	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-10-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-material-workloads	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-10-material-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-material-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
section4b-design-and-secure-the-cloud-10-material-workloads	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
section4b-design-and-secure-the-cloud-10-material-workloads	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-material-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-10-material-workloads	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
section4b-design-and-secure-the-cloud-10-material-workloads	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-10-material-workloads	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-10-material-workloads	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
section4b-design-and-secure-the-cloud-10-material-workloads	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-10-material-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-10-material-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-material-workloads	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-10-material-workloads	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-material-workloads	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
section4b-design-and-secure-the-cloud-10-material-workloads	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
section4b-design-and-secure-the-cloud-10-material-workloads	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
section4b-design-and-secure-the-cloud-11-material-workloads	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
section4b-design-and-secure-the-cloud-11-material-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-11-material-workloads	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
section4b-design-and-secure-the-cloud-11-material-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
section4b-design-and-secure-the-cloud-11-material-workloads	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-11-material-workloads	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
section4b-design-and-secure-the-cloud-11-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4b-design-and-secure-the-cloud-11-material-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-11-material-workloads	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
section4b-design-and-secure-the-cloud-11-material-workloads	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-11-material-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-11-material-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4b-design-and-secure-the-cloud-11-material-workloads	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
section4b-design-and-secure-the-cloud-11-material-workloads	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
section4b-design-and-secure-the-cloud-14-material-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
section4b-design-and-secure-the-cloud-14-material-workloads	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
section4b-design-and-secure-the-cloud-14-material-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-material-workloads	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
section4b-design-and-secure-the-cloud-14-material-workloads	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
section4b-design-and-secure-the-cloud-14-material-workloads	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
section4b-design-and-secure-the-cloud-14-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-material-workloads	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
section4b-design-and-secure-the-cloud-14-material-workloads	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
section4b-design-and-secure-the-cloud-14-material-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
section4b-design-and-secure-the-cloud-15-material-workloads	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
section4b-design-and-secure-the-cloud-15-material-workloads	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-material-workloads	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
section4b-design-and-secure-the-cloud-15-material-workloads	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
section4c-run-the-cloud-2-material-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-2-material-workloads	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained（过程检查）	确保制定和维护事件响应计划，并将其分发给负责人。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-4-material-workloads	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
section4c-run-the-cloud-4-material-workloads	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
section4c-run-the-cloud-4-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-4-material-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
section4c-run-the-cloud-6-material-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
section4c-run-the-cloud-6-material-workloads	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
section4c-run-the-cloud-6-material-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-6-material-workloads	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认值：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow （默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

模板

该模板可在以下网址获得 GitHub：ABS CCIG 2.0 材料工作负载运营最佳实践。

ABS CCIG 2.0 标准工作负载操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了 ABS 云计算实施指南 2.0-标准工作负载与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 ABS 云计算实施指南控件相关。一个 ABS 云计算实施指南控制可以与多个 Config 规则相关。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	AWS Config 规则	指南
section4a-govern-the-cloud-2-standard-workloads	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
section4a-govern-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
section4a-govern-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	AWS Config 规则	指南
section4a-govern-the-cloud-2-standard-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
section4a-govern-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
section4a-govern-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
section4a-govern-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4a-govern-the-cloud-3-standard-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
section4a-govern-the-cloud-3-standard-workloads	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	AWS Config 规则	指南
section4a-govern-the-cloud-3-standard-workloads	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
section4a-govern-the-cloud-3-standard-workloads	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
section4a-govern-the-cloud-3-standard-workloads	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
section4b-design-and-secure-the-cloud-1-standard-workloads	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
section4b-design-and-secure-the-cloud-1-standard-workloads	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
section4b-design-and-secure-the-cloud-1-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
section4b-design-and-secure-the-cloud-1-standard-workloads	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
section4b-design-and-secure-the-cloud-1-standard-workloads	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
section4b-design-and-secure-the-cloud-1-standard-workloads	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
section4b-design-and-secure-the-cloud-1-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
section4b-design-and-secure-the-cloud-1-standard-workloads	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-1-standard-workloads	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-1-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-1-standard-workloads	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
section4b-design-and-secure-the-cloud-1-standard-workloads	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。
section4b-design-and-secure-the-cloud-1-standard-workloads	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
section4b-design-and-secure-the-cloud-1-standard-workloads	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。 OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。 OpenSearch

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-1-standard-workloads	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
section4b-design-and-secure-the-cloud-1-standard-workloads	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
section4b-design-and-secure-the-cloud-2-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
section4b-design-and-secure-the-cloud-2-standard-workloads	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
section4b-design-and-secure-the-cloud-2-standard-workloads	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-3-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
section4b-design-and-secure-the-cloud-3-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
section4b-design-and-secure-the-cloud-3-standard-workloads	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-3-standard-workloads	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-3-standard-workloads	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
section4b-design-and-secure-the-cloud-3-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
section4b-design-and-secure-the-cloud-4-standard-workloads	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
section4b-design-and-secure-the-cloud-4-standard-workloads	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
section4b-design-and-secure-the-cloud-4-standard-workloads	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
section4b-design-and-secure-the-cloud-4-standard-workloads	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
section4b-design-and-secure-the-cloud-4-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
section4b-design-and-secure-the-cloud-4-standard-workloads	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
section4b-design-and-secure-the-cloud-4-standard-workloads	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
section4b-design-and-secure-the-cloud-4-standard-workloads	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
section4b-design-and-secure-the-cloud-4-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
section4b-design-and-secure-the-cloud-4-standard-workloads	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-4-standard-workloads	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-4-standard-workloads	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-4-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-4-standard-workloads	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-4-standard-workloads	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
section4b-design-and-secure-the-cloud-4-standard-workloads	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
section4b-design-and-secure-the-cloud-4-standard-workloads	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-5-standard-workloads	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-5-standard-workloads	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-5-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-5-standard-workloads	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
section4b-design-and-secure-the-cloud-6-standard-workloads	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
section4b-design-and-secure-the-cloud-6-standard-workloads	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-6-standard-workloads	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-6-standard-workloads	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
section4b-design-and-secure-the-cloud-6-standard-workloads	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-8-standard-workloads	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
section4b-design-and-secure-the-cloud-8-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
section4b-design-and-secure-the-cloud-8-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-8-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-8-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-standard-workloads	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
section4b-design-and-secure-the-cloud-9-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-9-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-9-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4b-design-and-secure-the-cloud-10-standard-workloads	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-10-standard-workloads	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-10-standard-workloads	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
section4b-design-and-secure-the-cloud-10-standard-workloads	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
section4b-design-and-secure-the-cloud-10-standard-workloads	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-10-standard-workloads	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-10-standard-workloads	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
section4b-design-and-secure-the-cloud-10-standard-workloads	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
section4b-design-and-secure-the-cloud-10-standard-workloads	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-10-standard-workloads	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
section4b-design-and-secure-the-cloud-10-standard-workloads	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
section4b-design-and-secure-the-cloud-10-standard-workloads	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
section4b-design-and-secure-the-cloud-10-standard-workloads	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-10-standard-workloads	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
section4b-design-and-secure-the-cloud-12-standard-workloads	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
section4b-design-and-secure-the-cloud-12-standard-workloads	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
section4b-design-and-secure-the-cloud-12-standard-workloads	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-12-standard-workloads	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-12-standard-workloads	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-12-standard-workloads	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-14-standard-workloads	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
section4b-design-and-secure-the-cloud-14-standard-workloads	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
section4b-design-and-secure-the-cloud-14-standard-workloads	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
section4b-design-and-secure-the-cloud-14-standard-workloads	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
section4b-design-and-secure-the-cloud-14-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4b-design-and-secure-the-cloud-14-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
section4b-design-and-secure-the-cloud-14-standard-workloads	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-14-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
section4b-design-and-secure-the-cloud-14-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-14-standard-workloads	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
section4b-design-and-secure-the-cloud-14-standard-workloads	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
section4b-design-and-secure-the-cloud-14-standard-workloads	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
section4b-design-and-secure-the-cloud-15-standard-workloads	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-15-standard-workloads	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
section4b-design-and-secure-the-cloud-15-standard-workloads	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-15-standard-workloads	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
section4b-design-and-secure-the-cloud-15-standard-workloads	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
section4b-design-and-secure-the-cloud-15-standard-workloads	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
section4b-design-and-secure-the-cloud-15-standard-workloads	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
section4b-design-and-secure-the-cloud-15-standard-workloads	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
section4c-run-the-cloud-1-standard-workloads	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-2-standard-workloads	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
section4c-run-the-cloud-2-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4c-run-the-cloud-2-standard-workloads	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-2-standard-workloads	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4c-run-the-cloud-2-standard-workloads	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4c-run-the-cloud-2-standard-workloads	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-2-standard-workloads	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
section4c-run-the-cloud-2-standard-workloads	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
section4c-run-the-cloud-2-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4c-run-the-cloud-3-standard-workloads	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
section4c-run-the-cloud-3-standard-workloads	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
section4c-run-the-cloud-3-standard-workloads	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
section4c-run-the-cloud-3-standard-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
section4c-run-the-cloud-3-standard-workloads	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
section4c-run-the-cloud-3-standard-workloads	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
section4c-run-the-cloud-3-standard-workloads	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
section4c-run-the-cloud-3-standard-workloads	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
section4c-run-the-cloud-3-standard-workloads	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
section4c-run-the-cloud-3-standard-workloads	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
section4c-run-the-cloud-3-standard-workloads	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
section4c-run-the-cloud-3-standard-workloads	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
section4c-run-the-cloud-3-standard-workloads	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-3-standard-workloads	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
section4c-run-the-cloud-3-standard-workloads	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
section4c-run-the-cloud-4-standard-workloads	response-plan-exists-maintained （过程检查）	确保制定和维护事件响应计划，并将其分发给负责人。
section4c-run-the-cloud-5-standard-workloads	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-5-standard-workloads	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
section4c-run-the-cloud-5-standard-workloads	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
section4c-run-the-cloud-5-standard-workloads	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-5-standard-workloads	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
section4c-run-the-cloud-5-standard-workloads	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
section4c-run-the-cloud-5-standard-workloads	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
section4c-run-the-cloud-5-standard-workloads	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-6-standard-workloads	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
section4c-run-the-cloud-6-standard-workloads	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
section4c-run-the-cloud-6-standard-workloads	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
section4c-run-the-cloud-6-standard-workloads	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

模板

该模板可在以下网址获得 GitHub：ABS CCIG 2.0 标准工作负载的操作最佳实践。

ACSC Essential 8 操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了澳大利亚网络安全中心 (ACSC) 基本八项成熟度模型与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 ACSC 基本八项控件相关。一个 ACSC Essential Eight 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。配置规则的一些映射是针对高阶部分（例如“限制网络安全事件范围的缓解策略”），而不是更加规范性的部分。

此示例合规性包模板包含与 ACSC Essential 8 中控制的映射，ACSC Essential 8 由澳大利亚联邦创建，可在 ACSC | Essential Eight 上找到。有关知识共享署名 4.0 国际公共许可证下的框架许可和该框架的版权信息（包括免责声明），请访问 ACSC | 版权。

控制 ID	AWS Config 规则	指南
Application_control	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响

控制 ID	AWS Config 规则	指南
		可用性、损害安全性或消耗环境中过多的资源。
Application_control	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
Application_control	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
Application_control	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。
Application_control	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。

控制 ID	AWS Config 规则	指南
Application_control	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
Application_control	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
Patch_applications	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	AWS Config 规则	指南
Patch_applications	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
Patch_applications	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。为了协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。
Patch_applications	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
Patch_applications	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	AWS Config 规则	指南
Patch_applications	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
Patch_applications	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
Restrict_administrative_privileges	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
Restrict_administrative_privileges	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
Restrict_administrative_privileges	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
Restrict_administrative_privileges	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。
Restrict_administrative_privileges	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。

控制 ID	AWS Config 规则	指南
Restrict_administrative_privileges	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
Restrict_administrative_privileges	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。
Restrict_administrative_privileges	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。
Restrict_administrative_privileges	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
Restrict_administrative_privileges	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
Restrict_administrative_privileges	rds-instance-iam-authentication-enabled	确保在亚马逊关系数据库服务 (Amazon RDS) 实例上启用 AWS 身份和访问管理 (IAM) 身份验证，以控制对系统和资产的访问。这会强制进出数据库的网络流量使用安全套接字层 (SSL) 进行加密。您无需将用户凭证存储在数据库中，因为身份验证在外部进行管理。
Restrict_administrative_privileges	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
Restrict_administrative_privileges	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	AWS Config 规则	指南
Restrict_administrative_privileges	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
Restrict_administrative_privileges	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
Restrict_administrative_privileges	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
Patch_operating_systems	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
Multi-factor_authentication	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
Multi-factor_authentication	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
Multi-factor_authentication	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
Multi-factor_authentication	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
Multi-factor_authentication	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
Regular_backups	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
Regular_backups	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
Regular_backups	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Regular_backups	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Regular_backups	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	AWS Config 规则	指南
Regular_backups	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Regular_backups	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
Regular_backups	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	AWS Config 规则	指南
Regular_backups	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Regular_backups	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
Regular_backups	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	AWS Config 规则	指南
Regular_backups	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Regular_backups	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

模板

该模板可在以下网址获得 GitHub：ACSC Essential 8 的运营最佳实践。

ACSC ISM 操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了澳大利亚网络安全中心 (ACSC)《信息安全手册》(ISM) 2020-06 与托管 C AWS onfig 规则之间的映射示例。每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个 ISM 控件相关。一个 ISM 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

此示例合规性包模板包含与 ISM 框架内控制的映射，该框架由澳大利亚联邦创建，可在澳大利亚政府信息安全手册中找到。有关知识共享署名 4.0 国际公共许可证下的框架许可和该框架的版权信息（包括免责声明），请访问 ACSC | 版权。

控制 ID	AWS Config 规则	指南
43	response-plan-exists-maintained（过程检查）	确保制定和维护事件响应计划，并将其分发给负责人。
252	security-awareness-program-exists（过程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
261	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
261	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
261	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
298	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
298	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
298	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	AWS Config 规则	指南
298	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
380	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
459	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
459	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	AWS Config 规则	指南
459	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
459	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
459	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
459	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
459	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
459	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
459	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
459	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
459	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
459	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
459	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
459	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
459	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。
459	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
459	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	AWS Config 规则	指南
459	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
459	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
459	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
580	audit-log-policy-exists （过程检查）	制定并维护审计日志管理策略，以定义贵组织的日志记录要求。这包括但不限于审查和保留审计日志。

控制 ID	AWS Config 规则	指南
634	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
859	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
974	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
974	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
1139	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELBSecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
1173	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
1173	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
1173	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
1173	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
1173	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
1228	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
1240	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
1240	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
1271	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
1271	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	AWS Config 规则	指南
1277	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1277	rds-instance-iam-authentication-enabled	确保在亚马逊关系数据库服务 (Amazon RDS) 实例上启用 AWS 身份和访问管理 (IAM) 身份验证，以控制对系统和资产的访问。这会强制进出数据库的网络流量使用安全套接字层 (SSL) 进行加密。您无需将用户凭证存储在数据库中，因为身份验证在外部进行管理。
1277	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
1380	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	AWS Config 规则	指南
1380	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
1380	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。为了协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。
1380	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
1380	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	AWS Config 规则	指南
1380	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
1380	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
1380	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
1380	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
1380	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
1380	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。
1380	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。

控制 ID	AWS Config 规则	指南
1380	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
1380	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。
1380	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。
1380	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
1380	rds-instance-iam-authentication-enabled	确保在亚马逊关系数据库服务 (Amazon RDS) 实例上启用 AWS 身份和访问管理 (IAM) 身份验证，以控制对系统和资产的访问。这会强制进出数据库的网络流量使用安全套接字层 (SSL) 进行加密。您无需将用户凭证存储在数据库中，因为身份验证在外部进行管理。
1380	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
1380	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	AWS Config 规则	指南
1380	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
1380	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
1380	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
1388	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
1388	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
1401	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
1401	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
1401	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
1401	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
1401	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
1402	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
1404	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCreden tialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
1405	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
1405	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
1405	multi-region-cloudtrail-enabled	MULTI_REGION_CLOUD _TRAIL_ENABLED

控制 ID	AWS Config 规则	指南
1405	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
1405	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
1405	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
1405	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
1405	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
1405	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
1405	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
1405	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	AWS Config 规则	指南
1405	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
1405	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
1405	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
1405	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。

控制 ID	AWS Config 规则	指南
1405	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
1405	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
1490	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
1490	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
1490	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。
1490	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。
1490	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
1490	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
1501	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
1504	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
1504	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
1504	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
1504	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
1504	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
1509	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
1509	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
1509	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
1509	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
1509	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
1509	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	AWS Config 规则	指南
1509	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
1509	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
1509	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
1509	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
1509	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
1509	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
1509	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
1509	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
1509	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
1509	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	AWS Config 规则	指南
1509	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
1511	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
1511	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
1511	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	AWS Config 规则	指南
1511	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
1511	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
1511	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	AWS Config 规则	指南
1511	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
1511	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
1511	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	AWS Config 规则	指南
1511	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
1511	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	AWS Config 规则	指南
1511	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays （配置默认值：35）参数。实际值应反映贵组织的需求。
1511	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
1511	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
1511	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
1511	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
1511	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	AWS Config 规则	指南
1515	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
1515	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
1515	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
1515	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
1515	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
1515	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
1515	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
1515	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
1515	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
1515	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
1515	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
1515	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
1515	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
1536	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
1537	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
1537	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
1552	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
1552	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
1552	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
1552	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1552	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
1579	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	AWS Config 规则	指南
1580	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
1580	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	AWS Config 规则	指南
1580	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
1650	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
1650	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
1650	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
1650	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
1650	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
1650	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	AWS Config 规则	指南
1650	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
1650	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
1650	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
1650	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
1650	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
1650	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
1650	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
1650	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
1650	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
1650	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	AWS Config 规则	指南
1650	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
1657	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
1657	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	AWS Config 规则	指南
1657	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
1657	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。
1657	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。
1657	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
1657	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
1661	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
1661	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
1661	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
1661	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
1661	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
1661	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
1661	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
1661	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
1661	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
1661	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
1661	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	AWS Config 规则	指南
1661	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
1661	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
1661	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
1679	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
1679	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
1679	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
1679	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
1679	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
1680	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
1680	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
1680	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
1680	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
1680	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
1681	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
1681	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
1681	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
1681	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
1681	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
1683	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
1683	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
1690	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
1690	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
1690	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。为了协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。
1690	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
1690	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
1690	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
1690	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
1691	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
1691	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
1691	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。为了协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。
1691	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
1691	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
1691	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
1691	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
1693	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
1693	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
1693	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。为了协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。
1693	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
1693	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
1693	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
1693	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
1694	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
1695	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
1707	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
P1	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
P1	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
P3	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	AWS Config 规则	指南
P5	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
P7	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
P7	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
P7	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
P7	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
P8	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
P9	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
P9	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
P9	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
P9	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
P9	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
P9	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	AWS Config 规则	指南
P9	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
P9	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
P9	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
P9	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
P9	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
P9	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
P9	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
P9	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
P10	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
P10	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
P10	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略

控制 ID	AWS Config 规则	指南
P10	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
P10	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
P11	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

模板

该模板可在以下网址获得 GitHub：ACSC ISM 操作最佳实践。

人工智能和机器学习操作最佳实践

此一致性包包含基于 AI 和 ML 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：AI 和 ML 最佳运营实践。

Amazon API Gateway 操作最佳实践

该合规包包含基于其中的亚马逊 API Gateway 使用情况的 AWS Config 规则。 AWS有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon API Gateway 最佳运营实践。

Amazon 最佳运营实践 CloudWatch

此合规包包含基于亚马逊 CloudWatch 内部 AWS使用情况的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon 最佳运营实践 CloudWatch。

Amazon DynamoDB 操作最佳实践

该模板可在 GitHub 上找到：Amazon DynamoDB 操作最佳实践。

Amazon S3 操作最佳实践

该模板可在 GitHub 上找到：Amazon S3 操作最佳实践。

APRA CPG 234 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全

确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了澳大利亚审慎监管局 (APRA) CPG 234 和托 AWS 管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 APRA CPG 234 控件相关。一个 APRA CPG 234 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

此示例合规性包模板包含与 APRA CPG 234 2019 内控制的映射，APRA CPG 234 2019 由澳大利亚联邦创建，可在审慎实践指南：CPG 234 信息安全中找到。有关澳大利亚知识共享署名 3.0 许可下的框架许可以及框架的版权信息（包括免责声明），请访问 APRA | 版权。

控制 ID	AWS Config 规则	指南
36a	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
36a	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
36a	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程

控制 ID	AWS Config 规则	指南
		序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
36b	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
36b	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
36b	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
36b	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
36b	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
36b	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
36b	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	AWS Config 规则	指南
36c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
36c	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
36c	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
36c	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
36c	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
36c	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
36c	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
36c	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
36c	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
36d	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
36d	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
36d	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
36d	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
36d	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
36d	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	AWS Config 规则	指南
36d	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
36d	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
36d	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	AWS Config 规则	指南
36d	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
36d	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
36d	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
36d	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
36d	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
36d	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
36d	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
36d	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	AWS Config 规则	指南
36d	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
36d	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
36d	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
36d	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
36d	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
36d	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
36d	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCreden tialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
36d	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
36d	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
36d	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
36d	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
36d	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
36d	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
36d	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
36d	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	AWS Config 规则	指南
36d	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
36d	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
36d	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
36d	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
36d	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	AWS Config 规则	指南
36d	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
36d	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
36d	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
36d	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
36d	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
36e	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
36e	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	AWS Config 规则	指南
36e	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
36e	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
36e	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
36e	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
36e	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
36e	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
36e	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
36e	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
36e	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
36e	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
36e	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
36e	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
36e	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
36e	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
36e	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
36e	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	AWS Config 规则	指南
36e	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
36e	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
36e	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
36e	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	AWS Config 规则	指南
36e	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
36e	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
36e	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
36e	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
36e	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
36f	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
36f	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
36f	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
36f	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
36f	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
36f	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
36f	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
36f	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	AWS Config 规则	指南
36f	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
36f	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
36f	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
36f	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
36f	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
36f	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
36f	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
36f	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
36f	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
36f	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	AWS Config 规则	指南
36f	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
36f	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
36f	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
36f	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	AWS Config 规则	指南
36f	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
36f	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
36f	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
36f	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	AWS Config 规则	指南
36f	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
36f	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
36f	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
36g	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
36g	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
36g	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认值：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。

控制 ID	AWS Config 规则	指南
36h	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
36h	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
36h	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认值：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。

控制 ID	AWS Config 规则	指南
36h	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
36h	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
36h	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
36h	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
36h	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
36i	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	AWS Config 规则	指南
36i	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
36i	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
36i	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
36i	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
36i	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
36i	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	AWS Config 规则	指南
36i	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
36i	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
36i	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	AWS Config 规则	指南
36i	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
36j	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
36j	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
36j	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认值：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。
36j	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
36j	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	AWS Config 规则	指南
36j	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
36j	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
36j	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
36j	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
36j	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	AWS Config 规则	指南
36j	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
36l	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
36l	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
36l	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	AWS Config 规则	指南
36l	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
36l	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
36l	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	AWS Config 规则	指南
36l	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
36l	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
36l	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
36l	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
36l	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
36l	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	AWS Config 规则	指南
36l	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
36l	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
36l	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	AWS Config 规则	指南
36l	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
39(a)(b)(d)	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
39(a)(b)(d)	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认值：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。

控制 ID	AWS Config 规则	指南
39(a)(b)(d)	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
40	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
40	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
40	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
40	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	AWS Config 规则	指南
44a	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
44a	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
44a	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
44b	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	AWS Config 规则	指南
44b	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
44b	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
44c	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
44c	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
44c	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
44c	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
45	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
45	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
45	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
45	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
45	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
45	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCreden tialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
45	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
45	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
45	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
45	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	AWS Config 规则	指南
45	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
45	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
45	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
45	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
45	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
45	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
45	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
45	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
45	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
45	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	AWS Config 规则	指南
45	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
45	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
45	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
45	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
45	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
45	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
45	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
45	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
45	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
45	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
45	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	AWS Config 规则	指南
45	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
45	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
45	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	AWS Config 规则	指南
45	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
45	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
45	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
45	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
45	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	AWS Config 规则	指南
45	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
45	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
45	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
45	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	AWS Config 规则	指南
47c	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
47c	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
47c	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
47c	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
47c	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
47c	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
47c	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
52c	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
52c	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
52c	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
52c	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
52c	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
52c	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	AWS Config 规则	指南
52c	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
52c	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
52c	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
52c	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
52c	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
52c	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
52c	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
52c	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
52c	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
52c	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
52c	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
52c	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
52d	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
52d	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
52d	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
52d	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
52d	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
52d	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
52d	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
52d	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
52d	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
52d	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
52d	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	AWS Config 规则	指南
52d	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
52d	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
52d	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
52d	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
52d	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
52d	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
52d	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	AWS Config 规则	指南
52d	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
52d	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
52d	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
52d	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
52d	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
52e	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
52e	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
53	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
53	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
53	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
53	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
53	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
53	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
53	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
53	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
53	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
53	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	AWS Config 规则	指南
53	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
53	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
53	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	AWS Config 规则	指南
53	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
53	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
53	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
53	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	AWS Config 规则	指南
53	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
53	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
53	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
53	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	AWS Config 规则	指南
53	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
53	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
54	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	AWS Config 规则	指南
54	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （ AWS 基础安全最佳实践值：90 ）。实际值应反映贵组织的策略。
54	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
54	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
54	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
54	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
54	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	AWS Config 规则	指南
54	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
54	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
54	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
54	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
54	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
54	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
54	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
54	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
54	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
54	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
54	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
54	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
54	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
54	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
54	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
54	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
54	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
54	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
54	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
55	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
55	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
67	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
67	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
67	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
67	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
67	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
67	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
67	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
67	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
67	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
67	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
67	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
67	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
67	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
67	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
67	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
67	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
67	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
67	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
68	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
68	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
73	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
73	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AttachmentA_1(b)(h)	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	AWS Config 规则	指南
AttachmentA_1(b)(h)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AttachmentA_1(b)(h)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AttachmentA_1(b)(h)	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
AttachmentA_1(b)(h)	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AttachmentA_1(b)(h)	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
AttachmentA_1(b)(h)	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
AttachmentA_1(b)(h)	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
AttachmentA_1(b)(h)	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
AttachmentA_1(b)(h)	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AttachmentA_1(c)	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AttachmentA_1(c)	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
AttachmentA_1(e)	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector 、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AttachmentA_1(e)	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AttachmentA_1(e)	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	AWS Config 规则	指南
AttachmentA_1(e)	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AttachmentA_1(e)	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AttachmentA_1(e)	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
AttachmentA_1(e)	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	AWS Config 规则	指南
AttachmentA_1(e)	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AttachmentA_1(e)	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
AttachmentA_1(e)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AttachmentA_1(e)	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
AttachmentA_1(e)	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
AttachmentA_1(e)	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AttachmentA_1(e)	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
AttachmentA_1(e)	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
AttachmentB_1	security-awareness-program-exists（过程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。

控制 ID	AWS Config 规则	指南
AttachmentC_4	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
AttachmentC_4	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	AWS Config 规则	指南
AttachmentC_4	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
AttachmentC_4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AttachmentC_4	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AttachmentC_4	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AttachmentC_4	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
AttachmentC_4	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AttachmentC_4	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AttachmentC_4	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
AttachmentC_4	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
AttachmentC_4	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
AttachmentC_4	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AttachmentC_4	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	AWS Config 规则	指南
AttachmentC_4	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AttachmentC_4	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略

控制 ID	AWS Config 规则	指南
AttachmentC_4	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
AttachmentC_4	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AttachmentC_4	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
AttachmentC_5	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AttachmentC_5	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
AttachmentC_5	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
AttachmentC_5	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AttachmentC_5	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
AttachmentC_6	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
AttachmentC_6	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
AttachmentC_6	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AttachmentC_7(c)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
AttachmentC_7(h)	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AttachmentC_7(h)	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AttachmentC_7(h)	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
AttachmentC_7(h)	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	AWS Config 规则	指南
AttachmentC_7(h)	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AttachmentC_7(h)	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AttachmentC_7(h)	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
AttachmentC_7(h)	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AttachmentC_7(h)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
AttachmentC_7(h)	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AttachmentC_7(h)	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
AttachmentC_7(h)	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
AttachmentC_7(h)	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
AttachmentC_7(h)	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AttachmentC_7(h)	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
AttachmentC_7(i)	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCreden tialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AttachmentC_7(j)	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
AttachmentC_7(j)	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
AttachmentC_7(j)	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
AttachmentC_7(j)	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
AttachmentC_8	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
AttachmentC_8	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	AWS Config 规则	指南
AttachmentC_8	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AttachmentC_8	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
AttachmentC_8	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
AttachmentC_8	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	AWS Config 规则	指南
AttachmentC_8	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AttachmentC_8	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
AttachmentC_8	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
AttachmentC_8	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AttachmentC_8	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AttachmentC_8	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
AttachmentD_1	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
AttachmentD_1	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
AttachmentE_4	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
AttachmentE_4	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
AttachmentE_5(d)	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。

控制 ID	AWS Config 规则	指南
AttachmentE_1(a)(b)(d)	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
AttachmentE_1(a)(b)(d)	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
AttachmentE_1(a)(b)(d)	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
AttachmentE_1(a)(b)(d)	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
AttachmentE_1(a)(b)(d)	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
AttachmentE_1(a)(b)(d)	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
AttachmentE_1(a)(b)(d)	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
AttachmentE_1(a)(b)(d)	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	AWS Config 规则	指南
AttachmentE_1(a)(b)(d)	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
AttachmentE_1(a)(b)(d)	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
AttachmentE_1(a)(b)(d)	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
AttachmentE_1(a)(b)(d)	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
AttachmentE_1(a)(b)(d)	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
AttachmentE_1(a)(b)(d)	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
AttachmentE_1(a)(b)(d)	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
AttachmentE_1(a)(b)(d)	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

模板

该模板可在以下网址获得 GitHub：APRA CPG 234 操作最佳实践。

资产管理操作最佳实践

此一致性包包含基于内部 AWS资产管理的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：资产管理最佳运营实践。

AWS Backup操作最佳实践

此一致性包包含基于 AWS Backup 内部 AWS的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：的运营最佳实践 AWS Backup。

AWS Identity And Access Management 操作最佳实践

该模板可在 GitHub 上找到：AWS Identity And Access Management 操作最佳实践。

Well-Architecte AWS d 框架可靠性支柱的运营最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了亚马逊网络服务的 Well-Architected Framework 可靠性支柱与托管配置规则之间的映射示例。 AWS 每条 Config 规则都适用于特定 AWS 资源，并与支柱的一个或多个设计原则相关。一个 Well-Architected Framework 类别可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
REL-1	您如何管理服务限额和限制？ 对于基于云	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon

控制 ID	控制描述	AWS Config 规则	指南
	的工作负载架构，存在服务限额（也称为服务限制）。这些限额的存在是为了防止意外调配超出所需的资源，并限制 API 操作的请求率，以保护服务不被滥用。还存在资源限制，例如，例如光缆的比特传输速率或物理磁盘的存储量。		DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
REL-1	您如何管理服务限额和限制？ 对于基于云的工作负载架构，存在服务限额（也称为服务限制）。这些限额的存在是为了防止意外调配超出所需的资源，并限制 API 操作的请求率，以保护服务不被滥用。还存在资源限制，例如，例如光缆的比特传输速率或物理磁盘的存储量。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。

控制 ID	控制描述	AWS Config 规则	指南
REL-1	您如何管理服务限额和限制？对于基于云的工作负载架构，存在服务限额（也称为服务限制）。这些限额的存在是为了防止意外调配超出所需的资源，并限制 API 操作的请求率，以保护服务不被滥用。还存在资源限制，例如，例如光缆的比特传输速率或物理磁盘的存储量。	ecs-task-definition-memory-hard-limit	限制 Amazon Elastic Container Service (ECS) 容器可用的最大内存可确保您的资源使用量不会在容器遭到恶意访问时被滥用。
REL-2	您如何规划网络拓扑？工作负载通常存在于多个环境中。其中包括多个云环境（可公开访问和私有），可能还包括您现有的数据中心基础架构。计划必须包括网络注意事项，例如系统内和系统间连接、公有 IP 地址管理、私有 IP 地址管理和域名解析。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
REL-2	您如何规划网络拓扑？工作负载通常存在于多个环境中。其中包括多个云环境（可公开访问和私有），可能还包括您现有的数据中心基础架构。计划必须包括网络注意事项，例如系统内和系统间连接、公有 IP 地址管理、私有 IP 地址管理和域名解析。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
REL-2	您如何规划网络拓扑？工作负载通常存在于多个环境中。其中包括多个云环境（可公开访问和私有），可能还包括您现有的数据中心基础架构。计划必须包括网络注意事项，例如系统内和系统间连接、公有 IP 地址管理、私有 IP 地址管理和域名解析。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
REL-5	如何在分布式系统中设计交互以缓解或抵御故障？ 分布式系统依靠通信网络来互连组件，例如服务器或服务。即使这些网络中出现数据丢失或延迟情况，您的工作负载也必须可靠运行。分布式系统组件的运行方式不得对其他组件或工作负载产生负面影响。这些最佳实践可以防止故障并缩短平均故障间隔时间 (MTBF)。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	api-gw-xray-enabled	AWS X-Ray 收集有关您的应用程序所处理的请求的数据，并提供可用于查看、筛选和深入了解这些数据的工具，以确定问题和优化机会。确保启用 X-Ray，这样您不仅可以查看有关请求和响应的详细信息，还可以查看应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	ecs-container-insights-enabled	监控是维护 Amazon 弹性容器服务 (ECS) 和您的 AWS 解决方案的可靠性、可用性和性能的重要组成部分。Container Insights 还提供诊断信息（如容器重新启动失败），以帮助您查明问题并快速解决问题。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
REL-6	如何监控工作负载资源？ 日志和指标是深入了解工作负载运行状况的强大工具。您可以将工作负载配置为监控日志和指标，并在超过阈值或发生重大事件时发送通知。监控使您的工作负载能够识别何时超过低性能阈值或发生故障，因此它可以自动恢复以做出响应。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
REL-7	如何设计工作负载以适应需求变化？ 可扩展工作负载提供了自动添加或删除资源的弹性，因此它们在任何给定时间点都非常符合当前需求。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
REL-7	如何设计工作负载以适应需求变化？ 可扩展工作负载提供了自动添加或删除资源的弹性，因此它们在任何给定时间点都非常符合当前需求。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
REL-7	如何设计工作负载以适应需求变化？ 可扩展工作负载提供了自动添加或删除资源的弹性，因此它们在任何给定时间点都非常符合当前需求。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
REL-8	您如何实施更改？为了部署新功能，确保工作负载和操作环境运行已知软件，并且能够以可预测的方式进行修补或更换，必须进行受控更改。如果这些更改不受控制，那么就很难预测这些更改的影响，也很难解决由此产生的问题。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
REL-8	您如何实施更改？为了部署新功能，确保工作负载和操作环境运行已知软件，并且能够以可预测的方式进行修补或更换，必须进行受控更改。如果这些更改不受控制，那么就很难预测这些更改的影响，也很难解决由此产生的问题。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
REL-8	您如何实施更改？ 为了部署新功能，确保工作负载和操作环境运行已知软件，并且能够以可预测的方式进行修补或更换，必须进行受控更改。如果这些更改不受控制，那么就很难预测这些更改的影响，也很难解决由此产生的问题。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
REL-8	您如何实施更改？ 为了部署新功能，确保工作负载和操作环境运行已知软件，并且能够以可预测的方式进行修补或更换，必须进行受控更改。如果这些更改不受控制，那么就很难预测这些更改的影响，也很难解决由此产生的问题。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays （配置默认值：35）参数。实际值应反映贵组织的需求。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	rds-snapshot-encry pted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
REL-9	您如何备份数据？ 备份数据、应用程序和配置，以满足您对恢复时间目标 (RTO) 和恢复点目标 (RPO) 的要求。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
REL-10	如何使用故障隔离来保护工作负载？ 故障隔离边界将工作负载内故障的影响限制在有限数量的组件内。边界之外的组件不受故障影响。通过使用多个故障隔离边界，您可以限制对工作负载的影响。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
REL-10	如何使用故障隔离来保护工作负载？ 故障隔离边界将工作负载内故障的影响限制在有限数量的组件内。边界之外的组件不受故障影响。通过使用多个故障隔离边界，您可以限制对工作负载的影响。	clb-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
REL-10	如何使用故障隔离来保护工作负载？ 故障隔离边界将工作负载内故障的影响限制在有限数量的组件内。边界之外的组件不受故障影响。通过使用多个故障隔离边界，您可以限制对工作负载的影响。	elbv2-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
REL-10	如何使用故障隔离来保护工作负载？ 故障隔离边界将工作负载内故障的影响限制在有限数量的组件内。边界之外的组件不受故障影响。通过使用多个故障隔离边界，您可以限制对工作负载的影响。	lambda-vpc-multi-az-check	如果您的 AWS Lambda 函数配置为连接到您账户中的虚拟私有云 (VPC)，请在至少两个不同的可用区中部署 AWS Lambda 函数，以确保在单个区域发生服务中断的情况下，您的函数可用于处理事件。

控制 ID	控制描述	AWS Config 规则	指南
REL-10	如何使用故障隔离来保护工作负载？ 故障隔离边界将工作负载内故障的影响限制在有限数量的组件内。边界之外的组件不受故障影响。通过使用多个故障隔离边界，您可以限制对工作负载的影响。	opensearch-data-node-fault-tolerance	为了实现高可用性和容错能力，Amazon OpenSearch OpenSearch 服务（服务）至少需要三个数据节点。部署具有至少三个数据节点的 OpenSearch 服务域可确保在节点出现故障时集群运行。
REL-10	如何使用故障隔离来保护工作负载？ 故障隔离边界将工作负载内故障的影响限制在有限数量的组件内。边界之外的组件不受故障影响。通过使用多个故障隔离边界，您可以限制对工作负载的影响。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
REL-10	如何使用故障隔离来保护工作负载？ 故障隔离边界将工作负载内故障的影响限制在有限数量的组件内。边界之外的组件不受故障影响。通过使用多个故障隔离边界，您可以限制对工作负载的影响。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

模板

该模板可在以下网址获得 GitHub：Well-Ar chitecte AWS d 可靠性支柱的运营最佳实践。

Well-Architecte AWS d Framework 安全支柱的运营最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了亚马逊网络服务的 Well-Architected Framework 安全支柱与托管配置规则之间的映射示例。 AWS 每条 Config 规则都适用于特定 AWS 资源，并与支柱的一个或多个设计原则相关。一个 Well-Architected Framework 类别可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
SEC-1	如何安全地操作工作负载？ 为了安全地操作您的工作负载，您必须将纲领性最佳实践应用于每个安全领域。将您在组织和工作负载级别的卓越运营中定义的要求和流程应用于所有领域。及时了解行业建议 AWS 和威胁情报可以帮助您发展威胁模型和控制目标。通过自动化安全流程、测试和验证，您可以扩大安全运营规模。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	secretsmanager-secret-periodic-rotation	此规则可确保 S AWS ecrets Manager 密钥启用定期轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。默认值为 90 天。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		

控制 ID	控制描述	AWS Config 规则	指南
SEC-2	您如何管理人员和机器的身份？在处理安全工作 AWS 负载时，您需要管理两种类型的身份。了解您需要管理和授予访问权限的身份类型有助于确保正确的身份能够在适当的条件下访问正确的资源。人类身份：您的管理员、开发人员、操作员和最终用户需要身份才能访问您的 AWS 环境和应用程序。这些是您组织的成员，或者是您与之合作的外部用户，他们通过 Web 浏览器、客户端应用程序或交互式命令行工具与您的 AWS 资源进行交互。机器身份：您的服务应用程序、操作工具和工作负载需要身份才能向 AWS 服务发出请求（例如，读取数据）。这些身份包括在您的 AWS 环境中运行的计算机，例如 Amazon EC2 实例或 AWS Lambda 函数。您还可以为需要访问权限的外部各方管理计算机身份。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
	此外，您可能还有外部 AWS 的计算机需要访问您的 AWS 环境。		
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？ 管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
SEC-3	如何管理人员和机器的权限？ 管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
SEC-3	如何管理人员和机器的权限？管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？ 管理员、最终用户或其他组件都需要访问工作负载的每个组件或资源。明确定义什么人或什么内容应该有权访问每个组件，选择适当的身份类型以及身份验证和授权方法。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
SEC-3	如何管理人员和机器的权限？ 建立通用控制措施，限制对组织中所有身份的访问。例如，您可以限制对特定 AWS 区域的访问权限，或者阻止操作员删除公共资源，例如用于中央安全团队的 IAM 角色	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls （配置默认值：True）、blockPublicPolicy （配置默认值：True）和参数 blockPublicAcls （配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SEC-3	如何管理人员和机器的权限？ 持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays（Config 默认值：90）。实际值应反映贵组织的策略。
SEC-3	如何管理人员和机器的权限？持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SEC-3	如何管理人员和机器的权限？持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
SEC-3	如何管理人员和机器的权限？持续监控突显公开和跨账户访问权限的调查结果。减少公众访问和跨账户访问，只允许需要此类访问的资源进行访问。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	控制描述	AWS Config 规则	指南
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	cw-loggroup-retent ion-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SEC-4	您如何检测和调查安全事件？从日志和指标中捕获和分析事件以获得可见性。对安全事件和潜在威胁采取行动，从而保护您的工作负载。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SEC-5	您如何保护您的网络资源？任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SEC-5	您如何保护您的网络资源？任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SEC-5	您如何保护您的网络资源？任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	ec2-instance-multiple-eni-check	此规则检查您的 Amazon Elastic Cloud (Amazon EC2) 实例是否有多个 ENI。拥有多个 ENI 可能会导致双宿主实例，即具有多个子网的实例。这可能会增加网络安全的复杂性，并引入意想不到的网络路径和访问。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls （配置默认值：True）、blockPublicPolicy （配置默认值：True）和参数 blockPublicAcls （配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SEC-5	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。
SEC-5	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
SEC-5	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SEC-5	您如何保护您的网络资源？ 任何具有某种形式网络连接（无论是互联网还是私有网络）的工作负载都需要多层防御，来帮助抵御基于外部和内部网络的威胁。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SEC-6	您如何保护自己的计算资源？工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
SEC-6	您如何保护自己的计算资源？工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ecs-container-insights-enabled	监控是维护 Amazon 弹性容器服务 (ECS) 和您的 AWS 解决方案的可靠性、可用性和性能的重要组成部分。Container Insights 还提供诊断信息（如容器重新启动失败），以帮助您查明问题并快速解决问题。
SEC-6	您如何保护自己的计算资源？工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。要协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。

控制 ID	控制描述	AWS Config 规则	指南
SEC-6	您如何保护自己的计算资源？工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
SEC-6	您如何保护自己的计算资源？工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-instance-multiple-eni-check	此规则检查您的 Amazon Elastic Cloud (Amazon EC2) 实例是否有多个 ENI。拥有多个 ENI 可能会导致双宿主实例，即具有多个子网的实例。这可能会增加网络安全的复杂性，并引入意想不到的网络路径和访问。
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
SEC-6	您如何保护自己的计算资源？工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SEC-6	您如何保护自己的计算资源？工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
SEC-6	您如何保护自己的计算资源？工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
SEC-6	您如何保护自己的计算资源？ 工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SEC-6	您如何保护自己的计算资源？工作负载中的计算资源需要多层防御，以帮助抵御外部和内部威胁。计算资源包括 EC2 实例、容器、 AWS Lambda 函数、数据库服务、物联网设备等。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SEC-8	您如何保护静态数据？通过实施多种控制措施来保护静态数据，以降低未经授权的访问或处理不当的风险。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
SEC-9	您如何保护传输中数据？ 通过实施多种控制措施来保护传输中数据，以降低未经授权的访问或丢失的风险。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

模板

该模板可在以下网址获得 GitHub：Well-Ar chitecte AWS d 安全支柱的运营最佳实践。

BCP 和 DR 操作最佳实践

此一致性包包含基于 BCP 和 DR 的 AWS Config 规则。 AWS有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：BCP 和 DR 操作最佳实践。

BNM RMiT 操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了马来西亚国家银行 (BNM) 科技风险管理 (RMiT) 和托 AWS 管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 BNM RMit 控件相关。一个 BNM RMiT 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.18	金融机构必须进行尽职调查，并评估与所使用技术相关的加密控制，以保护信息的保密性、完整性、身份验证、授权和不可否认性。如果金融机构不自行生成加密密钥，则应采取适当措施，确保建立健全的控制和流程来管理加密密钥。如果这依赖于第三方评估，金融机构应考虑这种依赖是否符合金融机构的风险偏好和承受能力。金融机构还必须适当考虑支持加密控制所需的系统资源，以及加密数据的网络流量可见性降低的风险。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.20	金融机构应根据风险等级将公有加密密钥存储在证书颁发机构颁发的证书中。与客户关联的此类证书应由认可的证书颁发机构颁发。金融机构必须确保使用此类证书的认证和签名协议的实施受到强有力的保护，以确保与用户证书相对应的私有加密密钥的使用具有法律约束力且不可辩驳。此类证书的初始颁发和后续续期必须符合行业最佳实践和适用的法律/监管规范。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.20	金融机构应根据风险等级将公有加密密钥存储在证书颁发机构颁发的证书中。与客户关联的此类证书应由认可的证书颁发机构颁发。金融机构必须确保使用此类证书的认证和签名协议的实施受到强有力的保护，以确保与用户证书相对应的私有加密密钥的使用具有法律约束力且不可辩驳。此类证书的初始颁发和后续续期必须符合行业最佳实践和适用的法律/监管规范。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
10.27	金融机构必须建立实时监控机制，以跟踪关键流程和服务的产能利用率和性能。这些监控机制应能够向管理员提供及时和切实可行的警报。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
10.27	金融机构必须建立实时监控机制，以跟踪关键流程和服务的产能利用率和性能。这些监控机制应能够向管理员提供及时和切实可行的警报。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
10.27	金融机构必须建立实时监控机制，以跟踪关键流程和服务的产能利用率和性能。这些监控机制应能够向管理员提供及时和切实可行的警报。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
10.27	金融机构必须建立实时监控机制，以跟踪关键流程和服务的产能利用率和性能。这些监控机制应能够向管理员提供及时和切实可行的警报。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
10.27	金融机构必须建立实时监控机制，以跟踪关键流程和服务的产能利用率和性能。这些监控机制应能够向管理员提供及时和切实可行的警报。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
10.27	金融机构必须建立实时监控机制，以跟踪关键流程和服务的产能利用率和性能。这些监控机制应能够向管理员提供及时和切实可行的警报。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
10.27	金融机构必须建立实时监控机制，以跟踪关键流程和服务的产能利用率和性能。这些监控机制应能够向管理员提供及时和切实可行的警报。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
10.27	金融机构必须建立实时监控机制，以跟踪关键流程和服务的产能利用率和性能。这些监控机制应能够向管理员提供及时和切实可行的警报。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
10.27	金融机构必须建立实时监控机制，以跟踪关键流程和服务的产能利用率和性能。这些监控机制应能够向管理员提供及时和切实可行的警报。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
10.34	金融机构必须确保其关键系统的网络服务可靠且没有 SPOF，以保护关键系统免遭潜在的网络故障和网络威胁的侵害。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
10.34	金融机构必须确保其关键系统的网络服务可靠且没有 SPOF，以保护关键系统免遭潜在的网络故障和网络威胁的侵害。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
10.35	金融机构必须建立实时网络带宽监控流程和相应的网络服务弹性指标，以标记任何带宽过度使用以及因带宽拥塞和网络故障造成的系统中断。这包括用于检测趋势和异常情况的流量分析。	api-gw-xray-enabled	AWS X-Ray 收集有关您的应用程序所处理的请求的数据，并提供可用于查看、筛选和深入了解这些数据的工具，以确定问题和优化机会。确保启用 X-Ray，这样您不仅可以查看有关请求和响应的详细信息，还可以查看应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。

控制 ID	控制描述	AWS Config 规则	指南
10.35	金融机构必须建立实时网络带宽监控流程和相应的网络服务弹性指标，以标记任何带宽过度使用以及因带宽拥塞和网络故障造成的系统中断。这包括用于检测趋势和异常情况的流量分析。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
10.35	金融机构必须建立实时网络带宽监控流程和相应的网络服务弹性指标，以标记任何带宽过度使用以及因带宽拥塞和网络故障造成的系统中断。这包括用于检测趋势和异常情况的流量分析。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
10.35	金融机构必须建立实时网络带宽监控流程和相应的网络服务弹性指标，以标记任何带宽过度使用以及因带宽拥塞和网络故障造成的系统中断。这包括用于检测趋势和异常情况的流量分析。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
10.36	金融机构必须确保设计和实施支持关键系统的网络服务，以保障数据的机密性、完整性和可用性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
10.36	金融机构必须确保设计和实施支持关键系统的网络服务，以保障数据的机密性、完整性和可用性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
10.36	金融机构必须确保设计和实施支持关键系统的网络服务，以保障数据的机密性、完整性和可用性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
10.36	金融机构必须确保设计和实施支持关键系统的网络服务，以保障数据的机密性、完整性和可用性。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
10.36	金融机构必须确保设计和实施支持关键系统的网络服务，以保障数据的机密性、完整性和可用性。	nlb-cross-zone-load-balancing-enabled	为网络负载均衡器 (NLB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
10.38	金融机构必须确保出于调查和取证目的将足够且相关的网络设备日志至少保留三年。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保 IAM 用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有 IAM 用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求 IAM 用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
10.51	金融机构在使用云服务时，必须对客户和交易方信息以及专有数据采取适当的保护措施，以防止未经授权的披露和访问。这应包括保留与客户和交易方信息、云端托管的专有数据和服务有关的所有数据的所有权、控制和管理，包括相关的加密密钥管理。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保 IAM 用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有 IAM 用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求 IAM 用户进行多重身份验证，从而减少账户被盗事件。
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
10.52	金融机构必须实施适当的访问控制政策，对用户（内部和外部用户，例如第三方服务提供商）进行识别、身份验证和授权。这必须涉及与未经授权访问其技术系统的风险程度相称的逻辑和物理技术访问控制	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
10.53(b)(h)(i)	在遵守第 10.52 段的规定时，金融机构应在其访问控制策略中考虑以下原则：(b) 使用“最低权限”访问权限或在“需要拥有”的基础上，仅向合法用户授予履行其职责所需的最低足够权限；(h) 限制和控制在多个用户之间共享用户 ID 和密码；(i) 控制通用用户 ID 命名惯例的使用，改用更容易识别个人身份的 ID。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
10.53(b)	在遵守第 10.52 段时，金融机构应在其访问控制政策中考虑以下原则：(b) 使用“最低权限”访问权限或在“需要拥有”的基础上，仅向合法用户授予履行其职责所需的最低足够权限；	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
10.53(b)	在遵守第 10.52 段时，金融机构应在其访问控制政策中考虑以下原则：(b) 使用“最低权限”访问权限或在“需要拥有”的基础上，仅向合法用户授予履行其职责所需的最低足够权限；	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
10.53(b)	在遵守第 10.52 段时，金融机构应在其访问控制政策中考虑以下原则：(b) 使用“最低权限”访问权限或在“需要拥有”的基础上，仅向合法用户授予履行其职责所需的最低足够权限；	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
10.53(b)	在遵守第 10.52 段时，金融机构应在其访问控制政策中考虑以下原则：(b) 使用“最低权限”访问权限或在“需要拥有”的基础上，仅向合法用户授予履行其职责所需的最低足够权限；	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
10.53(b)	在遵守第 10.52 段时，金融机构应在其访问控制政策中考虑以下原则：(b) 使用“最低权限”访问权限或在“需要拥有”的基础上，仅向合法用户授予履行其职责所需的最低足够权限；	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
10.53(b)	在遵守第 10.52 段时，金融机构应在其访问控制政策中考虑以下原则：(b) 使用“最低权限”访问权限或在“需要拥有”的基础上，仅向合法用户授予履行其职责所需的最低足够权限；	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保 IAM 用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
10.53(b)	在遵守第 10.52 段时，金融机构应在其访问控制政策中考虑以下原则：(b) 使用“最低权限”访问权限或在“需要拥有”的基础上，仅向合法用户授予履行其职责所需的最低足够权限；	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
10.53(c)(f)	在遵守第 10.52 段的规定时，金融机构应在其访问控制策略中考虑以下原则：(c) 使用有时限的访问权限，限制在特定时间段内访问，包括授予服务提供商的访问权限；(f) 对包括远程访问在内的关键活动采用更严格的身份验证	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.53(f)(h)	在遵守第 10.52 段的规定时，金融机构应在其访问控制策略中考虑以下原则：(f) 对包括远程访问在内的关键活动采用更严格的身份验证；(h) 限制和控制在多个用户之间共享用户 ID 和密码	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有 IAM 用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求 IAM 用户进行多重身份验证，从而减少账户被盗事件。
10.53(f)(h)	在遵守第 10.54 段的规定时，金融机构应在其访问控制策略中考虑以下原则：(f) 对包括远程访问在内的关键活动采用更严格的身份验证；(h) 限制和控制在多个用户之间共享用户 ID 和密码	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
10.53(f)(h)	在遵守第 10.54 段的规定时，金融机构应在其访问控制策略中考虑以下原则：(f) 对包括远程访问在内的关键活动采用更严格的身份验证；(h) 限制和控制在多个用户之间共享用户 ID 和密码	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
10.54	金融机构必须采用强大的身份验证流程来确保所用身份的真实性。身份验证机制应与功能的关键性相称，并采用这三个基本身份验证因素中的至少一个或多个，即用户知道的东西（例如密码、PIN）、用户拥有的东西（例如智能卡、安全设备）和用户的身份（例如生物识别特征，例如指纹或视网膜图案）。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有 IAM 用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求 IAM 用户进行多重身份验证，从而减少账户被盗事件。
10.54	金融机构必须采用强大的身份验证流程来确保所用身份的真实性。身份验证机制应与功能的关键性相称，并采用这三个基本身份验证因素中的至少一个或多个，即用户知道的东西（例如密码、PIN）、用户拥有的东西（例如智能卡、安全设备）和用户的身份（例如生物识别特征，例如指纹或视网膜图案）。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
10.54	金融机构必须采用强大的身份验证流程来确保所用身份的真实性。身份验证机制应与功能的关键性相称，并采用这三个基本身份验证因素中的至少一个或多个，即用户知道的东西（例如密码、PIN）、用户拥有的东西（例如智能卡、安全设备）和用户的身份（例如生物识别特征，例如指纹或视网膜图案）。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
10.55	金融机构应定期审查和调整其密码做法，以提高抵御不断演变的攻击的能力。这包括有效、安全地生成密码。必须有适当的控制措施来检查所创建密码的强度。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.56	依赖多个因素的身份验证方法通常比单因素系统更难破解。有鉴于此，我们鼓励金融机构适当地设计和实施（尤其是在高风险或“单点登录”系统中）多重身份验证 (MFA)，这种身份验证更加可靠，对欺诈行为的防御能力也更强。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有 IAM 用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求 IAM 用户进行多重身份验证，从而减少账户被盗事件。
10.56	依赖多个因素的身份验证方法通常比单因素系统更难破解。有鉴于此，我们鼓励金融机构适当地设计和实施（尤其是在高风险或“单点登录”系统中）多重身份验证 (MFA)，这种身份验证更加可靠，对欺诈行为的防御能力也更强。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
10.56	依赖多个因素的身份验证方法通常比单因素系统更难破解。有鉴于此，我们鼓励金融机构适当地设计和实施（尤其是在高风险或“单点登录”系统中）多重身份验证 (MFA)，这种身份验证更加可靠，对欺诈行为的防御能力也更强。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保 IAM 用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
10.59	金融机构必须确保 (a) 有效管理和监控对企业范围系统的访问控制；(b) 记录关键系统中的用户活动以供审核和调查。活动日志必须至少保存三年，并定期及时进行审查。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
10.60	在满足第 10.59 段的要求时，大型金融机构必须 (a) 部署身份访问管理系统，以有效管理和监控用户对企业范围系统的访问；(b) 部署自动审核工具以标记任何异常情况。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
10.60	在满足第 10.61 段的要求时，大型金融机构必须 (a) 部署身份访问管理系统，以有效管理和监控用户对企业范围系统的访问；(b) 部署自动审核工具以标记任何异常情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
10.60	在满足第 10.61 段的要求时，大型金融机构必须 (a) 部署身份访问管理系统，以有效管理和监控用户对企业范围系统的访问；(b) 部署自动审核工具以标记任何异常情况。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
10.61	金融机构必须确保关键系统不会在存在已知安全漏洞的过时系统或 end-of-life (EOL) 技术系统上运行。在这方面，金融机构必须向已确定的职能明确分配责任：(a) 持续监控和及时实施最新的补丁版本；(b) 确定生命周期即将结束的关键技术系统，以便采取进一步的补救行动。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
10.61	金融机构必须确保关键系统不会在存在已知安全漏洞的过时系统或 end-of-life (EOL) 技术系统上运行。在这方面，金融机构必须向已确定的职能明确分配责任：(a) 持续监控和及时实施最新的补丁版本；(b) 确定生命周期即将结束的关键技术系统，以便采取进一步的补救行动。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
10.61	金融机构必须确保关键系统不会在存在已知安全漏洞的过时系统或 end-of-life (EOL) 技术系统上运行。在这方面，金融机构必须向已确定的职能明确分配责任：(a) 持续监控和及时实施最新的补丁版本；(b) 确定生命周期即将结束的关键技术系统，以便采取进一步的补救行动。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
10.61	金融机构必须确保关键系统不会在存在已知安全漏洞的过时系统或 end-of-life (EOL) 技术系统上运行。在这方面，金融机构必须向已确定的职能明确分配责任：(a) 持续监控和及时实施最新的补丁版本；(b) 确定生命周期即将结束的关键技术系统，以便采取进一步的补救行动。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
10.61	金融机构必须确保关键系统不会在存在已知安全漏洞的过时系统或 end-of-life (EOL) 技术系统上运行。在这方面，金融机构必须向已确定的职能明确分配责任：(a) 持续监控和及时实施最新的补丁版本；(b) 确定生命周期即将结束的关键技术系统，以便采取进一步的补救行动。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.64(a)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，来确保以下几点：(a) 客户和交易方信息及交易的机密性和完整性	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.64(b)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(b) 通过各种渠道和设备提供的服务可靠性，同时尽可能减少服务中断	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
10.64(b)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(b) 通过各种渠道和设备提供的服务可靠性，同时尽可能减少服务中断	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
10.64(b)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(b) 通过各种渠道和设备提供的服务可靠性，同时尽可能减少服务中断	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
10.64(b)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(b) 通过各种渠道和设备提供的服务可靠性，同时尽可能减少服务中断	nlb-cross-zone-load-balancing-enabled	为平衡 NetworkLoad 器 (NLB) 启用跨区域负载平衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
10.64(b)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(b) 通过各种渠道和设备提供的服务可靠性，同时尽可能减少服务中断	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
10.64(b)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(b) 通过各种渠道和设备提供的服务可靠性，同时尽可能减少服务中断	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
10.64(b)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(b) 通过各种渠道和设备提供的服务可靠性，同时尽可能减少服务中断	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
10.64(d)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保：(d) 充足的审计跟踪记录和对异常交易的监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
10.64(e)	金融机构在提供数字服务时必须实施严格的技术安全控制措施，以确保以下几点：(e) 能够识别并恢复到事件或服务中断之前的恢复点	s3-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊简单存储服务 (S3) Simple Service 存储桶包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.7	金融机构必须部署有效的工具，以支持持续、主动监控并及时检测其技术基础设施中的异常活动。监控范围必须涵盖所有关键系统，包括支持基础设施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
11.7	金融机构必须部署有效的工具，以支持持续、主动监控并及时检测其技术基础设施中的异常活动。监控范围必须涵盖所有关键系统，包括支持基础设施。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
11.8	金融机构必须确保其网络安全操作能够持续预防和检测任何可能危及其安全控制或削弱其安全态势的情况。对于大型金融机构，这必须包括每季度对支持所有关键系统的外部和内部网络组件进行漏洞评估。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
11.8	金融机构必须确保其网络安全操作能够持续预防和检测任何可能危及其安全控制或削弱其安全态势的情况。对于大型金融机构，这必须包括每季度对支持所有关键系统的外部和内部网络组件进行漏洞评估。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
11.18(c)(f)	SOC 必须能够履行以下职能：(c) 漏洞管理；(f) 提供态势感知以检测对手和威胁，包括威胁情报分析和操作，以及监控入侵指标 (IOC)。这包括高级行为分析，以检测无签名和无文件的恶意软件，并识别可能构成安全威胁的异常情况，包括端点和网络层的异常情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
11.18(c)(f)	SOC 必须能够履行以下职能：(c) 漏洞管理；(f) 提供态势感知以检测对手和威胁，包括威胁情报分析和操作，以及监控入侵指标 (IOC)。这包括高级行为分析，以检测无签名和无文件的恶意软件，并识别可能构成安全威胁的异常情况，包括端点和网络层的异常情况。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
11.18(c)(f)	SOC 必须能够履行以下职能：(c) 漏洞管理；(f) 提供态势感知以检测对手和威胁，包括威胁情报分析和操作，以及监控入侵指标 (IOC)。这包括高级行为分析，以检测无签名和无文件的恶意软件，并识别可能构成安全威胁的异常情况，包括端点和网络层的异常情况。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
附录 5.1	定期审查所有安全设备的配置和规则设置。使用自动化工具来审查和监控配置和规则设置的更改。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
附录 5.1	定期审查所有安全设备的配置和规则设置。使用自动化工具来审查和监控配置和规则设置的更改。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
附录 5.5(b)	确保 server-to-server 外部网络连接的安全控制措施包括以下内容：(b) 使用安全隧道，例如传输层安全 (TLS) 和虚拟专用网络 (VPN) IPsec	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
附录 5.5(b)	确保 server-to-server 外部网络连接的安全控制措施包括以下内容：(b) 使用安全隧道，例如传输层安全 (TLS) 和虚拟专用网络 (VPN) IPsec	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
附录 5.5(b)	确保 server-to-server 外部网络连接的安全控制措施包括以下内容：(b) 使用安全隧道，例如传输层安全 (TLS) 和虚拟专用网络 (VPN) IPsec	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
附录 5.5(b)	确保 server-to-server 外部网络连接的安全控制措施包括以下内容：(b) 使用安全隧道，例如传输层安全 (TLS) 和虚拟专用网络 (VPN) IPsec	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
附录 5.5(b)	确保 server-to-server 外部网络连接的安全控制措施包括以下内容：(b) 使用安全隧道，例如传输层安全 (TLS) 和虚拟专用网络 (VPN) IPsec	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
附录 5.5(b)	确保 server-to-server 外部网络连接的安全控制措施包括以下内容：(b) 使用安全隧道，例如传输层安全 (TLS) 和虚拟专用网络 (VPN) IPsec	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
附录 5.5(c)	确保 server-to-server 外部网络连接的安全控制措施包括以下内容：(c) 部署具有足够外围防御和保护（例如防火墙、IPS 和防病毒软件）的登台服务器。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
附录 5.5(c)	确保 server-to-server 外部网络连接的安全控制措施包括以下内容：(c) 部署具有足够外围防御和保护（例如防火墙、IPS 和防病毒软件）的登台服务器。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
附录 5.5(c)	确保 server-to-server 外部网络连接的安全控制措施包括以下内容：(c) 部署具有足够外围防御和保护（例如防火墙、IPS 和防病毒软件）的登台服务器。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
附录 5.6	确保对服务器的远程访问的安全控制措施包括以下内容：(a) 只允许访问经过强化和锁定的端点设备；(b) 使用安全隧道，例如 TLS 和 VPN IPsec；(c) 部署具有足够外围防御和保护（例如防火墙、IPS 和防病毒软件）的“网关”服务器；以及 (d) 在远程访问失效后立即关闭相关端口。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
附录 5.6	确保对服务器的远程访问的安全控制措施包括以下内容：(a) 只允许访问经过强化和锁定的端点设备；(b) 使用安全隧道，例如 TLS 和 VPN IPsec；(c) 部署具有足够外围防御和保护（例如防火墙、IPS 和防病毒软件）的“网关”服务器；以及 (d) 在远程访问失效后立即关闭相关端口。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
附录 5.6	确保对服务器的远程访问的安全控制措施包括以下内容：(a) 只允许访问经过强化和锁定的端点设备；(b) 使用安全隧道，例如 TLS 和 VPN IPsec；(c) 部署具有足够外围防御和保护（例如防火墙、IPS 和防病毒软件）的“网关”服务器；以及 (d) 在远程访问失效后立即关闭相关端口。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
附录 5.6	确保对服务器的远程访问的安全控制措施包括以下内容：(a) 只允许访问经过强化和锁定的端点设备；(b) 使用安全隧道，例如 TLS 和 VPN IPsec；(c) 部署具有足够外围防御和保护（例如防火墙、IPS 和防病毒软件）的“网关”服务器；以及 (d) 在远程访问失效后立即关闭相关端口。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
附录 5.6	确保对服务器的远程访问的安全控制措施包括以下内容：(a) 只允许访问经过强化和锁定的端点设备；(b) 使用安全隧道，例如 TLS 和 VPN IPsec；(c) 部署具有足够外围防御和保护（例如防火墙、IPS 和防病毒软件）的“网关”服务器；以及 (d) 在远程访问失效后立即关闭相关端口。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
附录 5.6	确保对服务器的远程访问的安全控制措施包括以下内容：(a) 只允许访问经过强化和锁定的端点设备；(b) 使用安全隧道，例如 TLS 和 VPN IPsec；(c) 部署具有足够外围防御和保护（例如防火墙、IPS 和防病毒软件）的“网关”服务器；以及 (d) 在远程访问失效后立即关闭相关端口。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
附录 10 B 部分 - 1 (a)	金融机构应设计强大的云架构，并确保此类设计符合预期应用程序的相关国际标准。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
附录 10 B 部分 - 1 (b)	鼓励金融机构采用零信任原则，通过采取 “假设漏洞” 的思维方式，分层进行微分段、“默认拒绝”、“最低权限” 访问权限，并在适用时进行深入检查和持续验证，defense-in-depth 从而提供网络弹性架构。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 1 (b)	鼓励金融机构采用零信任原则，通过采取“假设漏洞”的思维方式，分层进行微分段、“默认拒绝”、“最低权限”访问权限，并在适用时进行深入检查和持续验证，defense-in-depth 从而提供网络弹性架构。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
附录 10 B 部分 - 1 (b)	鼓励金融机构采用零信任原则，通过采取“假设漏洞”的思维方式，分层进行微分段、“默认拒绝”、“最低权限”访问权限，并在适用时进行深入检查和持续验证，defense-in-depth 从而提供网络弹性架构。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 1 (b)	鼓励金融机构采用零信任原则，通过采取“假设漏洞”的思维方式，分层进行微分段、“默认拒绝”、“最低权限”访问权限，并在适用时进行深入检查和持续验证，defense-in-depth 从而提供网络弹性架构。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
附录 10 B 部分 - 1 (c)	金融机构应使用最新的网络架构方法和适当的网络设计概念和解决方案，来管理和监控精细的网络安全和集中式网络配置，以管理复杂的云网络环境。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
附录 10 B 部分 - 1 (c)	金融机构应使用最新的网络架构方法和适当的网络设计概念和解决方案，来管理和监控精细的网络安全和集中式网络配置，以管理复杂的云网络环境。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 1 (d)	金融机构应建立并利用安全和加密的通信渠道，将物理服务器、应用程序或数据迁移到云平台。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
附录 10 B 部分 - 1 (d)	金融机构应建立并利用安全和加密的通信渠道，将物理服务器、应用程序或数据迁移到云平台。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 1 (f) i)	金融机构越来越多地使应用程序编程接口 (API) 与外部应用程序服务提供商互联，这可以提高新服务的交付效率。但这也可能会增加网络攻击面，并且任何管理失误都可能会放大信息安全事件的影响。金融机构应确保其 API 受到严格的管理和控制机制的约束，其中包括以下各项：i) API 的设计应具有服务弹性，以避免单点故障的风险，并通过适当的访问控制进行安全配置；	api-gwv2-authorization-type-configured	确保您的 Amazon API Gateway v2 API 路由设置了授权类型，以防止未经授权访问底层后端资源。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 1 (f) ii)	金融机构越来越多地使应用程序编程接口 (API) 与外部应用程序服务提供商互联，这可以提高新服务的交付效率。但这也可能会增加网络攻击面，并且任何管理失误都可能会放大信息安全事件的影响。金融机构应确保对其 API 实施严格的管理和控制机制，其中包括：ii) 应对 API 进行跟踪和监控以防范网络攻击，并采取适当的事件响应措施，在 API 不再使用时及时将其停用。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 1 (f) ii)	金融机构越来越多地使应用程序编程接口 (API) 与外部应用程序服务提供商互联，这可以提高新服务的交付效率。但这也可能会增加网络攻击面，并且任何管理失误都可能会放大信息安全事件的影响。金融机构应确保对其 API 实施严格的管理和控制机制，其中包括：ii) 应对 API 进行跟踪和监控以防范网络攻击，并采取适当的事件响应措施，在 API 不再使用时及时将其停用。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
附录 10 B 部分 - 2 (b) ii)	金融机构应持续利用增强的云功能来提高云服务的安全性，并鼓励金融机构：ii) 使用不可变的基础设施实践来部署服务，通过使用最新的稳定版本软件创建新环境来降低故障风险。对云环境的持续监控应包括自动检测不可变基础设施的变化，以改善合规性审查并应对不断变化的网络攻击	cloudformation-stack-notification-check	要检测底层 AWS 资源的意外更改，请确保您的 CloudFormation 堆栈已配置为向 Amazon SNS 主题发送事件通知。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 3 (b) vi)	金融机构应确保对虚拟机和容器映像进行适当的配置、强化和监控。这包括以下各项：vi) 存储的映像受到安全监控，防止未经授权的访问和更改。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
附录 10 B 部分 - 5 (a) i)	作为有效恢复能力的一部分，金融机构应确保将现有的备份和恢复程序扩展至云服务，其中包括： i) 在云采用的规划阶段，确定并正式制定备份和恢复策略；	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 5 (a) i)	作为有效恢复能力的一部分，金融机构应确保将现有的备份和恢复程序扩展至云服务，其中包括： i) 在云采用的规划阶段，确定并正式制定备份和恢复策略；	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
附录 10 B 部分 - 5 (a) i)	作为有效恢复能力的一部分，金融机构应确保将现有的备份和恢复程序扩展至云服务，其中包括： i) 在云采用的规划阶段，确定并正式制定备份和恢复策略；	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 5 (a) i)	作为有效恢复能力的一部分，金融机构应确保将现有的备份和恢复程序扩展至云服务，其中包括： i) 在云采用的规划阶段，确定并正式制定备份和恢复策略；	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
附录 10 B 部分 - 5 (a) i)	作为有效恢复能力的一部分，金融机构应确保将现有的备份和恢复程序扩展至云服务，其中包括： i) 在云采用的规划阶段，确定并正式制定备份和恢复策略；	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 5 (a) i)	作为有效恢复能力的一部分，金融机构应确保将现有的备份和恢复程序扩展至云服务，其中包括： i) 在云采用的规划阶段，确定并正式制定备份和恢复策略；	s3-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊简单存储服务 (S3) Simple Service 存储桶包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 5 (b)	金融机构应确保定期测试备份和恢复程序，以验证恢复能力。备份程序的频率应与系统的重要性和系统的恢复点目标 (RPO) 相称。如果备份失败，金融机构应立即采取补救措施。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 5 (c) i)	金融机构应确保对虚拟机和容器进行足够的备份和恢复，包括备份配置设置（适用于 IaaS 和 PaaS，如果相关），其中包括以下内容：i) 确保能够 point-in-time 按照业务恢复目标的规定恢复虚拟机和容器；	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays （配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 5 (d) i)	金融机构应评估云服务的弹性要求，并确定与系统重要性相称的适当措施，以确保极端不利情况下的服务可用性。金融机构应考虑采取基于风险的方法，并逐步采用适当的缓解控制措施，以确保服务可用性并降低集中风险。可行的选择包括：i) 利用云服务的高可用性和冗余功能，确保生产数据中心在不同的可用区拥有冗余容量；	autoscaling-multiple-az	为确保高可用性，请确保将自动扩缩组配置为跨多个可用区。
附录 10 B 部分 - 5 (d) i)	金融机构应评估云服务的弹性要求，并确定与系统重要性相称的适当措施，以确保极端不利情况下的服务可用性。金融机构应考虑采取基于风险的方法，并逐步采用适当的缓解控制措施，以确保服务可用性并降低集中风险。可行的选择包括：i) 利用云服务的高可用性和冗余功能，确保生产数据中心在不同的可用区拥有冗余容量；	elbv2-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 5 (d) i)	金融机构应评估云服务的弹性要求，并确定与系统重要性相称的适当措施，以确保极端不利情况下的服务可用性。金融机构应考虑采取基于风险的方法，并逐步采用适当的缓解控制措施，以确保服务可用性并降低集中风险。可行的选择包括：i) 利用云服务的高可用性和冗余功能，确保生产数据中心在不同的可用区拥有冗余容量；	lambda-vpc-multi-az-check	如果您的 AWS Lambda 函数配置为连接到您账户中的虚拟私有云 (VPC)，请在至少两个不同的可用区中部署 AWS Lambda 函数，以确保在单个区域发生服务中断的情况下，您的函数可用于处理事件。
附录 10 B 部分 - 5 (d) i)	金融机构应评估云服务的弹性要求，并确定与系统重要性相称的适当措施，以确保极端不利情况下的服务可用性。金融机构应考虑采取基于风险的方法，并逐步采用适当的缓解控制措施，以确保服务可用性并降低集中风险。可行的选择包括：i) 利用云服务的高可用性和冗余功能，确保生产数据中心在不同的可用区拥有冗余容量；	nlb-cross-zone-load-balancing-enabled	为平衡 NetworkLoad 器 (NLB) 启用跨区域负载平衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 5 (d) i)	金融机构应评估云服务的弹性要求，并确定与系统重要性相称的适当措施，以确保极端不利情况下的服务可用性。金融机构应考虑采取基于风险的方法，并逐步采用适当的缓解控制措施，以确保服务可用性并降低集中风险。可行的选择包括：i) 利用云服务的高可用性和冗余功能，确保生产数据中心在不同的可用区拥有冗余容量；	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 5 (d) i)	金融机构应评估云服务的弹性要求，并确定与系统重要性相称的适当措施，以确保极端不利情况下的服务可用性。金融机构应考虑采取基于风险的方法，并逐步采用适当的缓解控制措施，以确保服务可用性并降低集中风险。可行的选择包括：i) 利用云服务的高可用性和冗余功能，确保生产数据中心在不同的可用区拥有冗余容量；	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	eks-secrets-encrypted	为了帮助保护静态数据，请确保您的 Amazon Elastic Kubernetes Service (EKS) 集群配置为加密 Kubernetes 机密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
附录 10 B 部分 - 8 (a)	金融机构应采用适当且相关的加密技术，以保护存储在云端的敏感数据的机密性和完整性。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 8 (d)	随着云采用率的提高，管理众多用于保护数据的加密密钥变得越来越复杂，并可能给金融机构带来新的挑战。金融机构应采用全面而集中的方法来管理密钥，包括使用集中式密钥管理系统，该系统能够以安全和可扩展的方式处理密钥的生成、存储和分发。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
附录 10 B 部分 - 8 (d)	随着云采用率的提高，管理众多用于保护数据的加密密钥变得越来越复杂，并可能给金融机构带来新的挑战。金融机构应采用全面而集中的方法来管理密钥，包括使用集中式密钥管理系统，该系统能够以安全和可扩展的方式处理密钥的生成、存储和分发。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 9 (a) ii)	管理平面是传统基础设施和默认支持远程访问的云计算之间的关键安全差异。该接入层很容易受到网络攻击，从而损害整个云部署的完整性。有鉴于此，金融机构应确保使用严格的控制措施来访问管理平面，其中可能包括以下内容：ii) 实施 “最低权限” 和强多因素身份验证 (MFA)，例如强密码、软令牌、特权访问管理工具和制造商检查器功能；	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 9 (a) ii)	管理平面是传统基础设施和默认支持远程访问的云计算之间的关键安全差异。该接入层很容易受到网络攻击，从而损害整个云部署的完整性。有鉴于此，金融机构应确保使用严格的控制措施来访问管理平面，其中可能包括以下内容：ii) 实施 “最低权限” 和强多因素身份验证 (MFA)，例如强密码、软令牌、特权访问管理工具和制造商检查器功能；	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有 IAM 用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求 IAM 用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 9 (a) ii)	管理平面是传统基础设施和默认支持远程访问的云计算之间的关键安全差异。该接入层很容易受到网络攻击，从而损害整个云部署的完整性。有鉴于此，金融机构应确保使用严格的控制措施来访问管理平面，其中可能包括以下内容：ii) 实施 “最低权限” 和强多因素身份验证 (MFA)，例如强密码、软令牌、特权访问管理工具和制造商检查器功能；	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 9 (a) ii)	管理平面是传统基础设施和默认支持远程访问的云计算之间的关键安全差异。该接入层很容易受到网络攻击，从而损害整个云部署的完整性。有鉴于此，金融机构应确保使用严格的控制措施来访问管理平面，其中可能包括以下内容：ii) 实施 “最低权限” 和强多因素身份验证 (MFA)，例如强密码、软令牌、特权访问管理工具和制造商检查器功能；	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
附录 10 B 部分 - 9 (a) iii)	管理平面是传统基础设施和默认支持远程访问的云计算之间的关键安全差异。该接入层很容易受到网络攻击，从而损害整个云部署的完整性。有鉴于此，金融机构应确保在访问管理平面时使用严格的控制措施，其中可能包括以下各项：iii) 对特权用户进行精细的权利分配；	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 9 (a) iii)	管理平面是传统基础设施和默认支持远程访问的云计算之间的关键安全差异。该接入层很容易受到网络攻击，从而损害整个云部署的完整性。有鉴于此，金融机构应确保在访问管理平面时使用严格的控制措施，其中可能包括以下各项：iii) 对特权用户进行精细的权利分配；	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
附录 10 B 部分 - 9 (a) iv)	管理平面是传统基础设施和默认支持远程访问的云计算之间的关键安全差异。该接入层很容易受到网络攻击，从而损害整个云部署的完整性。有鉴于此，金融机构应确保在进入管理平面时使用严格的控制措施，其中可能包括以下各项：iv) 持续监控特权用户执行的活动；	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 9 (a) iv)	管理平面是传统基础设施和默认支持远程访问的云计算之间的关键安全差异。该接入层很容易受到网络攻击，从而损害整个云部署的完整性。有鉴于此，金融机构应确保在进入管理平面时使用严格的控制措施，其中可能包括以下各项：iv) 持续监控特权用户执行的活动；	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
附录 10 B 部分 - 12 (a)	金融机构应按照本政策文件的“数据丢失防护”部分（第 11.14 至 11.16 段）的要求，保护托管在云服务中的数据，包括如果金融机构允许其员工使用自己的设备访问敏感数据，则应扩大端点覆盖范围。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 12 (a)	金融机构应按照本政策文件的“数据丢失防护”部分（第 11.14 至 11.16 段）的要求，保护托管在云服务中的数据，包括如果金融机构允许其员工使用自己的设备访问敏感数据，则应扩大端点覆盖范围。	macie-status-check	Amazon Macie 是一项数据安全服务，它使用机器学习 (ML) 和模式匹配来发现并帮助您保护 Amazon Simple Storage Service (S3) 存储桶中存储的敏感数据。
附录 10 B 部分 - 14 (c) i)	金融机构在制定其 CIRP 时应考虑以下额外措施：i) 增强其检测安全违例事件的能力，以实现有效的事件管理，包括检测暗网上的数据泄露的能力；	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
附录 10 B 部分 - 14 (c) i)	金融机构在制定其 CIRP 时应考虑以下额外措施：i) 增强其检测安全违例事件的能力，以实现有效的事件管理，包括检测暗网上的数据泄露的能力；	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

模板

该模板可在以下网址获得 GitHub：BNM RMiT 运营最佳实践。

加拿大网络安全中心 (CCCS) Medium Cloud Control Profile 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了加拿大网络安全中心 (CCCS) 中型云控制配置文件和 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CCCS 中型云控制配置文件控件相关。一个 CCCS Medium Cloud Control Profile 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(1)	AC-2(1) 账户管理 | 自动化系统账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(3)	AC-2(3) 账户管理 | 禁用非活动账户	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(3)	AC-2(3) 账户管理 | 禁用非活动账户	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2(4)	AC-2(4) 账户管理 | 自动审计操作	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
CCCS-fPBMM-AC-2(4)	AC-2(4) 账户管理 | 自动审计操作	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(4)	AC-2(4) 账户管理 | 自动审计操作	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AC-2(4)	AC-2(4) 账户管理 | 自动审计操作	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(4)	AC-2(4) 账户管理 | 自动审计操作	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
CCCS-fPBMM-AC-2(4)	AC-2(4) 账户管理 | 自动审计操作	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2(4)	AC-2(4) 账户管理 | 自动审计操作	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.A	AC-2.A 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.B	AC-2.B 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.C	AC-2.C 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.D	AC-2.D 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.E	AC-2.E 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatt erns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.F	AC-2.F 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.G	AC-2.G 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.H	AC-2.H 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.I	AC-2.I 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.J	AC-2.J 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-2.K	AC-2.K 账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-3.A	AC-3.A 强制访问权限	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-AC-4(21)	AC-4(21) 强制执行信息流 | 信息流的物理/逻辑分离	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-4(21)	AC-4(21) 强制执行信息流 | 信息流的物理/逻辑分离	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4(21)	AC-4(21) 强制执行信息流 | 信息流的物理/逻辑分离	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-4(21)	AC-4(21) 强制执行信息流 | 信息流的物理/逻辑分离	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4(21)	AC-4(21) 强制执行信息流 | 信息流的物理/逻辑分离	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
CCCS-fPBMM-AC-4(21)	AC-4(21) 强制执行信息流 | 信息流的物理/逻辑分离	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4(21)	AC-4(21) 强制执行信息流 | 信息流的物理/逻辑分离	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-4(21)	AC-4(21) 强制执行信息流 | 信息流的物理/逻辑分离	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-4(21)	AC-4(21) 强制执行信息流 | 信息流的物理/逻辑分离	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELBSecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-4.A	AC-4.A 强制执行信息流	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-AC-5.A	AC-5.A 职责分离	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-5.A	AC-5.A 职责分离	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-5.A	AC-5.A 职责分离	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-5.A	AC-5.A 职责分离	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-5.A	AC-5.A 职责分离	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-6(1)	AC-6(1) 最低权限 | 授权访问安全功能	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(1)	AC-6(1) 最低权限 | 授权访问安全功能	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-6(1)	AC-6(1) 最低权限 | 授权访问安全功能	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(1)	AC-6(1) 最低权限 | 授权访问安全功能	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
CCCS-fPBMM-AC-6(1)	AC-6(1) 最低权限 | 授权访问安全功能	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(2)	AC-6(2) 最低权限 | 非安全功能的非特权访问权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-6(2)	AC-6(2) 最低权限 | 非安全功能的非特权访问权限	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(2)	AC-6(2) 最低权限 | 非安全功能的非特权访问权限	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-AC-6(2)	AC-6(2) 最低权限 | 非安全功能的非特权访问权限	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(2)	AC-6(2) 最低权限 | 非安全功能的非特权访问权限	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
CCCS-fPBMM-AC-6(5)	AC-6(5) 最低权限 | 特权账户	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(5)	AC-6(5) 最低权限 | 特权账户	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-AC-6(5)	AC-6(5) 最低权限 | 特权账户	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(5)	AC-6(5) 最低权限 | 特权账户	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
CCCS-fPBMM-AC-6(9)	AC-6(9) 最低权限 | 审核特权功能的使用	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
CCCS-fPBMM-AC-6(9)	AC-6(9) 最低权限 | 审核特权功能的使用	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(9)	AC-6(9) 最低权限 | 审核特权功能的使用	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AC-6(9)	AC-6(9) 最低权限 | 审核特权功能的使用	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(9)	AC-6(9) 最低权限 | 审核特权功能的使用	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
CCCS-fPBMM-AC-6(9)	AC-6(9) 最低权限 | 审核特权功能的使用	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(9)	AC-6(9) 最低权限 | 审核特权功能的使用	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AC-6(10)	AC-6(10) 最低权限 | 禁止非特权用户执行特权功能	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(10)	AC-6(10) 最低权限 | 禁止非特权用户执行特权功能	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
CCCS-fPBMM-AC-6(10)	AC-6(10) 最低权限 | 禁止非特权用户执行特权功能	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6(10)	AC-6(10) 最低权限 | 禁止非特权用户执行特权功能	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
CCCS-fPBMM-AC-6(10)	AC-6(10) 最低权限 | 禁止非特权用户执行特权功能	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-6.A	AC-6.A 最低权限	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-AC-17(1)	AC-17 (1) 远程访问 | 自动监控/控制	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(2)	AC-17(2) 远程访问 | 使用加密来保护机密性/完整性	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-17(2)	AC-17(2) 远程访问 | 使用加密来保护机密性/完整性	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
CCCS-fPBMM-AC-17(2)	AC-17(2) 远程访问 | 使用加密来保护机密性/完整性	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(2)	AC-17(2) 远程访问 | 使用加密来保护机密性/完整性	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELBSecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
CCCS-fPBMM-AC-17(2)	AC-17(2) 远程访问 | 使用加密来保护机密性/完整性	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(2)	AC-17(2) 远程访问 | 使用加密来保护机密性/完整性	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-AC-17(3)	AC-17(3) 远程访问 | 托管访问控制点	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CCCS-fPBMM-AC-17(4)	AC-17(4) 远程访问 | 特权命令/访问	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17(4)	AC-17(4) 远程访问 | 特权命令/访问	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
CCCS-fPBMM-AC-17(4)	AC-17(4) 远程访问 | 特权命令/访问	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.A	AC-17.A 远程访问	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.AA	AC-17.AA 远程访问	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AC-17.B	AC-17.B 远程访问	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.A	AU-2.A 审计事件	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.B	AU-2.B 审计事件	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.C	AU-2.C 审计事件	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-2.D	AU-2.D 审计事件	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-AU-3(1)	AU-3(1) 审计记录的内容 | 其他审计信息	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CCCS-fPBMM-AU-3(1)	AU-3(1) 审计记录的内容 | 其他审计信息	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-3(1)	AU-3(1) 审计记录的内容 | 其他审计信息	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-3(1)	AU-3(1) 审计记录的内容 | 其他审计信息	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AU-3(1)	AU-3(1) 审计记录的内容 | 其他审计信息	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-3(1)	AU-3(1) 审计记录的内容 | 其他审计信息	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
CCCS-fPBMM-AU-3(1)	AU-3(1) 审计记录的内容 | 其他审计信息	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-3(1)	AU-3(1) 审计记录的内容 | 其他审计信息	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-3.A	AU-3.A 审计记录的内容	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-5.A	AU-5.A 对审计处理失败的响应	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-5.B	AU-5.B 对审计处理失败的响应	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(1)	AU-6(1) 审计审查、分析和报告 | 流程集成	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
CCCS-fPBMM-AU-6(1)	AU-6(1) 审计审查、分析和报告 | 流程集成	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(1)	AU-6(1) 审计审查、分析和报告 | 流程集成	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AU-6(1)	AU-6(1) 审计审查、分析和报告 | 流程集成	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(1)	AU-6(1) 审计审查、分析和报告 | 流程集成	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(1)	AU-6(1) 审计审查、分析和报告 | 流程集成	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-6(3)	AU-6(3) 审计审查、分析和报告 | 关联审计存储库	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-AU-7(1)	AU-7(1) 减少审计并生成报告 | 自动处理	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-8.B	AU-8.B 时间戳	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-9(2)	AU-9(2) 审计信息保护 | 在单独的物理系统/组件上进行审计备份	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-AU-9(2)	AU-9(2) 审计信息保护 | 在单独的物理系统/组件上进行审计备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-9(2)	AU-9(2) 审计信息保护 | 在单独的物理系统/组件上进行审计备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CCCS-fPBMM-AU-9.A	AU-9.A 审核信息的保护	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-9.A	AU-9.A 审核信息的保护	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-AU-9.A	AU-9.A 审核信息的保护	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-11.A	AU-11.A 审核记录保留	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
CCCS-fPBMM-AU-11.B	AU-11.B 审核记录保留	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
CCCS-fPBMM-AU-11.C	AU-11.C 审核记录保留	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.A	AU-12.A 审计生成	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-AU-12.C	AU-12.C 审计生成	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-3(5)	CA-3(5) 系统互连 | 对外部网络连接的限制	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	api-gw-xray-enabled	AWS X-Ray 收集有关您的应用程序所处理的请求的数据，并提供可用于查看、筛选和深入了解这些数据的工具，以识别问题和优化机会。确保启用 X-Ray，这样您不仅可以查看有关请求和响应的详细信息，还可以查看应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.A	CA-7.A 持续监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	api-gw-xray-enabled	AWS X-Ray 收集有关您的应用程序所处理的请求的数据，并提供可用于查看、筛选和深入了解这些数据的工具，以识别问题和优化机会。确保启用 X-Ray，这样您不仅可以查看有关请求和响应的详细信息，还可以查看应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.B	CA-7.B 持续监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	api-gw-xray-enabled	AWS X-Ray 收集有关您的应用程序所处理的请求的数据，并提供可用于查看、筛选和深入了解这些数据的工具，以识别问题和优化机会。确保启用 X-Ray，这样您不仅可以查看有关请求和响应的详细信息，还可以查看应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.C	CA-7.C 持续监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	api-gw-xray-enabled	AWS X-Ray 收集有关您的应用程序所处理的请求的数据，并提供可用于查看、筛选和深入了解这些数据的工具，以识别问题和优化机会。确保启用 X-Ray，这样您不仅可以查看有关请求和响应的详细信息，还可以查看应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.D	CA-7.D 持续监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	api-gw-xray-enabled	AWS X-Ray 收集有关您的应用程序所处理的请求的数据，并提供可用于查看、筛选和深入了解这些数据的工具，以识别问题和优化机会。确保启用 X-Ray，这样您不仅可以查看有关请求和响应的详细信息，还可以查看应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.E	CA-7.E 持续监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	api-gw-xray-enabled	AWS X-Ray 收集有关您的应用程序所处理的请求的数据，并提供可用于查看、筛选和深入了解这些数据的工具，以识别问题和优化机会。确保启用 X-Ray，这样您不仅可以查看有关请求和响应的详细信息，还可以查看应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.F	CA-7.F 持续监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	api-gw-xray-enabled	AWS X-Ray 收集有关您的应用程序所处理的请求的数据，并提供可用于查看、筛选和深入了解这些数据的工具，以识别问题和优化机会。确保启用 X-Ray，这样您不仅可以查看有关请求和响应的详细信息，还可以查看应用程序对下游 AWS 资源、微服务、数据库和 HTTP Web API 的调用的详细信息。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-7.G	CA-7.G 持续监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CA-9.A	CA-9.A 内部系统连接	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-CM-2.A	CM-2.A 基线配置	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-2.A	CM-2.A 基线配置	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CCCS-fPBMM-CM-2.A	CM-2.A 基线配置	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-2.A	CM-2.A 基线配置	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CCCS-fPBMM-CM-2.A	CM-2.A 基线配置	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-2.A	CM-2.A 基线配置	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-2.A	CM-2.A 基线配置	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-3.A	CM-3.A 配置变更控制	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-3.A	CM-3.A 配置变更控制	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-CM-3.B	CM-3.B 配置变更控制	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-3.B	CM-3.B 配置变更控制	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-CM-3.C	CM-3.C 配置变更控制	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-3.C	CM-3.C 配置变更控制	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-CM-3.D	CM-3.D 配置变更控制	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-3.D	CM-3.D 配置变更控制	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-CM-3.E	CM-3.E 配置变更控制	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-3.E	CM-3.E 配置变更控制	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-CM-3.F	CM-3F 配置变更控制	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-3.F	CM-3F 配置变更控制	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-CM-3.G	CM-3.G 配置变更控制	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-3.G	CM-3.G 配置变更控制	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
CCCS-fPBMM-CM-5(1)	CM-5(1) 变更访问限制 | 强制自动访问/审计	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5(5)	CM-5(5) 变更访问限制 | 限制生产/操作权限	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-5.A	CM-5.A 变更访问限制	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6(1)	CM-6(1) 配置设置 | 自动集中管理/应用程序/验证	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6(1)	CM-6(1) 配置设置 | 自动集中管理/应用程序/验证	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CCCS-fPBMM-CM-6(1)	CM-6(1) 配置设置 | 自动集中管理/应用程序/验证	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CCCS-fPBMM-CM-6.A	CM-6.A 配置设置	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CCCS-fPBMM-CM-6.B	CM-6.B 配置设置	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CCCS-fPBMM-CM-6.C	CM-6.C 配置设置	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CCCS-fPBMM-CM-6.D	CM-6.D 配置设置	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-7.A	CM-7.A 最少功能	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CCCS-fPBMM-CM-7.A	CM-7.A 最少功能	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-7.B	CM-7.B 最少功能	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CCCS-fPBMM-CM-7.B	CM-7.B 最少功能	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-8(1)	CM-8(1) 信息系统组件清单 | 安装/移除期间更新	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CM-8(1)	CM-8(1) 信息系统组件清单 | 安装/移除期间更新	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-8(2)	CM-8(2) 信息系统组件清单 | 自动维护	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CM-8(2)	CM-8(2) 信息系统组件清单 | 自动维护	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-8(3)	CM-8(3) 信息系统组件清单 | 自动检测未经授权的组件	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CM-8(3)	CM-8(3) 信息系统组件清单 | 自动检测未经授权的组件	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-8(3)	CM-8(3) 信息系统组件清单 | 自动检测未经授权的组件	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-CM-8(3)	CM-8(3) 信息系统组件清单 | 自动检测未经授权的组件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-8.A	CM-8.A 信息系统组件清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CM-8.A	CM-8.A 信息系统组件清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-8.B	CM-8.B 信息系统组件清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CM-8.B	CM-8.B 信息系统组件清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-8.C	CM-8.C 信息系统组件清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CM-8.C	CM-8.C 信息系统组件清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-8.D	CM-8.D 信息系统组件清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CM-8.D	CM-8.D 信息系统组件清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CM-8.E	CM-8.E 信息系统组件清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-CM-8.E	CM-8.E 信息系统组件清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	rds-cluster-multi-az-enabled	Amazon Relationa l Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(5)	CP-2(5) 应急计划 | 继续执行基本任务/业务职能	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-CP-2(6)	CP-2(6) 应急计划 | 备用处理/存储地点	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(6)	CP-2(6) 应急计划 | 备用处理/存储地点	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CCCS-fPBMM-CP-2(6)	CP-2(6) 应急计划 | 备用处理/存储地点	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(6)	CP-2(6) 应急计划 | 备用处理/存储地点	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(6)	CP-2(6) 应急计划 | 备用处理/存储地点	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2(6)	CP-2(6) 应急计划 | 备用处理/存储地点	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-CP-2.A	CP-2.A 应急计划	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.A	CP-2.A 应急计划	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CCCS-fPBMM-CP-2.A	CP-2.A 应急计划	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CCCS-fPBMM-CP-2.A	CP-2.A 应急计划	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.A	CP-2.A 应急计划	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CCCS-fPBMM-CP-2.A	CP-2.A 应急计划	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.A	CP-2.A 应急计划	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.A	CP-2.A 应急计划	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-CP-2.B	CP-2.B 应急计划	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.B	CP-2.B 应急计划	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CCCS-fPBMM-CP-2.B	CP-2.B 应急计划	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CCCS-fPBMM-CP-2.B	CP-2.B 应急计划	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.B	CP-2.B 应急计划	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CCCS-fPBMM-CP-2.B	CP-2.B 应急计划	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.B	CP-2.B 应急计划	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.B	CP-2.B 应急计划	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-CP-2.C	CP-2.C 应急计划	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.C	CP-2.C 应急计划	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CCCS-fPBMM-CP-2.C	CP-2.C 应急计划	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CCCS-fPBMM-CP-2.C	CP-2.C 应急计划	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.C	CP-2.C 应急计划	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CCCS-fPBMM-CP-2.C	CP-2.C 应急计划	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.C	CP-2.C 应急计划	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.C	CP-2.C 应急计划	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-CP-2.D	CP-2.D 应急计划	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.D	CP-2.D 应急计划	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CCCS-fPBMM-CP-2.D	CP-2.D 应急计划	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CCCS-fPBMM-CP-2.D	CP-2.D 应急计划	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.D	CP-2.D 应急计划	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CCCS-fPBMM-CP-2.D	CP-2.D 应急计划	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.D	CP-2.D 应急计划	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.D	CP-2.D 应急计划	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-CP-2.E	CP-2.E 应急计划	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.E	CP-2.E 应急计划	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CCCS-fPBMM-CP-2.E	CP-2.E 应急计划	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CCCS-fPBMM-CP-2.E	CP-2.E 应急计划	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.E	CP-2.E 应急计划	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CCCS-fPBMM-CP-2.E	CP-2.E 应急计划	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.E	CP-2.E 应急计划	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.E	CP-2.E 应急计划	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-CP-2.F	CP-2.F 应急计划	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.F	CP-2.F 应急计划	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CCCS-fPBMM-CP-2.F	CP-2.F 应急计划	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CCCS-fPBMM-CP-2.F	CP-2.F 应急计划	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.F	CP-2.F 应急计划	rds-cluster-multi-az-enabled	Amazon Relationa l Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CCCS-fPBMM-CP-2.F	CP-2.F 应急计划	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.F	CP-2.F 应急计划	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.F	CP-2.F 应急计划	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-CP-2.G	CP-2.G 应急计划	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.G	CP-2.G 应急计划	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CCCS-fPBMM-CP-2.G	CP-2.G 应急计划	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CCCS-fPBMM-CP-2.G	CP-2.G 应急计划	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.G	CP-2.G 应急计划	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CCCS-fPBMM-CP-2.G	CP-2.G 应急计划	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.G	CP-2.G 应急计划	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-2.G	CP-2.G 应急计划	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-6(1)	CP-6(1) 备用存储站点 | 与主站点分离	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-6(2)	CP-6(2) 备用存储站点 | 恢复时间/恢复点目标	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-6.A	CP-6.A 备用存储站点	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-6.B	CP-6.B 备用存储站点	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays （配置默认值：35）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(3)	CP-9(3) 信息系统备份 | 独立存储关键信息	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CCCS-fPBMM-CP-9(7)	CP-9(7) 信息系统备份 | 双重授权	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9(7)	CP-9(7) 信息系统备份 | 双重授权	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-9.A	CP-9.A 信息系统备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-9.AA	CP-9.AA 信息系统备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-9.B	CP-9.B 信息系统备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-9.C	CP-9.C 信息系统备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CCCS-fPBMM-CP-9.D	CP-9.D 信息系统备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CCCS-fPBMM-CP-10.A	CP-10.A 信息系统的恢复和重建	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-2(1)	IA-2(1) 识别和身份验证（组织用户）| 特权账户的网络访问权限	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-2(1)	IA-2(1) 识别和身份验证（组织用户）| 特权账户的网络访问权限	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-2(1)	IA-2(1) 识别和身份验证（组织用户）| 特权账户的网络访问权限	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
CCCS-fPBMM-IA-2(3)	IA-2(3) 识别和身份验证（组织用户）| 特权账户的本地访问权限	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-2(3)	IA-2(3) 识别和身份验证（组织用户）| 特权账户的本地访问权限	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
CCCS-fPBMM-IA-2(3)	IA-2(3) 识别和身份验证（组织用户）| 特权账户的本地访问权限	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-2(8)	IA-2(8) 识别和身份验证（组织用户）| 特权账户的网络访问权限 - 防重播	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-2(8)	IA-2(8) 识别和身份验证（组织用户）| 特权账户的网络访问权限 - 防重播	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-2(8)	IA-2(8) 识别和身份验证（组织用户）| 特权账户的网络访问权限 - 防重播	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
CCCS-fPBMM-IA-2(11)	IA-2(11) 识别和身份验证（组织用户）| 远程访问 - 独立设备	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-2(11)	IA-2(11) 识别和身份验证（组织用户）| 远程访问 - 独立设备	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
CCCS-fPBMM-IA-2(11)	IA-2(11) 识别和身份验证（组织用户）| 远程访问 - 独立设备	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-2.A	IA-2.A 识别和身份验证（组织用户）	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-2.A	IA-2.A 识别和身份验证（组织用户）	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-2.A	IA-2.A 识别和身份验证（组织用户）	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-2.A	IA-2.A 识别和身份验证（组织用户）	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
CCCS-fPBMM-IA-4(4)	IA-4(4) 标识符管理 | 识别用户状态	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.A	IA-4.A 标识符管理	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.A	IA-4.A 标识符管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.A	IA-4.A 标识符管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
CCCS-fPBMM-IA-4.B	IA-4.B 标识符管理	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.B	IA-4.B 标识符管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.B	IA-4.B 标识符管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
CCCS-fPBMM-IA-4.C	IA-4.C 标识符管理	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.C	IA-4.C 标识符管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.C	IA-4.C 标识符管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
CCCS-fPBMM-IA-4.D	IA-4.D 标识符管理	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.D	IA-4.D 标识符管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.D	IA-4.D 标识符管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
CCCS-fPBMM-IA-4.E	IA-4.E 标识符管理	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.E	IA-4.E 标识符管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-4.E	IA-4.E 标识符管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5(1)	IA-5(1) 身份验证器管理 | 基于密码的身份验证	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5(2)	IA-5(2) 身份验证器管理 | 基于 PKI 的身份验证	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
CCCS-fPBMM-IA-5(2)	IA-5(2) 身份验证器管理 | 基于 PKI 的身份验证	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5(4)	IA-5(4) 身份验证器管理 | 自动支持密码强度确定	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5(8)	IA-5(8) 身份验证器管理 | 多个信息系统账户	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
CCCS-fPBMM-IA-5(8)	IA-5(8) 身份验证器管理 | 多个信息系统账户	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5(8)	IA-5(8) 身份验证器管理 | 多个信息系统账户	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.A	IA-5.A 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.A	IA-5.A 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.A	IA-5.A 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.A	IA-5.A 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.B	IA-5.B 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.B	IA-5.B 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.B	IA-5.B 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.B	IA-5.B 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.C	IA-5.C 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.C	IA-5.C 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.C	IA-5.C 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.C	IA-5.C 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.D	IA-5.D 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.D	IA-5.D 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.D	IA-5.D 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.D	IA-5.D 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.E	IA-5.E 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.E	IA-5.E 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.E	IA-5.E 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.E	IA-5.E 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.F	IA-5.F 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.F	IA-5.F 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.F	IA-5.F 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.F	IA-5.F 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.G	IA-5.G 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.G	IA-5.G 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.G	IA-5.G 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.G	IA-5.G 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.H	IA-5.H 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.H	IA-5.H 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.H	IA-5.H 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.H	IA-5.H 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.I	IA-5.I 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.I	IA-5.I 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.I	IA-5.I 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.I	IA-5.I 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.J	IA-5.J 身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.J	IA-5.J 身份验证器管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
CCCS-fPBMM-IA-5.J	IA-5.J 身份验证器管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-IA-5.J	IA-5.J 身份验证器管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
CCCS-fPBMM-IR-6(1)	IR-6(1) 事件报告 | 自动报告	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MA-3.A	MA-3.A 维护工具	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-MA-3.A	MA-3.A 维护工具	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MA-4(1)	MA-4(1) 非本地维护 | 审计和审查	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-MP-2.A	MP-2.A 媒体访问权限	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-RA-5.A	RA-5.A 漏洞扫描	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-RA-5.B	RA-5.B 漏洞扫描	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-RA-5.C	RA-5.C 漏洞扫描	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-RA-5.D	RA-5.D 漏洞扫描	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-RA-5.E	RA-5.E 漏洞扫描	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SA-10(1)	SA-10(1) 开发人员配置管理 | 软件/固件完整性验证	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-SC-5.A	SC-5.A 拒绝服务防护	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-5.A	SC-5.A 拒绝服务防护	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-SC-6.A	SC-6.A 资源可用性	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-6.A	SC-6.A 资源可用性	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CCCS-fPBMM-SC-6.A	SC-6.A 资源可用性	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-6.A	SC-6.A 资源可用性	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-6.A	SC-6.A 资源可用性	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-6.A	SC-6.A 资源可用性	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-6.A	SC-6.A 资源可用性	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-6.A	SC-6.A 资源可用性	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(3)	SC-7(3) 边界保护 | 接入点	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(4)	SC-7(4) 边界保护 | 外部电信服务	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-SC-7(5)	SC-7(5) 边界保护 | 默认拒绝/允许按例外处理	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(5)	SC-7(5) 边界保护 | 默认拒绝/允许按例外处理	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-7(5)	SC-7(5) 边界保护 | 默认拒绝/允许按例外处理	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(5)	SC-7(5) 边界保护 | 默认拒绝/允许按例外处理	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-SC-7(7)	SC-7(7) 边界保护 | 防止为远程设备分割隧道	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.A	SC-7.A 边界保护	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.B	SC-7.B 边界保护	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-7.C	SC-7.C 边界保护	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CCCS-fPBMM-SC-8(1)	SC-8(1) 传输机密性和完整性 | 加密或备用物理保护	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-8(1)	SC-8(1) 传输机密性和完整性 | 加密或备用物理保护	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-8(1)	SC-8(1) 传输机密性和完整性 | 加密或备用物理保护	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-8(1)	SC-8(1) 传输机密性和完整性 | 加密或备用物理保护	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-8(1)	SC-8(1) 传输机密性和完整性 | 加密或备用物理保护	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELBSecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
CCCS-fPBMM-SC-8(1)	SC-8(1) 传输机密性和完整性 | 加密或备用物理保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-8(1)	SC-8(1) 传输机密性和完整性 | 加密或备用物理保护	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-8(1)	SC-8(1) 传输机密性和完整性 | 加密或备用物理保护	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-8(1)	SC-8(1) 传输机密性和完整性 | 加密或备用物理保护	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-8.A	SC-8.A 传输机密性和完整性	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-8.A	SC-8.A 传输机密性和完整性	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
CCCS-fPBMM-SC-8.A	SC-8.A 传输机密性和完整性	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-8.A	SC-8.A 传输机密性和完整性	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
CCCS-fPBMM-SC-8.A	SC-8.A 传输机密性和完整性	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-8.A	SC-8.A 传输机密性和完整性	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-8.A	SC-8.A 传输机密性和完整性	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-8.A	SC-8.A 传输机密性和完整性	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-8.A	SC-8.A 传输机密性和完整性	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-12(1)	SC-12(1) 加密密钥的建立和管理 | 可用性	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
CCCS-fPBMM-SC-12(2)	SC-12(2) 加密密钥的建立和管理 | 对称密钥	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-12(2)	SC-12(2) 加密密钥的建立和管理 | 对称密钥	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
CCCS-fPBMM-SC-12.A	SC-12.A 加密密钥的建立和管理	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
CCCS-fPBMM-SC-12.A	SC-12.A 加密密钥的建立和管理	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-13.A	SC-13.A 加密保护	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-22.A	SC-22.A 名称/地址解析服务的架构和配置	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CCCS-fPBMM-SC-23.A	SC-23.A 真实性	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-23.A	SC-23.A 真实性	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
CCCS-fPBMM-SC-23.A	SC-23.A 真实性	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-23.A	SC-23.A 真实性	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-23.A	SC-23.A 真实性	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELBSecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
CCCS-fPBMM-SC-23.A	SC-23.A 真实性	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-23.A	SC-23.A 真实性	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-23.A	SC-23.A 真实性	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-23.A	SC-23.A 真实性	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28(1)	SC-28(1) 静态信息保护 | 加密保护	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CCCS-fPBMM-SC-28.A	SC-28.A 静态信息保护	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2(2)	SI-2(2) 缺陷修复 | 自动缺陷修复状态	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2(3)	SI-2(3) 缺陷修复 | 缺陷修复时间/纠正措施的基准	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.A	SI-2.A 缺陷修复	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.B	SI-2.B 缺陷修复	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.C	SI-2.C 缺陷修复	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-2.D	SI-2.D 缺陷修复	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
CCCS-fPBMM-SI-3(1)	SI-3(1) 恶意代码防护 | 集中管理	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-3(7)	SI-3(7) 恶意代码防护 | 非基于签名的检测	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-SI-3.A	SI-3.A 恶意代码防护	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-3.A	SI-3.A 恶意代码防护	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-SI-3.A	SI-3.A 恶意代码防护	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-3.A	SI-3.A 恶意代码防护	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-SI-3.A	SI-3.A 恶意代码防护	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-3.B	SI-3.B 恶意代码防护	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-SI-3.B	SI-3.B 恶意代码防护	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-3.B	SI-3.B 恶意代码防护	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-SI-3.B	SI-3.B 恶意代码防护	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-3.C	SI-3.C 恶意代码防护	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-SI-3.C	SI-3.C 恶意代码防护	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-3.C	SI-3.C 恶意代码防护	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-SI-3.C	SI-3.C 恶意代码防护	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-3.D	SI-3.D 恶意代码防护	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CCCS-fPBMM-SI-3.D	SI-3.D 恶意代码防护	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-3.D	SI-3.D 恶意代码防护	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CCCS-fPBMM-SI-3.D	SI-3.D 恶意代码防护	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-SI-4(1)	SI-4(1) 信息系统监控 | 全系统入侵检测系统	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4(1)	SI-4(1) 信息系统监控 | 全系统入侵检测系统	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-SI-4(2)	SI-4(2) 信息系统监控 | 用于实时分析的自动化工具	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4(2)	SI-4(2) 信息系统监控 | 用于实时分析的自动化工具	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CCCS-fPBMM-SI-4(4)	SI-4(4) 信息系统监控 | 入站和出站通信流量	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4(4)	SI-4(4) 信息系统监控 | 入站和出站通信流量	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
CCCS-fPBMM-SI-4(5)	SI-4(5) 信息系统监控 | 系统生成的警报	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4(11)	SI-4(11) 信息系统监控 | 分析通信流量异常	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-SI-4(11)	SI-4(11) 信息系统监控 | 分析通信流量异常	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4(16)	SI-4(16) 信息系统监控 | 关联监控信息	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-SI-4(16)	SI-4(16) 信息系统监控 | 关联监控信息	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4(20)	SI-4(20) 信息系统监控 | 特权用户	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CCCS-fPBMM-SI-4(23)	SI-4(23) 信息系统监控 | 基于主机的设备	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4(23)	SI-4(23) 信息系统监控 | 基于主机的设备	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.A	SI-4.A 信息系统监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.A	SI-4.A 信息系统监控	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-SI-4.A	SI-4.A 信息系统监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.A	SI-4.A 信息系统监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-SI-4.A	SI-4.A 信息系统监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.B	SI-4.B 信息系统监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.B	SI-4.B 信息系统监控	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-SI-4.B	SI-4.B 信息系统监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.B	SI-4.B 信息系统监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-SI-4.B	SI-4.B 信息系统监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.C	SI-4.C 信息系统监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.C	SI-4.C 信息系统监控	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-SI-4.C	SI-4.C 信息系统监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.C	SI-4.C 信息系统监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-SI-4.C	SI-4.C 信息系统监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.D	SI-4.D 信息系统监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.D	SI-4.D 信息系统监控	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-SI-4.D	SI-4.D 信息系统监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.D	SI-4.D 信息系统监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-SI-4.D	SI-4.D 信息系统监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.E	SI-4.E 信息系统监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.E	SI-4.E 信息系统监控	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-SI-4.E	SI-4.E 信息系统监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.E	SI-4.E 信息系统监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-SI-4.E	SI-4.E 信息系统监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.F	SI-4.F 信息系统监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.F	SI-4.F 信息系统监控	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-SI-4.F	SI-4.F 信息系统监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.F	SI-4.F 信息系统监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-SI-4.F	SI-4.F 信息系统监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.G	SI-4.G 信息系统监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.G	SI-4.G 信息系统监控	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-SI-4.G	SI-4.G 信息系统监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-4.G	SI-4.G 信息系统监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CCCS-fPBMM-SI-4.G	SI-4.G 信息系统监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-5.A	SI-5.A 安全警报、公告和指令	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-SI-5.B	SI-5.B 安全警报、公告和指令	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-SI-5.C	SI-5.C 安全警报、公告和指令	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-5.D	SI-5.D 安全警报、公告和指令	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CCCS-fPBMM-SI-7(1)	SI-7(1) 软件、固件和信息完整性 | 完整性检查	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-7(7)	SI-7(7) 软件、固件和信息完整性 | 检测和响应集成	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CCCS-fPBMM-SI-7.A	SI-7.A 软件、固件和信息完整性	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
CCCS-fPBMM-SI-12.A	SI-12.A 信息处理和保留	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

模板

该模板可在以下网址获得 GitHub：加拿大网络安全中心 (CCCS) 中型云控制概况的运营最佳实践。

CIS AWS 基金会运营最佳实践基准 v1.4 第 1 级

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了互联网安全中心 (CIS) Amazon Web Services Foundation v1.4 第 1 级与 AWS 托管配置规则/AWS Config 流程检查之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CIS Amazon Web Services Foundation v1.4 第 1 级控制相关。一个 CIS Amazon Web Services Foundation v1.4 Level 1 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

有关流程检查的更多信息，请参阅 process-checks。

控制 ID	控制描述	AWS Config 规则	指南
1.1	维护最新的联系人详细信息	account-contact-details-configured（过程检查）	确保 AWS 账户的联系人电子邮件和电话号码是最新的，并映射到组织中的多个人员。在控制台的“我

控制 ID	控制描述	AWS Config 规则	指南
			的账户”部分，确保在“联系信息”部分指定了正确的信息。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
1.2	确保注册安全联系人信息	account-security-contact-configured（流程检查）	确保贵组织安全团队的联系电子邮件和电话号码是最新的。在 AWS 管理控制台的 “我的帐户” 部分中，确保在 “安全” 部分中指定了正确的信息。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
1.4	确保不存在“root”用户访问密钥	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
1.5	确保为“root”用户启用 MFA	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
1.7	无需使用“root”用户执行管理和日常任务	root-account-regular-use（流程检查）	确保避免在日常任务中使用根账户。在 IAM 中，运行凭证报告以检查上次使用根用户的时间。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
1.8	确保 IAM 密码策略要求最短长度不低于 14	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.9	确保 IAM 密码策略阻止重复使用密码	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.10	确保为拥有控制台密码的所有用户启用多重身份验证 (MFA)	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
1.11	在初始用户设置期间，不要为具有控制台密码的所有用户设置访问密钥	iam-user-console-and-（流程检查）api-access-at-creation	在初始用户设置期间，确保不要为具有控制台密码的所有用户设置访问密钥。对于所有具有控制台访问权限的用户，请将用户的“创建时间”与访问密钥“创建”日期进行比较。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
1.12	确保禁用 45 天或更长时间未使用的凭证	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 maxCredentialUsage年龄设置一个值（CIS 标准值：45）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.13	确保只有一个有效的访问密钥可供任何一个用户使用	iam-user-single-access-key（流程检查）	确保只有一个有效的访问密钥可供任何一个用户使用。对于所有用户，请检查 IAM 中每个用户的“安全凭证”选项卡中是否只使用了一个活动密钥。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
1.14	确保访问密钥每 90 天或更短时间轮换一次	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.15	确保用户只能通过组获得权限	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
1.15	确保用户只能通过组获得权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
1.15	确保用户只能通过组获得权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
1.16	确保未附加允许完全“*:*”管理权限的 IAM 策略	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含“效果”：“允许”和“操作”：“*”而不是“资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
1.17	确保已创建支持角色来管理 AWS 支持 Support 的事件	iam-policy-in-use	AWS Identity and Access Management 可确保将 IAM 策略分配给相应的用户、角色或群组，从而帮助您管理访问权限和授权。限制这些策略还包括最低权限和职责分离原则。此规则要求你将 policYarn 设置为 arn: aws: iam:: aws: policy/，以便使用 Support 进行事件管理AWSSupportAccess。 AWS

控制 ID	控制描述	AWS Config 规则	指南
1.19	确保移除存储在 AWS IAM 中的所有过期 SSL/TLS 证书	iam-expired-certificates（流程检查）	确保移除存储在 IAM 中的所有过期 SSL/TLS 证书。在安装了 AWS CLI 的命令行中运行 “i AWS a list-server-certificates m” 命令并确定是否有任何过期的服务器证书。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
1.20	确保启用 AWS IAM 访问分析器	iam-access-analyzer-enabled（流程检查）	确保启用 IAM Access Analyzer。在控制台的 IAM 部分中，选择 Access Analyzer 并确保将“状态”设置为“活动”。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
2.1.3	确保在 S3 存储桶上启用 MFA 删除	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。向 S3 存储桶添加多重身份验证 (MFA) 删除需要额外的身份验证因素，才能更改存储桶的版本状态或删除对象版本。MFA 删除可以在安全凭据泄露或未经授权的访问被批准的情况下增加一层安全保护。

控制 ID	控制描述	AWS Config 规则	指南
2.1.5	确保 S3 存储桶配置“阻止公开访问权限（存储桶设置）”	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
2.1.5	确保 S3 存储桶配置“阻止公开访问权限（存储桶设置）”	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
2.2.1	确保已启用 EBS 卷加密	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
2.2.1	确保已启用 EBS 卷加密	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2.3.1	确保已为 RDS 实例启用加密	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
2.3.1	确保已为 RDS 实例启用加密	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.1	确保 CloudTrail 在所有地区都已启用	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REG ION_CLOUD _TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.3	确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.3	确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.3	确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.4	确保 CloudTrail 跟踪与 CloudWatch日志集成	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
3.6	确保在 S3 存储桶上启用 CloudTrail S3 存储桶访问日志记录	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
4.1	确保存在关于未经授权的 API 调用的日志指标筛选条件和警报	alarm-unauthorized-api-calls （流程检查）	确保存在关于未经授权的 API 调用的日志指标筛选条件和警报 有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.2	确保存在关于无 MFA 的管理控制台登录的日志指标筛选条件和警报	警报-sign-in-without-mfa （过程检查）	确保存在关于无多重身份验证 (MFA) 的 AWS 管理控制台登录的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.3	确保存在关于使用“根”账户的日志指标筛选条件和警报	alarm-root-account-use（流程检查）	确保存在关于使用根账户的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.4	确保存在关于 IAM 策略更改的日志指标筛选条件和警报	alarm-iam-policy-change（流程检查）	确保存在关于 IAM 策略更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.5	确保存在 CloudTrail配置更改的日志指标筛选器和警报	alarm-cloudtrail-config-change（流程检查）	确保有日志指标筛选器，并且存在 AWS CloudTrail 配置更改警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.8	确保存在关于 S3 存储桶策略更改的日志指标筛选条件和警报	alarm-s3-bucket-policy-change（进程检查）	确保存在关于 Amazon S3 存储桶策略更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.12	确保存在关于网络网关更改的日志指标筛选条件和警报	警报-vpc-network-gateway-change（过程检查）	确保存在关于网络网关更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.13	确保存在关于路由表更改的日志指标筛选条件和警报	警报-vpc-route-table-change（过程检查）	确保存在关于路由表更改的日志指标筛选条件和警报 有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.14	确保存在关于 VPC 更改的日志指标筛选条件和警报	alarm-vpc-change（流程检查）	确保存在关于 Amazon Virtual Private Cloud (VPC) 更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.15	确保存在关于 AWS Organizations 更改的日志指标筛选条件和警报	alarm-organizations-change（流程检查）	确保存在关于 AWS Organizations 更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
5.1	确保没有网络 ACL 允许从 0.0.0.0/0 进入远程服务器管理端口	nacl-no-unrestricted-ssh-rdp	确保没有网络 ACL 允许远程服务器管理端口的公共入口。在控制台的 VPC 部分，确保有源为“0.0.0.0/0”的网络 ACL，允许使用包括远程服务器管理端口在内的端口或端口范围。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
5.2	确保没有安全组允许从 0.0.0.0/0 进入远程服务器管理端口	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
5.2	确保没有安全组允许从 0.0.0.0/0 进入远程服务器管理端口	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（CIS 标准值：3389）。实际值应反映贵组织的策略。

模板

该模板可在以下网址获得 GitHub：CIS AWS 基金会运营最佳实践基准 v1.4 第 1 级。

CIS AWS 基金会运营最佳实践基准 v1.4 第 2 级

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了互联网安全中心 (CIS) Amazon Web Services Foundation v1.4 第 2 级与 AWS 托管配置规则/AWS Config 流程检查之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CIS Amazon Web Services Foundation v1.4 第 2 级控制相关。一个 CIS Amazon Web Services Foundation v1.4 Level 2 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

有关流程检查的更多信息，请参阅 process-checks。

AWS 区域：除了（美国东部 AWS 区域 ）、（美国西部）和中东 AWS GovCloud （巴林）以外的所有地区都支持一致性包 AWS GovCloud （区域支持）

控制 ID	控制描述	AWS Config 规则	指南
1.1	维护最新的联系人详细信息	account-contact-details-configured （过程检查）	确保 AWS 账户的联系人电子邮件和电话号码是最新的，并映射到组织中的多个人员。在控制台的“我的账户”部分，确保在“联系信息”部分指定了正确的信息。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
1.2	确保注册安全联系人信息	account-security-contact-configured （流程检查）	确保贵组织安全团队的联系电子邮件和电话号码是最新的。在 AWS 管理控制台的 “我的帐户” 部分中，确保在 “安全” 部分中指定了正确的信息。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为

控制 ID	控制描述	AWS Config 规则	指南
			https://www.cisecurity.org/benchmark/amazon_web_services/
1.4	确保不存在“root”用户访问密钥	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
1.5	确保为“root”用户启用 MFA	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
1.6	确保为“root”用户账户启用硬件 MFA	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
1.7	无需使用“root”用户执行管理和日常任务	root-account-regular-use（流程检查）	确保避免在日常任务中使用根账户。在 IAM 中，运行凭证报告以检查上次使用根用户的时间。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
1.8	确保 IAM 密码策略要求最短长度不低于 14	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.9	确保 IAM 密码策略阻止重复使用密码	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.10	确保为拥有控制台密码的所有用户启用多重身份验证 (MFA)	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
1.11	在初始用户设置期间，不要为具有控制台密码的所有用户设置访问密钥	iam-user-console-and-（流程检查）api-access-at-creation	在初始用户设置期间，确保不要为具有控制台密码的所有用户设置访问密钥。对于所有具有控制台访问权限的用户，请将用户的“创建时间”与访问密钥“创建”日期进行比较。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
1.12	确保禁用 45 天或更长时间未使用的凭证	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 maxCredentialUsage年龄设置一个值（CIS 标准值：45）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.13	确保只有一个有效的访问密钥可供任何一个用户使用	iam-user-single-access-key（流程检查）	确保只有一个有效的访问密钥可供任何一个用户使用。对于所有用户，请检查 IAM 中每个用户的“安全凭证”选项卡中是否只使用了一个活动密钥。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
1.14	确保访问密钥每 90 天或更短时间轮换一次	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.15	确保用户只能通过组获得权限	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
1.15	确保用户只能通过组获得权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
1.15	确保用户只能通过组获得权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
1.16	确保未附加允许完全“*:*”管理权限的 IAM 策略	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含“效果”：“允许”和“操作”：“*”而不是“资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
1.17	确保已创建支持角色来管理与 AWS Support 发生的事件	iam-policy-in-use	AWS Identity and Access Management 可确保将 IAM 策略分配给相应的用户、角色或群组，从而帮助您管理访问权限和授权。限制这些策略还包括最低权限和职责分离原则。此规则要求你将 policYarn 设置为 arn: aws: iam:: aws: policy/，以便使用 Support 进行事件管理AWSSupportAccess。 AWS

控制 ID	控制描述	AWS Config 规则	指南
1.18	确保使用 IAM 实例角色从实例访问 AWS 资源	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
1.19	确保移除存储在 AWS IAM 中的所有过期 SSL/TLS 证书	iam-expired-certificates（流程检查）	确保移除存储在 IAM 中的所有过期 SSL/TLS 证书。在安装了 AWS CLI 的命令行中运行 “i AWS a list-server-certificates m” 命令并确定是否有任何过期的服务器证书。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
1.20	确保已启用 AWS IAM 访问分析器	iam-access-analyzer-enabled （流程检查）	确保启用 IAM Access Analyzer。在控制台的 IAM 部分中，选择 Access Analyzer 并确保将“状态”设置为“活动”。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
1.21	确保通过联合身份验证或 Organizations（适用于多账户 AWS 环境）对用户进行集中管理	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
2.1.1	确保所有 S3 存储桶都使用 encryption-at-rest	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
2.1.2	确保 S3 存储桶策略已设置为拒绝 HTTP 请求	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
2.1.3	确保在 S3 存储桶上启用 MFA 删除	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。向 S3 存储桶添加多重身份验证 (MFA) 删除需要额外的身份验证因素，才能更改存储桶的版本状态或删除对象版本。MFA 删除可以在安全凭据泄露或未经授权的访问被批准的情况下增加一层安全保护。

控制 ID	控制描述	AWS Config 规则	指南
2.1.5	确保 S3 存储桶配置“阻止公开访问权限（存储桶设置）”	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
2.1.5	确保 S3 存储桶配置“阻止公开访问权限（存储桶设置）”	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
2.2.1	确保已启用 EBS 卷加密	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
2.2.1	确保已启用 EBS 卷加密	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2.3.1	确保已为 RDS 实例启用加密	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
2.3.1	确保已为 RDS 实例启用加密	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.1	确保 CloudTrail 在所有地区都已启用	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.2	确保已启用 CloudTrail 日志文件验证	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
3.3	确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.3	确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.3	确保用于存储 CloudTrail 日志的 S3 存储桶不可公开访问	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
3.4	确保 CloudTrail 跟踪与 CloudWatch日志集成	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.5	确保所有区域都启用了 AWS Config	config-enabled-all-regions（流程检查）	确保所有 AWS 区域都启用了 AWS Config。在控制台的 AWS Config 部分中，对于每个启用的区域，请确保 AWS 配置记录器配置正确。确保至少在一个区域启用全局 AWS 资源记录。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
3.6	确保在 S3 存储桶上启用 CloudTrail S3 存储桶访问日志记录	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
3.7	确保使用 KMS CMK 对 CloudTrail 日志进行静态加密	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
3.8	确保为客户创建的 CMK 启用轮换	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
3.9	确保在所有 VPC 中启用 VPC 流日志记录	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
3.10	确保已为 S3 存储桶启用写入事件的对象级日志记录	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
3.11	确保已为 S3 存储桶启用读取事件的对象级日志记录	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
4.1	确保存在关于未经授权的 API 调用的日志指标筛选条件和警报	alarm-unauthorized-api-calls （流程检查）	确保存在关于未经授权的 API 调用的日志指标筛选条件和警报 有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.2	确保存在关于无 MFA 的管理控制台登录的日志指标筛选条件和警报	警报-sign-in-without-mfa （进程检查）	确保存在关于无多重身份验证 (MFA) 的 AWS 管理控制台登录的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.3	确保存在关于使用“根”账户的日志指标筛选条件和警报	alarm-root-account-use（流程检查）	确保存在关于使用根账户的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.4	确保存在关于 IAM 策略更改的日志指标筛选条件和警报	alarm-iam-policy-change（流程检查）	确保存在关于 IAM 策略更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.5	确保存在 CloudTrail配置更改的日志指标筛选器和警报	alarm-cloudtrail-config-change（流程检查）	确保有日志指标筛选器，并且存在 AWS CloudTrail 配置更改警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.6	确保存在关于 AWS 管理控制台身份验证失败的日志指标筛选条件和警报	alarm-console-auth-failures（流程检查）	确保存在关于 AWS 管理控制台身份验证失败的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.7	确保存在关于禁用或计划删除客户创建的 CMK 的日志指标筛选条件和警报	alarm-kms-disable-or-delete-cmk（进程检查）	确保存在关于禁用或计划删除客户创建的 CMK 的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.8	确保存在关于 S3 存储桶策略更改的日志指标筛选条件和警报	alarm-s3-bucket-policy-change（进程检查）	确保存在关于 Amazon S3 存储桶策略更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.9	确保存在针对 AWS Config 配置更改的日志指标筛选器和警报	alarm-aws-config-change（流程检查）	确保存在关于 AWS Config 配置更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.10	确保存在关于安全组更改的日志指标筛选条件和警报	警报-vpc-secrity-group-change（进程检查）	确保存在关于安全组更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.11	确保存在关于网络访问控制列表 (NACL) 更改的日志指标筛选条件和警报	alarm-vpc-nacl-change（流程检查）	确保存在关于网络访问控制列表 (NACL) 更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.12	确保存在关于网络网关更改的日志指标筛选条件和警报	警报-vpc-network-gateway-change（进程检查）	确保存在关于网络网关更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.13	确保存在关于路由表更改的日志指标筛选条件和警报	警报-vpc-route-table-change（进程检查）	确保存在关于路由表更改的日志指标筛选条件和警报 有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
4.14	确保存在关于 VPC 更改的日志指标筛选条件和警报	alarm-vpc-change（流程检查）	确保存在关于 Amazon Virtual Private Cloud (VPC) 更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
4.15	确保存在关于 AWS Organizations 更改的日志指标筛选条件和警报	alarm-organizations-change（流程检查）	确保存在关于 AWS Organizations 更改的日志指标筛选条件和警报。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/
5.1	确保没有网络 ACL 允许从 0.0.0.0/0 进入远程服务器管理端口	nacl-no-unrestricted-ssh-rdp	确保没有网络 ACL 允许远程服务器管理端口的公共入口。在控制台的 VPC 部分，确保有源为“0.0.0.0/0”的网络 ACL，允许使用包括远程服务器管理端口在内的端口或端口范围。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

控制 ID	控制描述	AWS Config 规则	指南
5.2	确保没有安全组允许从 0.0.0.0/0 进入远程服务器管理端口	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
5.2	确保没有安全组允许从 0.0.0.0/0 进入远程服务器管理端口	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（CIS 标准值：3389）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.3	确保每个 VPC 的默认安全组限制所有流量	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
5.4	确保 VPC 对等连接的路由表为“最少访问”	vpc-peering-least-access （流程检查）	确保 Amazon VPC 对等连接的路由表为“最少访问”。在控制台的 VPC 部分中，检查路由表条目，确保实现对等互连目的所需的最少数量子网或主机可路由。有关该控制审计的更多详情，请参阅 CIS Amazon Web Services Foundations Benchmark 版本 1.4.0 文档，网址为 https://www.cisecurity.org/benchmark/amazon_web_services/

模板

该模板可在以下网址获得 GitHub：CIS AWS 基金会运营最佳实践基准 v1.4 第 2 级。

CIS 关键安全控制 v8 IG1 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了互联网安全中心 (CIS) 关键安全控制 v8 IG1 和托管 C AWS onfig 规则之间的映射示例。每个控件都 AWS Config 适用于特定的 AWS 资源，并与一个或多个 CIS 关键安全控制 v8 IG1 控件相关。一个 CIS 关键安全控制 v8 IG1 控制可以与多个 AWS Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
1.1	建立和维护详细的企业资产清单	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
1.1	建立和维护详细的企业资产清单	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
1.1	建立和维护详细的企业资产清单	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud

控制 ID	控制描述	AWS Config 规则	指南
			(VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
1.1	建立和维护详细的企业资产清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
1.1	建立和维护详细的企业资产清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
1.1	建立和维护详细的企业资产清单	ec2-security-group-attached-to-eni	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
2.2	确保授权软件当前受支持	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
2.2	确保授权软件当前受支持	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
2.2	确保授权软件当前受支持	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。为了协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
3.3	配置数据访问控制列表	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
3.3	配置数据访问控制列表	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.3	配置数据访问控制列表	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
3.3	配置数据访问控制列表	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
3.3	配置数据访问控制列表	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.3	配置数据访问控制列表	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.3	配置数据访问控制列表	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3.3	配置数据访问控制列表	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.3	配置数据访问控制列表	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.3	配置数据访问控制列表	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
3.3	配置数据访问控制列表	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
3.3	配置数据访问控制列表	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.3	配置数据访问控制列表	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.3	配置数据访问控制列表	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.3	配置数据访问控制列表	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.3	配置数据访问控制列表	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.3	配置数据访问控制列表	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.3	配置数据访问控制列表	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
3.3	配置数据访问控制列表	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。
3.3	配置数据访问控制列表	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.3	配置数据访问控制列表	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
3.4	强制数据留存	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
3.4	强制数据留存	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
4.1	建立和维护安全的配置流程	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
4.1	建立和维护安全的配置流程	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
4.1	建立和维护安全的配置流程	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
4.1	建立和维护安全的配置流程	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
4.1	建立和维护安全的配置流程	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
4.1	建立和维护安全的配置流程	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
4.6	安全管理企业资产和软件	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4.6	安全管理企业资产和软件	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4.6	安全管理企业资产和软件	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
4.6	安全管理企业资产和软件	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
4.6	安全管理企业资产和软件	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4.6	安全管理企业资产和软件	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
4.7	管理企业资产和软件的默认账户	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
5.1	建立和维护账户清单	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
5.2	使用唯一的密码	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.2	使用唯一的密码	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
5.2	使用唯一的密码	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
5.2	使用唯一的密码	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
5.3	禁用休眠账户	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.4	将管理员特权限制为专用管理员账户	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
5.4	将管理员特权限制为专用管理员账户	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
6.4	远程网络访问需要 MFA	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
6.4	远程网络访问需要 MFA	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
6.4	远程网络访问需要 MFA	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
6.5	管理访问需要 MFA	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
7.1	建立和维护漏洞管理流程	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
7.1	建立和维护漏洞管理流程	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
7.1	建立和维护漏洞管理流程	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
7.3	执行自动操作系统补丁管理	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
7.3	执行自动操作系统补丁管理	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
7.3	执行自动操作系统补丁管理	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
7.4	执行自动应用程序补丁管理	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
7.4	执行自动应用程序补丁管理	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
7.4	执行自动应用程序补丁管理	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
8.1	建立和维护审计日志管理流程	audit-log-policy-exists（过程检查）	制定并维护审计日志管理策略，以定义贵组织的日志记录要求。这包括但不限于审查和保留审计日志。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
8.2	收集审计日志	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
8.2	收集审计日志	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
8.2	收集审计日志	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
8.2	收集审计日志	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
8.2	收集审计日志	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
8.2	收集审计日志	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
8.2	收集审计日志	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
8.3	确保有足够的审计日志存储空间	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
10.1	部署和维护防恶意软件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
10.2	配置自动防恶意软件签名更新	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
11.2	执行自动备份	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.2	执行自动备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
11.2	执行自动备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
11.2	执行自动备份	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
11.2	执行自动备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
11.2	执行自动备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
11.3	保护恢复数据	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.3	保护恢复数据	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
11.3	保护恢复数据	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	保护恢复数据	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.4	建立和维护隔离的恢复数据实例	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.4	建立和维护隔离的恢复数据实例	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
11.4	建立和维护隔离的恢复数据实例	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
11.4	建立和维护隔离的恢复数据实例	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
11.4	建立和维护隔离的恢复数据实例	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
11.4	建立和维护隔离的恢复数据实例	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

模板

该模板可在以下网址获得 GitHub：CI S 关键安全控制操作最佳实践 v8 IG1。

CIS 关键安全控制 v8 IG2 操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了互联网安全中心 (CIS) 关键安全控制 v8 IG2 和托管 C AWS onfig 规则之间的映射示例。每个都 AWS Config 适用于特定的 AWS 资源，并与一个或多个 CIS 关键安全控制 v8 IG2 控件相关。一个 CIS 关键安全控制 v8 IG2 控制可以与多个 AWS Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
1.1	建立和维护详细的企业资产清单	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2)

控制 ID	控制描述	AWS Config 规则	指南
			实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
1.1	建立和维护详细的企业资产清单	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
1.1	建立和维护详细的企业资产清单	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	控制描述	AWS Config 规则	指南
1.1	建立和维护详细的企业资产清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
1.1	建立和维护详细的企业资产清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
1.1	建立和维护详细的企业资产清单	ec2-security-group-attached-to-eni	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
2.2	确保授权软件当前受支持	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
2.2	确保授权软件当前受支持	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
2.2	确保授权软件当前受支持	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。要协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。
2.4	利用自动软件清点工具	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
2.4	利用自动软件清点工具	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
3.3	配置数据访问控制列表	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
3.3	配置数据访问控制列表	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.3	配置数据访问控制列表	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
3.3	配置数据访问控制列表	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
3.3	配置数据访问控制列表	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.3	配置数据访问控制列表	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.3	配置数据访问控制列表	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3.3	配置数据访问控制列表	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.3	配置数据访问控制列表	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.3	配置数据访问控制列表	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
3.3	配置数据访问控制列表	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
3.3	配置数据访问控制列表	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.3	配置数据访问控制列表	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.3	配置数据访问控制列表	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.3	配置数据访问控制列表	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.3	配置数据访问控制列表	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.3	配置数据访问控制列表	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.3	配置数据访问控制列表	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
3.3	配置数据访问控制列表	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。
3.3	配置数据访问控制列表	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.3	配置数据访问控制列表	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
3.4	强制数据留存	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
3.4	强制数据留存	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
3.10	加密传输中的敏感数据	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
3.10	加密传输中的敏感数据	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.10	加密传输中的敏感数据	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.10	加密传输中的敏感数据	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.10	加密传输中的敏感数据	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.10	加密传输中的敏感数据	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.10	加密传输中的敏感数据	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.10	加密传输中的敏感数据	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
3.10	加密传输中的敏感数据	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.10	加密传输中的敏感数据	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.11	加密静态敏感数据	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
3.11	加密静态敏感数据	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
3.11	加密静态敏感数据	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
3.11	加密静态敏感数据	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
3.11	加密静态敏感数据	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
3.11	加密静态敏感数据	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
4.1	建立和维护安全的配置流程	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
4.1	建立和维护安全的配置流程	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
4.1	建立和维护安全的配置流程	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
4.1	建立和维护安全的配置流程	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
4.1	建立和维护安全的配置流程	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
4.6	安全管理企业资产和软件	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4.6	安全管理企业资产和软件	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4.6	安全管理企业资产和软件	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
4.6	安全管理企业资产和软件	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
4.6	安全管理企业资产和软件	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4.6	安全管理企业资产和软件	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
4.7	管理企业资产和软件的默认账户	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
5.1	建立和维护账户清单	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
5.2	使用唯一的密码	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.2	使用唯一的密码	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
5.2	使用唯一的密码	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
5.2	使用唯一的密码	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
5.3	禁用休眠账户	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.4	将管理员特权限制为专用管理员账户	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
5.4	将管理员特权限制为专用管理员账户	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
5.6	集中管理账户	account-part-of-organizations	Organizations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
6.4	远程网络访问需要 MFA	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
6.4	远程网络访问需要 MFA	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
6.4	远程网络访问需要 MFA	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
6.5	管理访问需要 MFA	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
6.7	集中管理访问控制	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
7.1	建立和维护漏洞管理流程	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
7.1	建立和维护漏洞管理流程	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
7.1	建立和维护漏洞管理流程	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
7.3	执行自动操作系统补丁管理	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
7.3	执行自动操作系统补丁管理	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
7.3	执行自动操作系统补丁管理	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认为 1）。实际值应反映贵组织的策略。
7.4	执行自动应用程序补丁管理	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
7.4	执行自动应用程序补丁管理	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
7.4	执行自动应用程序补丁管理	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
7.5	对企业内部资产执行自动漏洞扫描	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
8.1	建立和维护审计日志管理流程	audit-log-policy-exists（过程检查）	制定并维护审计日志管理策略，以定义贵组织的日志记录要求。这包括但不限于审查和保留审计日志。
8.2	收集审计日志	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
8.2	收集审计日志	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
8.2	收集审计日志	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
8.2	收集审计日志	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
8.2	收集审计日志	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
8.2	收集审计日志	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
8.2	收集审计日志	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
8.3	确保有足够的审计日志存储空间	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
8.5	收集详细的审计日志	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
8.5	收集详细的审计日志	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
8.5	收集详细的审计日志	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
8.5	收集详细的审计日志	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
8.5	收集详细的审计日志	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
8.5	收集详细的审计日志	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
8.5	收集详细的审计日志	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
8.5	收集详细的审计日志	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
8.7	收集 URL 请求审计日志	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
8.9	集中管理审计日志	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
8.10	保留审计日志	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
8.10	保留审计日志	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
10.1	部署和维护防恶意软件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
10.2	配置自动防恶意软件签名更新	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
10.4	配置可移动媒体的自动防恶意软件扫描	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
10.6	集中管理防恶意软件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
10.7	使用基于行为的防恶意软件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
11.2	执行自动备份	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.2	执行自动备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
11.2	执行自动备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
11.2	执行自动备份	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
11.2	执行自动备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认为 1）。实际值应反映贵组织的策略。
11.2	执行自动备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
11.3	保护恢复数据	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.3	保护恢复数据	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
11.3	保护恢复数据	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	保护恢复数据	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.4	建立和维护隔离的恢复数据实例	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.4	建立和维护隔离的恢复数据实例	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
11.4	建立和维护隔离的恢复数据实例	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
11.4	建立和维护隔离的恢复数据实例	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
11.4	建立和维护隔离的恢复数据实例	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认为 1）。实际值应反映贵组织的策略。
11.4	建立和维护隔离的恢复数据实例	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
12.2	建立和维护安全的网络架构	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
12.2	建立和维护安全的网络架构	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
12.2	建立和维护安全的网络架构	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
12.2	建立和维护安全的网络架构	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
12.2	建立和维护安全的网络架构	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
12.2	建立和维护安全的网络架构	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
12.2	建立和维护安全的网络架构	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
12.2	建立和维护安全的网络架构	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
12.2	建立和维护安全的网络架构	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
12.2	建立和维护安全的网络架构	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
12.2	建立和维护安全的网络架构	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
12.2	建立和维护安全的网络架构	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
12.2	建立和维护安全的网络架构	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
12.2	建立和维护安全的网络架构	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
12.2	建立和维护安全的网络架构	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
12.2	建立和维护安全的网络架构	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
12.2	建立和维护安全的网络架构	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
12.2	建立和维护安全的网络架构	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
12.2	建立和维护安全的网络架构	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	elbv2-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
12.3	安全管理网络基础设施	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
12.3	安全管理网络基础设施	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
12.3	安全管理网络基础设施	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
12.3	安全管理网络基础设施	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.3	安全管理网络基础设施	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
12.3	安全管理网络基础设施	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.3	安全管理网络基础设施	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
12.3	安全管理网络基础设施	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
12.6	使用安全的网络管理和通信协议	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
12.6	使用安全的网络管理和通信协议	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.6	使用安全的网络管理和通信协议	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
12.6	使用安全的网络管理和通信协议	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
12.6	使用安全的网络管理和通信协议	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.6	使用安全的网络管理和通信协议	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.6	使用安全的网络管理和通信协议	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
12.6	使用安全的网络管理和通信协议	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
13.1	集中管理安全事件警报	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
13.1	集中管理安全事件警报	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
13.3	部署网络入侵检测解决方案	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
13.6	收集网络流量日志	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
13.6	收集网络流量日志	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
16.1	建立和维护安全的应用程序开发流程	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
16.1	建立和维护安全的应用程序开发流程	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
16.1	建立和维护安全的应用程序开发流程	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。

控制 ID	控制描述	AWS Config 规则	指南
16.1	建立和维护安全的应用程序开发流程	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
16.1	建立和维护安全的应用程序开发流程	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

模板

该模板可在以下网址获得 GitHub：CI S 关键安全控制操作最佳实践 v8 IG2。

CIS 关键安全控制 v8 IG3 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了互联网安全中心 (CIS) 关键安全控制 v8 IG3 和托管 C AWS onfig 规则之间的映射示例。每个都 AWS Config 适用于特定的 AWS 资源，并与一个或多个 CIS 关键安全控制 v8 IG3 控件相关。一个 CIS 关键安全控制 v8 IG3 控制可以与多个 AWS Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
1.1	建立和维护详细的企业资产清单	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
1.1	建立和维护详细的企业资产清单	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
1.1	建立和维护详细的企业资产清单	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
1.1	建立和维护详细的企业资产清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，

控制 ID	控制描述	AWS Config 规则	指南
			可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
1.1	建立和维护详细的企业资产清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
1.1	建立和维护详细的企业资产清单	ec2-security-group-attached-to-eni	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。

控制 ID	控制描述	AWS Config 规则	指南
2.2	确保授权软件当前受支持	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
2.2	确保授权软件当前受支持	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
2.2	确保授权软件当前受支持	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。要协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。

控制 ID	控制描述	AWS Config 规则	指南
2.4	利用自动软件清点工具	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
2.4	利用自动软件清点工具	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
3.3	配置数据访问控制列表	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
3.3	配置数据访问控制列表	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.3	配置数据访问控制列表	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
3.3	配置数据访问控制列表	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
3.3	配置数据访问控制列表	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.3	配置数据访问控制列表	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.3	配置数据访问控制列表	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3.3	配置数据访问控制列表	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.3	配置数据访问控制列表	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.3	配置数据访问控制列表	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
3.3	配置数据访问控制列表	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
3.3	配置数据访问控制列表	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.3	配置数据访问控制列表	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.3	配置数据访问控制列表	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.3	配置数据访问控制列表	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.3	配置数据访问控制列表	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.3	配置数据访问控制列表	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.3	配置数据访问控制列表	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
3.3	配置数据访问控制列表	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。
3.3	配置数据访问控制列表	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
3.3	配置数据访问控制列表	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.3	配置数据访问控制列表	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
3.4	强制数据留存	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
3.4	强制数据留存	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
3.10	加密传输中的敏感数据	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
3.10	加密传输中的敏感数据	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.10	加密传输中的敏感数据	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.10	加密传输中的敏感数据	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.10	加密传输中的敏感数据	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.10	加密传输中的敏感数据	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.10	加密传输中的敏感数据	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.10	加密传输中的敏感数据	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
3.10	加密传输中的敏感数据	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.10	加密传输中的敏感数据	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.11	加密静态敏感数据	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
3.11	加密静态敏感数据	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
3.11	加密静态敏感数据	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
3.11	加密静态敏感数据	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
3.11	加密静态敏感数据	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.11	加密静态敏感数据	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.11	加密静态敏感数据	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
3.11	加密静态敏感数据	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
3.14	记录敏感数据访问	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
3.14	记录敏感数据访问	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.14	记录敏感数据访问	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
3.14	记录敏感数据访问	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
3.14	记录敏感数据访问	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.14	记录敏感数据访问	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
3.14	记录敏感数据访问	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
3.14	记录敏感数据访问	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
3.14	记录敏感数据访问	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
3.14	记录敏感数据访问	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
3.14	记录敏感数据访问	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
3.14	记录敏感数据访问	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
3.14	记录敏感数据访问	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.14	记录敏感数据访问	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
4.1	建立和维护安全的配置流程	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
4.1	建立和维护安全的配置流程	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
4.1	建立和维护安全的配置流程	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
4.1	建立和维护安全的配置流程	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
4.1	建立和维护安全的配置流程	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
4.1	建立和维护安全的配置流程	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
4.6	安全管理企业资产和软件	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4.6	安全管理企业资产和软件	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4.6	安全管理企业资产和软件	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
4.6	安全管理企业资产和软件	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
4.6	安全管理企业资产和软件	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4.6	安全管理企业资产和软件	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
4.7	管理企业资产和软件的默认账户	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
5.1	建立和维护账户清单	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
5.2	使用唯一的密码	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.2	使用唯一的密码	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
5.2	使用唯一的密码	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
5.2	使用唯一的密码	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
5.3	禁用休眠账户	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.4	将管理员特权限制为专用管理员账户	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
5.4	将管理员特权限制为专用管理员账户	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
5.6	集中管理账户	account-part-of-organizations	Organizations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
6.4	远程网络访问需要 MFA	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
6.4	远程网络访问需要 MFA	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
6.4	远程网络访问需要 MFA	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
6.5	管理访问需要 MFA	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
6.7	集中管理访问控制	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
7.1	建立和维护漏洞管理流程	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
7.1	建立和维护漏洞管理流程	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
7.1	建立和维护漏洞管理流程	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
7.3	执行自动操作系统补丁管理	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
7.3	执行自动操作系统补丁管理	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
7.3	执行自动操作系统补丁管理	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
7.4	执行自动应用程序补丁管理	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
7.4	执行自动应用程序补丁管理	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
7.4	执行自动应用程序补丁管理	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
7.5	对企业内部资产执行自动漏洞扫描	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
8.1	建立和维护审计日志管理流程	audit-log-policy-exists（过程检查）	制定并维护审计日志管理策略，以定义贵组织的日志记录要求。这包括但不限于审查和保留审计日志。
8.2	收集审计日志	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
8.2	收集审计日志	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
8.2	收集审计日志	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
8.2	收集审计日志	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
8.2	收集审计日志	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
8.2	收集审计日志	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
8.2	收集审计日志	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
8.2	收集审计日志	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
8.3	确保有足够的审计日志存储空间	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
8.5	收集详细的审计日志	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
8.5	收集详细的审计日志	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
8.5	收集详细的审计日志	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
8.5	收集详细的审计日志	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
8.5	收集详细的审计日志	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
8.5	收集详细的审计日志	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
8.5	收集详细的审计日志	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
8.5	收集详细的审计日志	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
8.5	收集详细的审计日志	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
8.7	收集 URL 请求审计日志	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
8.9	集中管理审计日志	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
8.10	保留审计日志	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
8.10	保留审计日志	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
10.1	部署和维护防恶意软件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
10.2	配置自动防恶意软件签名更新	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
10.4	配置可移动媒体的自动防恶意软件扫描	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
10.6	集中管理防恶意软件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
10.7	使用基于行为的防恶意软件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
11.2	执行自动备份	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.2	执行自动备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
11.2	执行自动备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
11.2	执行自动备份	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
11.2	执行自动备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
11.2	执行自动备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
11.2	执行自动备份	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
11.3	保护恢复数据	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.3	保护恢复数据	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
11.3	保护恢复数据	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	保护恢复数据	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.4	建立和维护隔离的恢复数据实例	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.4	建立和维护隔离的恢复数据实例	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
11.4	建立和维护隔离的恢复数据实例	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
11.4	建立和维护隔离的恢复数据实例	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
11.4	建立和维护隔离的恢复数据实例	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
11.4	建立和维护隔离的恢复数据实例	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
11.4	建立和维护隔离的恢复数据实例	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
12.2	建立和维护安全的网络架构	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
12.2	建立和维护安全的网络架构	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
12.2	建立和维护安全的网络架构	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
12.2	建立和维护安全的网络架构	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
12.2	建立和维护安全的网络架构	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
12.2	建立和维护安全的网络架构	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
12.2	建立和维护安全的网络架构	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
12.2	建立和维护安全的网络架构	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
12.2	建立和维护安全的网络架构	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
12.2	建立和维护安全的网络架构	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
12.2	建立和维护安全的网络架构	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
12.2	建立和维护安全的网络架构	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
12.2	建立和维护安全的网络架构	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
12.2	建立和维护安全的网络架构	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
12.2	建立和维护安全的网络架构	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
12.2	建立和维护安全的网络架构	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
12.2	建立和维护安全的网络架构	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
12.2	建立和维护安全的网络架构	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
12.2	建立和维护安全的网络架构	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
12.2	建立和维护安全的网络架构	elbv2-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
12.3	安全管理网络基础设施	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
12.3	安全管理网络基础设施	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
12.3	安全管理网络基础设施	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
12.3	安全管理网络基础设施	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.3	安全管理网络基础设施	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
12.3	安全管理网络基础设施	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.3	安全管理网络基础设施	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
12.3	安全管理网络基础设施	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
12.6	使用安全的网络管理和通信协议	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
12.6	使用安全的网络管理和通信协议	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.6	使用安全的网络管理和通信协议	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
12.6	使用安全的网络管理和通信协议	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
12.6	使用安全的网络管理和通信协议	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.6	使用安全的网络管理和通信协议	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
12.6	使用安全的网络管理和通信协议	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
12.6	使用安全的网络管理和通信协议	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
13.1	集中管理安全事件警报	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
13.1	集中管理安全事件警报	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
13.3	部署网络入侵检测解决方案	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
13.6	收集网络流量日志	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
13.6	收集网络流量日志	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
13.10	执行应用程序层过滤	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则基于您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
16.1	建立和维护安全的应用程序开发流程	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
16.1	建立和维护安全的应用程序开发流程	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
16.1	建立和维护安全的应用程序开发流程	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。
16.1	建立和维护安全的应用程序开发流程	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。

控制 ID	控制描述	AWS Config 规则	指南
16.1	建立和维护安全的应用程序开发流程	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
16.12	实施代码级安全检查	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
16.12	实施代码级安全检查	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	控制描述	AWS Config 规则	指南
16.12	实施代码级安全检查	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。
16.12	实施代码级安全检查	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
16.12	实施代码级安全检查	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

模板

该模板可在以下网址获得 GitHub：CI S 关键安全控制操作最佳实践 v8 IG3。

CIS Top 20 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全

确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了互联网安全中心 (CIS) 20 大关键安全控制措施与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个 CIS 前 20 大控件相关。CIS Top 20 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

该合规包已通过 AWS 安全保障服务有限责任公司（AWS SAS）的验证，该公司由支付卡行业合格安全评估员（QSA）、HITRUST认证的通用安全框架从业人员（CCSFP）和经过认证的合规专业人员组成，可以为各种行业框架提供指导和评估。 AWS SAS 专业人员设计此一致性包是为了让客户能够与 CIS 前 20 名中的一部分保持一致。

控制 ID	AWS Config 规则	指南
CIS.2	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CIS.2	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CIS.2	ec2-security-group-attached-to-eni	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。

控制 ID	AWS Config 规则	指南
CIS.2	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
CIS.2	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CIS.2	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CIS.3	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
CIS.3	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认值：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。
CIS.3	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CIS.4	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
CIS.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CIS.4	iam-root-access-key-检查	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
CIS.4	root-account-hardware-mfa-已启用	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
CIS.4	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
CIS.4	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CIS.5	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
CIS.5	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CIS.5	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CIS.5	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
CIS.5	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
CIS.6	api-gw-execution-logging-已启用	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CIS.6	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CIS.6	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在“ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
CIS.6	cloud-trail-log-file-已启用验证	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CIS.6	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户 信息、IP 地址和事件时间。
CIS.6	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	AWS Config 规则	指南
CIS.6	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
CIS.6	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CIS.6	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认值：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。

控制 ID	AWS Config 规则	指南
CIS.6	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有日志文件传送 AWS 区域 到你的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CIS.6	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
CIS.6	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CIS.6	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector 、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CIS.6	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	AWS Config 规则	指南
CIS.8	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CIS.9	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.9	ebs-snapshot-public-restorable-检查	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.9	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
CIS.9	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CIS.9	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.9	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
CIS.9	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CIS.9	internet-gateway-authorized-vpc-只有	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CIS.9	lambda-function-public-access-禁止	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	AWS Config 规则	指南
CIS.9	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
CIS.9	rds-instance-public-access-检查	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CIS.9	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
CIS.9	redshift-cluster-public-access-检查	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CIS.9	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CIS.9	s3 account-level-public-access-方块	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
CIS.9	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CIS.9	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CIS.9	sagemaker-notebook-no-direct-互联网接入	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
CIS.9	vpc-default-security-group-已关闭	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	AWS Config 规则	指南
CIS.9	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CIS.10	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CIS.10	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
CIS.10	elasticache-redis-cluster-automatic-备份检查	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	AWS Config 规则	指南
CIS.10	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CIS.10	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CIS.11	ec2-security-group-attached-to-eni	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
CIS.11	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
CIS.11	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CIS.11	vpc-default-security-group-已关闭	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CIS.11	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
CIS.12	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.12	ebs-snapshot-public-restorable-检查	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.12	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.12	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
CIS.12	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.12	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CIS.12	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
CIS.12	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
CIS.12	internet-gateway-authorized-vpc-只有	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CIS.12	lambda-function-public-access-禁止	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	AWS Config 规则	指南
CIS.12	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
CIS.12	rds-instance-public-access-检查	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CIS.12	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
CIS.12	redshift-cluster-public-access-检查	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CIS.12	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CIS.12	s3 account-level-public-access-方块	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
CIS.12	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CIS.12	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CIS.12	sagemaker-notebook-no-direct-互联网接入	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
CIS.12	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
CIS.12	vpc-default-security-group-已关闭	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CIS.12	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CIS.13	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （ AWS 基础安全最佳实践值：90 ）。实际值应反映贵组织的策略。
CIS.13	alb-http-to-https-重定向检查	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CIS.13	api-gw-cache-enabled并已加密	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
CIS.13	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
CIS.13	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
CIS.13	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CIS.13	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
CIS.13	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
CIS.13	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
CIS.13	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CIS.13	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CIS.13	kms-cmk-not-scheduled-用于删除	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	AWS Config 规则	指南
CIS.13	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CIS.13	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CIS.13	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
CIS.13	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CIS.13	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
CIS.13	s3-已bucket-server-side-encryption启用	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
CIS.13	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CIS.13	sagemaker-endpoint-configuration-kms-密钥已配置	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CIS.13	sagemaker-notebook-instance-kms-密钥已配置	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
CIS.13	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CIS.14	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （ AWS 基础安全最佳实践值：90 ）。实际值应反映贵组织的策略。
CIS.14	alb-http-to-https-重定向检查	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CIS.14	api-gw-cache-enabled并已加密	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
CIS.14	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
CIS.14	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
CIS.14	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.14	ebs-snapshot-public-restorable-检查	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.14	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CIS.14	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CIS.14	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
CIS.14	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
CIS.14	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	AWS Config 规则	指南
CIS.14	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
CIS.14	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CIS.14	kms-cmk-not-scheduled-用于删除	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	AWS Config 规则	指南
CIS.14	rds-instance-public-access-检查	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CIS.14	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CIS.14	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CIS.14	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CIS.14	redshift-cluster-public-access-检查	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CIS.14	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CIS.14	s3 account-level-public-access-方块	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
CIS.14	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
CIS.14	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
CIS.14	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CIS.14	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
CIS.14	s3-已bucket-server-side-encryption启用	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
CIS.14	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CIS.14	sagemaker-endpoint-configuration-kms-密钥已配置	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
CIS.14	sagemaker-notebook-instance-kms-密钥已配置	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CIS.14	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CIS.16	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
CIS.16	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在“ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
CIS.16	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
CIS.16	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	AWS Config 规则	指南
CIS.16	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CIS.16	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认值：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。

控制 ID	AWS Config 规则	指南
CIS.16	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了NIST SP 800-63和互联网安全中心 (CIS) AWS 基金会基准对密码强度的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
CIS.16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CIS.16	iam-root-access-key-检查	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
CIS.16	iam-user-group-membership-检查	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
CIS.16	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
CIS.16	iam-user-no-policies-检查	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
CIS.16	iam-user-unused-credentials-检查	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCreden tialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CIS.16	mfa-enabled-for-iam-控制台访问权限	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
CIS.16	root-account-hardware-mfa-已启用	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
CIS.16	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
CIS.16	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
CIS.16	secretsmanager-scheduled-rotation-success-检查	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	AWS Config 规则	指南
CIS.16	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CIS.18	codebuild-project-envvar-awscred-检查	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
CIS.18	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	AWS Config 规则	指南
CIS.19	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CIS.19	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
CIS.19	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
CIS.2	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

模板

该模板可在以下网址获得 GitHub：独联体前20名的运营最佳实践。

CISA 网络基本要素操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了网络安全与基础设施安全局 (CISA) Cyber Essentials (CE) 和 AWS 托管 Config 规则之间的映射示例。每 AWS Config 条规则都适用于特定的 AWS 资源，并与一个或多个 CISA CE 控制措施有关。CISA CE 控制可以与多个 AWS Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
您的员工-1	培养意识文化，鼓励员工在网上做出正确的选择。	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。

控制 ID	控制描述	AWS Config 规则	指南
您的员工-2	了解网络钓鱼和商业电子邮件入侵等风险。	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
您的员工-3	保持对当前网络安全相关事件的认识，利用汲取的教训和报告的事件，对当前的威胁环境保持警惕，并对网络安全趋势保持敏捷。	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
您的员工-4	利用基本的网络安全培训，提高对网络安全概念、术语以及与实施网络安全最佳实践相关的活动的了解。	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
您的员工-5	确定专业协会、学术机构、私营部门和政府渠道提供的培训资源。	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-1	了解您的网络上有什么。维护硬件和软件资产清单，以了解哪些资产在使用中，哪些资产面临攻击风险。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
您的系统-1	了解您的网络上有什么。维护硬件和软件资产清单，以了解哪些资产在使用中，哪些资产面临攻击风险。	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-1	了解您的网络上有什么。维护硬件和软件资产清单，以了解哪些资产在使用中，哪些资产面临攻击风险。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
您的系统-1	了解您的网络上有什么。维护硬件和软件资产清单，以了解哪些资产在使用中，哪些资产面临攻击风险。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-1	了解您的网络上有什么。维护硬件和软件资产清单，以了解哪些资产在使用中，哪些资产面临攻击风险。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
您的系统-1	了解您的网络上有什么。维护硬件和软件资产清单，以了解哪些资产在使用中，哪些资产面临攻击风险。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
您的系统-1	了解您的网络上有什么。维护硬件和软件资产清单，以了解哪些资产在使用中，哪些资产面临攻击风险。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-2	利用适用于所有操作系统和第三方软件的自动更新。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
您的系统-2	利用适用于所有操作系统和第三方软件的自动更新。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-2	利用适用于所有操作系统和第三方软件的自动更新。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
您的系统-2	利用适用于所有操作系统和第三方软件的自动更新。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
您的系统-3	为所有硬件和软件资产实施安全配置。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
您的系统-3	为所有硬件和软件资产实施安全配置。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
您的系统-3	为所有硬件和软件资产实施安全配置。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
您的系统-3	为所有硬件和软件资产实施安全配置。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
您的系统-3	为所有硬件和软件资产实施安全配置。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
您的系统-3	为所有硬件和软件资产实施安全配置。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
您的系统-3	为所有硬件和软件资产实施安全配置。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
您的系统-3	为所有硬件和软件资产实施安全配置。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
您的系统-3	为所有硬件和软件资产实施安全配置。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
您的系统-3	为所有硬件和软件资产实施安全配置。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
您的系统-3	为所有硬件和软件资产实施安全配置。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
您的系统-3	为所有硬件和软件资产实施安全配置。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
您的系统-3	为所有硬件和软件资产实施安全配置。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
您的系统-3	为所有硬件和软件资产实施安全配置。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
您的系统-3	为所有硬件和软件资产实施安全配置。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
您的系统-3	为所有硬件和软件资产实施安全配置。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
您的系统-3	为所有硬件和软件资产实施安全配置。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
您的系统-3	为所有硬件和软件资产实施安全配置。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
您的系统-3	为所有硬件和软件资产实施安全配置。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
您的系统-3	为所有硬件和软件资产实施安全配置。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
您的系统-3	为所有硬件和软件资产实施安全配置。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
您的系统-3	为所有硬件和软件资产实施安全配置。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
您的系统-3	为所有硬件和软件资产实施安全配置。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
您的系统-3	为所有硬件和软件资产实施安全配置。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
您的系统-3	为所有硬件和软件资产实施安全配置。	opensearch-data-node-fault-tolerance	为了实现高可用性和容错能力，Amazon OpenSearch OpenSearch 服务（服务）至少需要三个数据节点。部署具有至少三个数据节点的 OpenSearch 服务域可确保在节点出现故障时集群运行。
您的系统-3	为所有硬件和软件资产实施安全配置。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
您的系统-3	为所有硬件和软件资产实施安全配置。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
您的系统-3	为所有硬件和软件资产实施安全配置。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
您的系统-3	为所有硬件和软件资产实施安全配置。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
您的系统-3	为所有硬件和软件资产实施安全配置。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
您的系统-3	为所有硬件和软件资产实施安全配置。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
您的系统-3	为所有硬件和软件资产实施安全配置。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
您的系统-3	为所有硬件和软件资产实施安全配置。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
您的系统-3	为所有硬件和软件资产实施安全配置。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
您的系统-3	为所有硬件和软件资产实施安全配置。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCreden tialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
您的系统-3	为所有硬件和软件资产实施安全配置。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
您的系统-3	为所有硬件和软件资产实施安全配置。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
您的系统-3	为所有硬件和软件资产实施安全配置。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
您的系统-3	为所有硬件和软件资产实施安全配置。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
您的系统-3	为所有硬件和软件资产实施安全配置。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
您的系统-3	为所有硬件和软件资产实施安全配置。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
您的系统-3	为所有硬件和软件资产实施安全配置。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
您的系统-3	为所有硬件和软件资产实施安全配置。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的系统-3	为所有硬件和软件资产实施安全配置。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
您的系统-3	为所有硬件和软件资产实施安全配置。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
您的系统-3	为所有硬件和软件资产实施安全配置。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
您的系统-3	为所有硬件和软件资产实施安全配置。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的系统-3	为所有硬件和软件资产实施安全配置。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
您的系统-3	为所有硬件和软件资产实施安全配置。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
您的系统-3	为所有硬件和软件资产实施安全配置。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
您的系统-3	为所有硬件和软件资产实施安全配置。	secretsmanager-secret-periodic-rotation	此规则可确保 S AWS ecrets Manager 密钥启用定期轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。默认值为 90 天。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays（Config 默认值：90）。实际值应反映贵组织的策略。
您的系统-3	为所有硬件和软件资产实施安全配置。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的系统-3	为所有硬件和软件资产实施安全配置。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
您的系统-3	为所有硬件和软件资产实施安全配置。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
您的系统-3	为所有硬件和软件资产实施安全配置。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
您的系统-3	为所有硬件和软件资产实施安全配置。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
您的系统-3	为所有硬件和软件资产实施安全配置。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的系统-3	为所有硬件和软件资产实施安全配置。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
您的系统-3	为所有硬件和软件资产实施安全配置。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
您的系统-3	为所有硬件和软件资产实施安全配置。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
您的系统-4	从系统中移除不受支持或未经授权的硬件和软件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
您的周围环境-1	了解谁在您的网络上。维护网络连接清单（用户、供应商、业务合作伙伴等）。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
您的周围环境-1	了解谁在您的网络上。维护网络连接清单（用户、供应商、业务合作伙伴等）。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
您的周围环境-1	了解谁在您的网络上。维护网络连接清单（用户、供应商、业务合作伙伴等）。	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	控制描述	AWS Config 规则	指南
您的周围环境-2	从特权用户、管理用户和远程访问用户开始，对所有用户进行多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
您的周围环境-2	从特权用户、管理用户和远程访问用户开始，对所有用户进行多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
您的周围环境-2	从特权用户、管理用户和远程访问用户开始，对所有用户进行多重身份验证。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
您的周围环境-2	从特权用户、管理用户和远程访问用户开始，对所有用户进行多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
您的周围环境-3	根据权限和最低权限授予访问权限 need-to-know 和管理员权限。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
您的周围环境-3	根据权限和最低权限授予访问权限 need-to-know 和管理员权限。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
您的周围环境-3	根据权限和最低权限授予访问权限 need-to-know 和管理员权限。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
您的周围环境-3	根据权限和最低权限授予访问权限 need-to-know 和管理员权限。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
您的周围环境-3	根据权限和最低权限授予访问权限 need-to-know 和管理员权限。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
您的周围环境-3	根据权限和最低权限授予访问权限 need-to-know 和管理员权限。	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
您的周围环境-3	根据权限和最低权限授予访问权限 need-to-know 和管理员权限。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch

控制 ID	控制描述	AWS Config 规则	指南
您的周围环境-4	为所有用户使用唯一的密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-1	了解您的数据如何受到保护。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
您的数据-1	了解您的数据如何受到保护。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
您的数据-1	了解您的数据如何受到保护。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-1	了解您的数据如何受到保护。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
您的数据-1	了解您的数据如何受到保护。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
您的数据-1	了解您的数据如何受到保护。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
您的数据-1	了解您的数据如何受到保护。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-1	了解您的数据如何受到保护。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-1	了解您的数据如何受到保护。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
您的数据-1	了解您的数据如何受到保护。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
您的数据-1	了解您的数据如何受到保护。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-1	了解您的数据如何受到保护。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
您的数据-1	了解您的数据如何受到保护。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
您的数据-1	了解您的数据如何受到保护。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-1	了解您的数据如何受到保护。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-1	了解您的数据如何受到保护。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-1	了解您的数据如何受到保护。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-1	了解您的数据如何受到保护。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
您的数据-1	了解您的数据如何受到保护。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-1	了解您的数据如何受到保护。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
您的数据-1	了解您的数据如何受到保护。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
您的数据-1	了解您的数据如何受到保护。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-1	了解您的数据如何受到保护。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-1	了解您的数据如何受到保护。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls （配置默认值：True）、blockPublicPolicy （配置默认值：True）和参数 blockPublicAcls （配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件， data-at-rest 以及传输和用户行为活动。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
您的数据-2	了解您的网络上正在发生的事情。管理网络和外围组件、主机和设备组件，data-at-rest 以及传输和用户行为活动。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-3	域名系统保护。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
您的数据-4	建立关键系统的定期自动备份和冗余。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
您的数据-4	建立关键系统的定期自动备份和冗余。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-4	建立关键系统的定期自动备份和冗余。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
您的数据-4	建立关键系统的定期自动备份和冗余。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
您的数据-4	建立关键系统的定期自动备份和冗余。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-4	建立关键系统的定期自动备份和冗余。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
您的数据-4	建立关键系统的定期自动备份和冗余。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-4	建立关键系统的定期自动备份和冗余。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
您的数据-4	建立关键系统的定期自动备份和冗余。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-4	建立关键系统的定期自动备份和冗余。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
您的数据-4	建立关键系统的定期自动备份和冗余。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-4	建立关键系统的定期自动备份和冗余。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
您的数据-4	建立关键系统的定期自动备份和冗余。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-4	建立关键系统的定期自动备份和冗余。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-4	建立关键系统的定期自动备份和冗余。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-4	建立关键系统的定期自动备份和冗余。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
您的数据-4	建立关键系统的定期自动备份和冗余。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
您的数据-4	建立关键系统的定期自动备份和冗余。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
您的数据-5	利用备份保护，包括物理安全、加密和离线副本。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
您的数据-5	利用备份保护，包括物理安全、加密和离线副本。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
您的危机应对措施-2	领导开发内部报告结构，以检测、交流和遏制攻击。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
您的危机应对措施-2	领导开发内部报告结构，以检测、交流和遏制攻击。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
启动：首先要做的事情-1	采用自动持续备份关键数据和系统配置的备份解决方案。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-2	尽可能要求在访问系统时使用多重身份验证 (MFA)。应要求所有用户使用多重身份验证，但应从特权用户、管理用户和远程访问用户开始。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
启动：首先要做的事情-2	尽可能要求在访问系统时使用多重身份验证 (MFA)。应要求所有用户使用多重身份验证，但应从特权用户、管理用户和远程访问用户开始。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
启动：首先要做的事情-2	尽可能要求在访问系统时使用多重身份验证 (MFA)。应要求所有用户使用多重身份验证，但应从特权用户、管理用户和远程访问用户开始。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-2	尽可能要求在访问系统时使用多重身份验证 (MFA)。应要求所有用户使用多重身份验证，但应从特权用户、管理用户和远程访问用户开始。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
启动：首先要做的事情-3	尽可能启用自动更新。更换不支持的操作系统、应用程序和硬件。快速测试和部署补丁。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
启动：首先要做的事情-3	尽可能启用自动更新。更换不支持的操作系统、应用程序和硬件。快速测试和部署补丁。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
启动：首先要做的事情-3	尽可能启用自动更新。更换不支持的操作系统、应用程序和硬件。快速测试和部署补丁。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
启动：首先要做的事情-3	尽可能启用自动更新。更换不支持的操作系统、应用程序和硬件。快速测试和部署补丁。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

模板

该模板可在以下网址获得 GitHub：CISA Cyber Essentials 运营最佳实践。

刑事司法信息服务 (CJIS) 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了刑事司法信息服务 (CJIS) 合规要求和 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CJIS 控件相关。一个 CJIS 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
5.2	安全意识培训	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
5.3	事件响应	response-plan-exists-maintained（流程检查）	确保制定和维护事件响应计划，并将其分发给负责人。更新并正式记录响应计划，有助于确保响应人员了解自己的角色、责任以及在事件发生时应遵循的流程。
5.3	事件响应	response-plan-tested（流程检查）	确保对事件响应和恢复计划进行测试。这有助于了解您的计划在事件期间是否有效，以及是否需要弥补任何不足或进行更新。

控制 ID	控制描述	AWS Config 规则	指南
5.4	审计和问责	audit-log-policy-exists（过程检查）	制定并维护审计日志管理策略，以定义贵组织的日志记录要求。这包括但不限于审查和保留审计日志。
5.4.1	可审计的事件和内容（信息系统）	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
5.4.1	可审计的事件和内容（信息系统）	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
5.4.1	可审计的事件和内容（信息系统）	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
5.4.1	可审计的事件和内容（信息系统）	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
5.4.1	可审计的事件和内容（信息系统）	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
5.4.1	可审计的事件和内容（信息系统）	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。

控制 ID	控制描述	AWS Config 规则	指南
5.4.1	可审计的事件和内容（信息系统）	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
5.4.1	可审计的事件和内容（信息系统）	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
5.4.1	可审计的事件和内容（信息系统）	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
5.4.1	可审计的事件和内容（信息系统）	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
5.4.1	可审计的事件和内容（信息系统）	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
5.4.1	可审计的事件和内容（信息系统）	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
5.4.1	可审计的事件和内容（信息系统）	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
5.4.1	可审计的事件和内容（信息系统）	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
5.4.1	可审计的事件和内容（信息系统）	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	控制描述	AWS Config 规则	指南
5.4.1	可审计的事件和内容（信息系统）	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
5.4.1	可审计的事件和内容（信息系统）	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
5.4.5	保护审计信息	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
5.4.5	保护审计信息	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
5.4.5	保护审计信息	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。
5.4.6	审计记录保留	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
5.4.6	审计记录保留	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
5.5.2	强制访问权限	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
5.5.2	强制访问权限	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2	强制访问权限	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
5.5.2	强制访问权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2	强制访问权限	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为 IAM 密码策略设置 RequireUppercaseCharacters（CJIS 值：假）、RequireLowercaseCharacters（CJIS 值：假）、 RequireSymbols（CJIS 值：假）、 RequireNumbers（CJIS 值：假）、（CJIS 值：false）、 MinimumPasswordLength（CJIS 值：8）、 PasswordReusePrevention（CJIS 值：10）和 MaxPasswordAge（CJIS 值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2	强制访问权限	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
5.5.2	强制访问权限	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
5.5.2	强制访问权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2	强制访问权限	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
5.5.2	强制访问权限	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2	强制访问权限	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
5.5.2	强制访问权限	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2	强制访问权限	rds-instance-iam-authentication-enabled	确保在亚马逊关系数据库服务 (Amazon RDS) 实例上启用 AWS 身份和访问管理 (IAM) 身份验证，以控制对系统和资产的访问。这会强制进出数据库的网络流量使用安全套接字层 (SSL) 进行加密。您无需将用户凭证存储在数据库中，因为身份验证在外部进行管理。
5.5.2	强制访问权限	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2.1	最低权限	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。
5.5.2.1	最低权限	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2.1	最低权限	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2.1	最低权限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
5.5.2.1	最低权限	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2.1	最低权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
5.5.2.1	最低权限	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
5.5.2.1	最低权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2.1	最低权限	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
5.5.2.1	最低权限	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2.1	最低权限	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
5.5.2.1	最低权限	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。
5.5.2.1	最低权限	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

控制 ID	控制描述	AWS Config 规则	指南
5.5.2.1	最低权限	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays（Config 默认值：90）。实际值应反映贵组织的策略。
5.5.6	远程访问	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
5.5.6	远程访问	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
5.6.2.1.1	密码	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为 IAM 密码策略设置 RequireUppercaseCharacters（CJIS 值：假）、RequireLowercaseCharacters（CJIS 值：假）、 RequireSymbols（CJIS 值：假）、 RequireNumbers（CJIS 值：假）、（CJIS 值：false）、 MinimumPasswordLength（CJIS 值：8）、 PasswordReusePrevention（CJIS 值：10）和 MaxPasswordAge（CJIS 值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.6.2.2	高级身份验证	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
5.6.2.2	高级身份验证	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
5.6.2.2	高级身份验证	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
5.6.2.2	高级身份验证	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
5.6.2.2	高级身份验证	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
5.6.3.1	标识符管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
5.7.1.1	最少功能	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
5.7.1.1	最少功能	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
5.7.1.1	最少功能	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
5.7.1.1	最少功能	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
5.7.1.1	最少功能	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
5.7.1.1	最少功能	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
5.7.1.1	最少功能	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
5.7.1.1	最少功能	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
5.7.1.1	最少功能	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
5.7.1.1	最少功能	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
5.7.1.1	最少功能	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
5.7.1.1	最少功能	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
5.7.1.1	最少功能	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
5.7.1.1	最少功能	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
5.7.1.1	最少功能	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
5.7.1.1	最少功能	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.7.1.1	最少功能	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
5.7.1.1	最少功能	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
5.10	系统和通信保护与信息完整性	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10	系统和通信保护与信息完整性	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10	系统和通信保护与信息完整性	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
5.10	系统和通信保护与信息完整性	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10	系统和通信保护与信息完整性	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10	系统和通信保护与信息完整性	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10	系统和通信保护与信息完整性	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.10	系统和通信保护与信息完整性	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10	系统和通信保护与信息完整性	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
5.10	系统和通信保护与信息完整性	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10	系统和通信保护与信息完整性	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。

控制 ID	控制描述	AWS Config 规则	指南
5.10	系统和通信保护与信息完整性	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
5.10	系统和通信保护与信息完整性	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
5.10.1	强制执行信息流	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10.1	强制执行信息流	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10.1	强制执行信息流	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
5.10.1	强制执行信息流	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10.1	强制执行信息流	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
5.10.1	强制执行信息流	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
5.10.1	强制执行信息流	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
5.10.1	强制执行信息流	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
5.10.1	强制执行信息流	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
5.10.1	强制执行信息流	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
5.10.1	强制执行信息流	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
5.10.1	强制执行信息流	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
5.10.1	强制执行信息流	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
5.10.1	强制执行信息流	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
5.10.1	强制执行信息流	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
5.10.1	强制执行信息流	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1	强制执行信息流	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
5.10.1.1	边界保护	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.1	边界保护	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
5.10.1.1	边界保护	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
5.10.1.1	边界保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.1	边界保护	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
5.10.1.1	边界保护	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.1	边界保护	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
5.10.1.1	边界保护	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon OpenSearch 服务域的连接启用 HTTPS。
5.10.1.1	边界保护	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。
5.10.1.1	边界保护	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.1	边界保护	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
5.10.1.2	加密	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10.1.2	加密	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10.1.2	加密	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
5.10.1.2	加密	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
5.10.1.2	加密	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
5.10.1.2	加密	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
5.10.1.2	加密	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
5.10.1.2	加密	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
5.10.1.2	加密	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
5.10.1.2	加密	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10.1.2	加密	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
5.10.1.2	加密	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10.1.2	加密	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
5.10.1.2	加密	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
5.10.1.2	加密	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
5.10.1.2	加密	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
5.10.1.2	加密	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10.1.2	加密	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
5.10.1.2	加密	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
5.10.1.2	加密	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
5.10.1.2	加密	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.2	加密	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
5.10.1.2	加密	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
5.10.1.2	加密	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.3	入侵检测工具和技术	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
5.10.1.3	入侵检测工具和技术	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
5.10.1.3	入侵检测工具和技术	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
5.10.4.1	补丁管理	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
5.10.4.1	补丁管理	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
5.10.4.1	补丁管理	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
5.10.4.1	补丁管理	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。要协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。
5.10.4.1	补丁管理	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
5.10.4.4	安全警报和建议	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
5.10.4.4	安全警报和建议	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
5.10.4.4	安全警报和建议	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

模板

该模板可在以下网址获得 GitHub：CJIS 操作最佳实践。

CMMC Level 1 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了网络安全成熟度模型认证 (CMMC) 第 1 级与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CMMC 1 级控件相关。一个 CMMC Level 1 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因

控制 ID	控制描述	AWS Config 规则	指南
			此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.1.211	在组织信息系统的适当位置提供恶意代码防护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

模板

该模板可在以下网址获得 GitHub：CMMC 第 1 级运营最佳实践。

CMMC Level 2 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了网络安全成熟度模型认证 (CMMC) 第 2 级和 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CMMC 2 级控件相关。一个 CMMC Level 2 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理

控制 ID	控制描述	AWS Config 规则	指南
	程或设备（包括其他信息系统）访问信息系统。		对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.013	监视和控制远程访问会话。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AC.2.013	监视和控制远程访问会话。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.013	监视和控制远程访问会话。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AC.2.013	监视和控制远程访问会话。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.2.016	根据批准的授权控制 CUI 流。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
AC.2.016	根据批准的授权控制 CUI 流。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.2.016	根据批准的授权控制 CUI 流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.2.016	根据批准的授权控制 CUI 流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
AC.2.016	根据批准的授权控制 CUI 流。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC.2.016	根据批准的授权控制 CUI 流。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.016	根据批准的授权控制 CUI 流。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.2.016	根据批准的授权控制 CUI 流。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.2.016	根据批准的授权控制 CUI 流。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.2.016	根据批准的授权控制 CUI 流。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
CA.2.159	制定和实施旨在纠正缺陷并减少或消除组织系统漏洞的行动计划。	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.063	控制和监控用户安装的软件。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.2.063	控制和监控用户安装的软件。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.063	控制和监控用户安装的软件。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.2.078	在创建新密码时，强制执行最低密码复杂度和更改字符的规定。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.079	禁止在指定的次数范围内重复使用密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
IA.2.081	仅存储和传输受加密保护的密码。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
IA.2.081	仅存储和传输受加密保护的密码。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
IA.2.081	仅存储和传输受加密保护的密码。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	response-plan-exists-maintained（流程检查）	确保制定和维护事件响应计划，并将其分发给负责人。更新并正式记录响应计划，有助于确保响应人员了解自己的角色、责任以及在事件发生时应遵循的流程。
IR.2.093	检测和报告事件。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.093	检测和报告事件。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
IR.2.093	检测和报告事件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.093	检测和报告事件。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
IR.2.093	检测和报告事件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
MA.2.113	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
MA.2.113	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
RE.2.137	定期执行和测试数据备份。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.2.137	定期执行和测试数据备份。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.2.137	定期执行和测试数据备份。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
RE.2.137	定期执行和测试数据备份。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RE.2.137	定期执行和测试数据备份。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
RE.2.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	vuln-scans-performed（流程检查）	确保根据您的合规要求执行漏洞扫描。扫描节奏、使用的工具和结果的使用应由您的组织定义。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.2.179	使用加密会话管理网络设备。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.2.179	使用加密会话管理网络设备。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC.2.179	使用加密会话管理网络设备。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC.2.179	使用加密会话管理网络设备。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.2.179	使用加密会话管理网络设备。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.1.211	在组织信息系统的适当位置提供恶意代码防护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SI.2.217	识别对组织系统的未经授权使用。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SI.2.217	识别对组织系统的未经授权使用。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.2.217	识别对组织系统的未经授权使用。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
SI.2.217	识别对组织系统的未经授权使用。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
SI.2.217	识别对组织系统的未经授权使用。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.217	识别对组织系统的未经授权使用。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

模板

该模板可在以下网址获得 GitHub：CMMC 第 2 级运营最佳实践。

CMMC Level 3 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了网络安全成熟度模型认证 (CMMC) 第 3 级与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CMMC 3 级控件相关。一个 CMMC Level 3 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

> **Note**
>
> 根据国防部和CMMC认证机构就CMMC3-5级的FedRAMP互惠性提供了初步指导，因此建议客户此时 AWS GovCloud 使用（美国）地区来处理任何需要符合CMMC 3-5级的工作负载。因此，为避免混淆，合规包控制台中不提供 CMMC Level 3 - 5 的合规包模板。客户可以使用本文档中链接的示例 YAML 文件，独立安装 CMMC 第 3-5 级（不带一致性包模板）的暂定指南的 Con CloudFormation fig 规则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：

控制 ID	控制描述	AWS Config 规则	指南
			90）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.013	监视和控制远程访问会话。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AC.2.013	监视和控制远程访问会话。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.013	监视和控制远程访问会话。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AC.2.013	监视和控制远程访问会话。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.2.016	根据批准的授权控制 CUI 流。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
AC.2.016	根据批准的授权控制 CUI 流。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.2.016	根据批准的授权控制 CUI 流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.2.016	根据批准的授权控制 CUI 流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
AC.2.016	根据批准的授权控制 CUI 流。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC.2.016	根据批准的授权控制 CUI 流。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.016	根据批准的授权控制 CUI 流。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.2.016	根据批准的授权控制 CUI 流。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.2.016	根据批准的授权控制 CUI 流。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.2.016	根据批准的授权控制 CUI 流。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.046	在审计日志记录过程失败时发出警报。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU.3.046	在审计日志记录过程失败时发出警报。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.046	在审计日志记录过程失败时发出警报。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU.3.046	在审计日志记录过程失败时发出警报。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
AU.3.051	关联审计记录审查、分析和报告流程，以便调查和应对非法、未授权、可疑或异常活动的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.051	关联审计记录审查、分析和报告流程，以便调查和应对非法、未授权、可疑或异常活动的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CA.2.159	制定和实施旨在纠正缺陷并减少或消除组织系统漏洞的行动计划。	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。

控制 ID	控制描述	AWS Config 规则	指南
CA.3.161	持续监控安全控制措施，以确保控制措施的持续有效性。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
CA.3.161	持续监控安全控制措施，以确保控制措施的持续有效性。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CA.3.161	持续监控安全控制措施，以确保控制措施的持续有效性。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.063	控制和监控用户安装的软件。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.2.063	控制和监控用户安装的软件。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.063	控制和监控用户安装的软件。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.2.078	在创建新密码时，强制执行最低密码复杂度和更改字符的规定。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.079	禁止在指定的次数范围内重复使用密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
IA.2.081	仅存储和传输受加密保护的密码。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
IA.2.081	仅存储和传输受加密保护的密码。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
IA.2.081	仅存储和传输受加密保护的密码。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.3.086	在规定的非活动时间后禁用标识符。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.3.086	在规定的非活动时间后禁用标识符。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
IR.2.093	检测和报告事件。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.093	检测和报告事件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
IR.2.093	检测和报告事件。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.093	检测和报告事件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
MA.2.113	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
MA.2.113	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
RE.2.137	定期执行和测试数据备份。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.2.137	定期执行和测试数据备份。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.2.137	定期执行和测试数据备份。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
RE.2.137	定期执行和测试数据备份。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RE.2.137	定期执行和测试数据备份。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
RE.2.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.2.179	使用加密会话管理网络设备。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.2.179	使用加密会话管理网络设备。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC.2.179	使用加密会话管理网络设备。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC.2.179	使用加密会话管理网络设备。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.2.179	使用加密会话管理网络设备。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.187	为组织系统中使用的密码技术建立和管理加密密钥。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.187	为组织系统中使用的密码技术建立和管理加密密钥。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC.3.190	保护通信会话的真实性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.190	保护通信会话的真实性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.190	保护通信会话的真实性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.3.190	保护通信会话的真实性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.3.190	保护通信会话的真实性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.190	保护通信会话的真实性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
SC.3.191	保护静态 CUI 的机密性。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC.3.191	保护静态 CUI 的机密性。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC.3.191	保护静态 CUI 的机密性。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.1.211	在组织信息系统的适当位置提供恶意代码防护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.213	定期扫描信息系统，并在下载、打开或执行来自外部来源的文件时实时扫描。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SI.2.217	识别对组织系统的未经授权使用。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SI.2.217	识别对组织系统的未经授权使用。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.2.217	识别对组织系统的未经授权使用。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
SI.2.217	识别对组织系统的未经授权使用。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
SI.2.217	识别对组织系统的未经授权使用。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.217	识别对组织系统的未经授权使用。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

模板

该模板可在以下网址获得 GitHub：CMMC 第 3 级运营最佳实践。

CMMC Level 4 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了网络安全成熟度模型认证 (CMMC) 第 4 级与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CMMC 4 级控件相关。一个 CMMC Level 4 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

> **Note**
>
> 根据国防部和CMMC认证机构就CMMC3-5级的FedRAMP互惠性提供了初步指导，因此建议客户此时 AWS GovCloud 使用（美国）地区来处理任何需要符合CMMC 3-5级的工作负载。因此，为避免混淆，合规包控制台中不提供 CMMC Level 3 - 5 的合规包模板。客户可以使用本文档中链接的示例 YAML 文件，独立安装 CMMC 第 3-5 级（不带一致性包模板）的暂定指南的 Con CloudFormation fig 规则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：9

控制 ID	控制描述	AWS Config 规则	指南
			0）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.013	监视和控制远程访问会话。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AC.2.013	监视和控制远程访问会话。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.013	监视和控制远程访问会话。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AC.2.013	监视和控制远程访问会话。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.2.016	根据批准的授权控制 CUI 流。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
AC.2.016	根据批准的授权控制 CUI 流。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.2.016	根据批准的授权控制 CUI 流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.2.016	根据批准的授权控制 CUI 流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
AC.2.016	根据批准的授权控制 CUI 流。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC.2.016	根据批准的授权控制 CUI 流。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.016	根据批准的授权控制 CUI 流。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.2.016	根据批准的授权控制 CUI 流。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.2.016	根据批准的授权控制 CUI 流。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.2.016	根据批准的授权控制 CUI 流。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AC.4.023	控制联网系统上安全域之间的信息流。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
AC.4.023	控制联网系统上安全域之间的信息流。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.4.023	控制联网系统上安全域之间的信息流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.4.023	控制联网系统上安全域之间的信息流。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.4.023	控制联网系统上安全域之间的信息流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.4.023	控制联网系统上安全域之间的信息流。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.4.023	控制联网系统上安全域之间的信息流。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.4.023	控制联网系统上安全域之间的信息流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.4.023	控制联网系统上安全域之间的信息流。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.4.023	控制联网系统上安全域之间的信息流。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.4.023	控制联网系统上安全域之间的信息流。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.4.023	控制联网系统上安全域之间的信息流。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AM.4.226	利用功能来发现和识别库存中具有特定组件属性（例如固件级别、操作系统类型）的系统。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
AM.4.226	利用功能来发现和识别库存中具有特定组件属性（例如固件级别、操作系统类型）的系统。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
AM.4.226	利用功能来发现和识别库存中具有特定组件属性（例如固件级别、操作系统类型）的系统。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.046	在审计日志记录过程失败时发出警报。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU.3.046	在审计日志记录过程失败时发出警报。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.046	在审计日志记录过程失败时发出警报。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU.3.046	在审计日志记录过程失败时发出警报。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
AU.3.051	关联审计记录审查、分析和报告流程，以便调查和应对非法、未授权、可疑或异常活动的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.051	关联审计记录审查、分析和报告流程，以便调查和应对非法、未授权、可疑或异常活动的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AU.4.053	自动分析审计日志，以识别关键指标 (TTP) 和/或组织定义的可疑活动并采取行动。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU.4.053	自动分析审计日志，以识别关键指标 (TTP) 和/或组织定义的可疑活动并采取行动。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.4.053	自动分析审计日志，以识别关键指标 (TTP) 和/或组织定义的可疑活动并采取行动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU.4.053	自动分析审计日志，以识别关键指标 (TTP) 和/或组织定义的可疑活动并采取行动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AU.4.054	除每台计算机的活动外，还要查看有关广泛活动的审计信息。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU.4.054	除每台计算机的活动外，还要查看有关广泛活动的审计信息。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AU.4.054	除每台计算机的活动外，还要查看有关广泛活动的审计信息。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CA.3.161	持续监控安全控制措施，以确保控制措施的持续有效性。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
CA.3.161	持续监控安全控制措施，以确保控制措施的持续有效性。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CA.3.161	持续监控安全控制措施，以确保控制措施的持续有效性。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.063	控制和监控用户安装的软件。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.2.063	控制和监控用户安装的软件。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.063	控制和监控用户安装的软件。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.2.078	在创建新密码时，强制执行最低密码复杂度和更改字符的规定。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.079	禁止在指定的次数范围内重复使用密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
IA.2.081	仅存储和传输受加密保护的密码。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
IA.2.081	仅存储和传输受加密保护的密码。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
IA.2.081	仅存储和传输受加密保护的密码。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.3.086	在规定的非活动时间后禁用标识符。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.3.086	在规定的非活动时间后禁用标识符。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
IR.2.093	检测和报告事件。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.093	检测和报告事件。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
IR.2.093	检测和报告事件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.093	检测和报告事件。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
IR.2.093	检测和报告事件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
MA.2.113	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
MA.2.113	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
RE.2.137	定期执行和测试数据备份。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.2.137	定期执行和测试数据备份。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.2.137	定期执行和测试数据备份。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
RE.2.137	定期执行和测试数据备份。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RE.2.137	定期执行和测试数据备份。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
RE.2.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
RM.4.150	利用威胁情报为系统和安全架构的开发、安全解决方案的选择、监控、威胁搜寻以及响应和恢复活动提供信息。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
RM.4.151	通过组织的互联网网络边界和组织定义的其他边界，扫描周边网络边界上的未经授权端口。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
RM.4.151	通过组织的互联网网络边界和组织定义的其他边界，扫描周边网络边界上的未经授权端口。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
RM.4.151	通过组织的互联网网络边界和组织定义的其他边界，扫描周边网络边界上的未经授权端口。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
RM.4.151	通过组织的互联网网络边界和组织定义的其他边界，扫描周边网络边界上的未经授权端口。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SA.4.171	建立并维护网络威胁搜寻能力，以搜索组织系统中的漏洞指标，并检测、跟踪和破坏逃避现有控制的威胁。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.2.179	使用加密会话管理网络设备。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.2.179	使用加密会话管理网络设备。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC.2.179	使用加密会话管理网络设备。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC.2.179	使用加密会话管理网络设备。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.2.179	使用加密会话管理网络设备。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.187	为组织系统中使用的密码技术建立和管理加密密钥。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.187	为组织系统中使用的密码技术建立和管理加密密钥。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC.3.190	保护通信会话的真实性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.190	保护通信会话的真实性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.190	保护通信会话的真实性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.3.190	保护通信会话的真实性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.3.190	保护通信会话的真实性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.190	保护通信会话的真实性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
SC.3.191	保护静态 CUI 的机密性。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC.3.191	保护静态 CUI 的机密性。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC.3.191	保护静态 CUI 的机密性。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.4.199	利用威胁情报主动阻止 DNS 请求到达恶意域。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.4.199	利用威胁情报主动阻止 DNS 请求到达恶意域。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SC.4.202	使用机制来分析穿越互联网网络边界或其他组织定义边界的可执行代码和脚本（例如沙箱）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.1.211	在组织信息系统的适当位置提供恶意代码防护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.213	定期扫描信息系统，并在下载、打开或执行来自外部来源的文件时实时扫描。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SI.2.217	识别对组织系统的未经授权使用。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SI.2.217	识别对组织系统的未经授权使用。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.2.217	识别对组织系统的未经授权使用。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
SI.2.217	识别对组织系统的未经授权使用。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
SI.2.217	识别对组织系统的未经授权使用。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.217	识别对组织系统的未经授权使用。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI.4.221	使用与受保护的信息和系统相关的威胁指标信息以及从外部组织获得的有效缓解措施，为入侵检测和威胁搜寻提供信息。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

模板

该模板可在以下网址获得 GitHub：CMMC 第 4 级运营最佳实践。

CMMC Level 5 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了网络安全成熟度模型认证 (CMMC) 第 5 级与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CMMC 5 级控件相关。一个 CMMC Level 5 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

> **Note**
>
> 根据国防部和CMMC认证机构就CMMC3-5级的FedRAMP互惠性提供了初步指导，因此建议客户此时 AWS GovCloud 使用（美国）地区来处理任何需要符合CMMC 3-5级的工作负载。因此，为避免混淆，合规包控制台中不提供 CMMC Level 3 - 5 的合规包模板。客户可以使用本文档中链接的示例 YAML 文件，独立安装 CMMC 第 3-5 级（不带一致性包模板）的暂定指南的 Con CloudFormation fig 规则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic

控制 ID	控制描述	AWS Config 规则	指南
	信息系统）访问信息系统。		Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.001	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.1.002	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.1.003	验证和控制/限制外部信息系统的连接和使用。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.007	采用最低权限原则，包括特定的安全功能和特权账户。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.2.008	访问非安全功能时，请使用非特权账户或角色。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.013	监视和控制远程访问会话。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AC.2.013	监视和控制远程访问会话。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.013	监视和控制远程访问会话。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AC.2.013	监视和控制远程访问会话。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.2.016	根据批准的授权控制 CUI 流。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
AC.2.016	根据批准的授权控制 CUI 流。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.2.016	根据批准的授权控制 CUI 流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.2.016	根据批准的授权控制 CUI 流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
AC.2.016	根据批准的授权控制 CUI 流。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC.2.016	根据批准的授权控制 CUI 流。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.2.016	根据批准的授权控制 CUI 流。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.016	根据批准的授权控制 CUI 流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.2.016	根据批准的授权控制 CUI 流。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.2.016	根据批准的授权控制 CUI 流。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.2.016	根据批准的授权控制 CUI 流。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.2.016	根据批准的授权控制 CUI 流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.2.016	根据批准的授权控制 CUI 流。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.014	使用加密机制来保护远程访问会话的机密性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.014	使用加密机制来保护远程访问会话的机密性。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.017	分离个人职责，在不串通的情况下降低恶意活动的风险。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
AC.3.018	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AC.4.023	控制联网系统上安全域之间的信息流。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
AC.4.023	控制联网系统上安全域之间的信息流。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.4.023	控制联网系统上安全域之间的信息流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.4.023	控制联网系统上安全域之间的信息流。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.4.023	控制联网系统上安全域之间的信息流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.4.023	控制联网系统上安全域之间的信息流。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.4.023	控制联网系统上安全域之间的信息流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.4.023	控制联网系统上安全域之间的信息流。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.4.023	控制联网系统上安全域之间的信息流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.4.023	控制联网系统上安全域之间的信息流。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.4.023	控制联网系统上安全域之间的信息流。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.4.023	控制联网系统上安全域之间的信息流。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.4.023	控制联网系统上安全域之间的信息流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.4.023	控制联网系统上安全域之间的信息流。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.5.024	识别并降低与网络连接的未识别无线接入点相关的风险。	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
AM.4.226	利用功能来发现和识别库存中具有特定组件属性（例如固件级别、操作系统类型）的系统。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
AM.4.226	利用功能来发现和识别库存中具有特定组件属性（例如固件级别、操作系统类型）的系统。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
AM.4.226	利用功能来发现和识别库存中具有特定组件属性（例如固件级别、操作系统类型）的系统。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.041	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
AU.2.042	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.046	在审计日志记录过程失败时发出警报。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU.3.046	在审计日志记录过程失败时发出警报。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.046	在审计日志记录过程失败时发出警报。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU.3.046	在审计日志记录过程失败时发出警报。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
AU.3.049	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
AU.3.051	关联审计记录审查、分析和报告流程，以便调查和应对非法、未授权、可疑或异常活动的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AU.3.051	关联审计记录审查、分析和报告流程，以便调查和应对非法、未授权、可疑或异常活动的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AU.4.053	自动分析审计日志，以识别关键指标 (TTP) 和/或组织定义的可疑活动并采取行动。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU.4.053	自动分析审计日志，以识别关键指标 (TTP) 和/或组织定义的可疑活动并采取行动。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.4.053	自动分析审计日志，以识别关键指标 (TTP) 和/或组织定义的可疑活动并采取行动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU.4.053	自动分析审计日志，以识别关键指标 (TTP) 和/或组织定义的可疑活动并采取行动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AU.4.054	除每台计算机的活动外，还要查看有关广泛活动的审计信息。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU.4.054	除每台计算机的活动外，还要查看有关广泛活动的审计信息。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AU.4.054	除每台计算机的活动外，还要查看有关广泛活动的审计信息。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AU.5.055	识别未报告审计日志的资产，并确保相应的组织定义系统正在记录日志。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
CA.3.161	持续监控安全控制措施，以确保控制措施的持续有效性。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
CA.3.161	持续监控安全控制措施，以确保控制措施的持续有效性。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CA.3.161	持续监控安全控制措施，以确保控制措施的持续有效性。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CM.2.061	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CM.2.062	采用最少功能原则，将组织系统配置为仅提供基本功能。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.063	控制和监控用户安装的软件。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.2.063	控制和监控用户安装的软件。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.063	控制和监控用户安装的软件。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.064	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CM.2.065	跟踪、审查、批准或不批准，并记录对组织系统的更改。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.3.068	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CM.5.074	验证组织定义的关键安全软件或基本软件（例如，信任根、形式验证或加密签名）的完整性和正确性。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
CM.5.074	验证组织定义的关键安全软件或基本软件（例如，信任根、形式验证或加密签名）的完整性和正确性。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.5.074	验证组织定义的关键安全软件或基本软件（例如，信任根、形式验证或加密签名）的完整性和正确性。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.5.074	验证组织定义的关键安全软件或基本软件（例如，信任根、形式验证或加密签名）的完整性和正确性。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
IA.1.076	识别信息系统用户、代表用户行事的进程或设备。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.1.077	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.2.078	在创建新密码时，强制执行最低密码复杂度和更改字符的规定。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.079	禁止在指定的次数范围内重复使用密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
IA.2.081	仅存储和传输受加密保护的密码。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
IA.2.081	仅存储和传输受加密保护的密码。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
IA.2.081	仅存储和传输受加密保护的密码。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	sagemaker-notebook-instance-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.2.081	仅存储和传输受加密保护的密码。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.2.081	仅存储和传输受加密保护的密码。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA.3.083	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.3.086	在规定的非活动时间后禁用标识符。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.3.086	在规定的非活动时间后禁用标识符。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.092	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
IR.2.093	检测和报告事件。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.093	检测和报告事件。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
IR.2.093	检测和报告事件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR.2.093	检测和报告事件。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
IR.2.093	检测和报告事件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
IR.5.102	对符合事件模式的异常活动使用手动和自动的实时响应组合。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
IR.5.102	对符合事件模式的异常活动使用手动和自动的实时响应组合。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR.5.102	对符合事件模式的异常活动使用手动和自动的实时响应组合。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
IR.5.102	对符合事件模式的异常活动使用手动和自动的实时响应组合。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
MA.2.113	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
MA.2.113	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
RE.2.137	定期执行和测试数据备份。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.2.137	定期执行和测试数据备份。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.2.137	定期执行和测试数据备份。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
RE.2.137	定期执行和测试数据备份。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RE.2.137	定期执行和测试数据备份。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
RE.2.137	定期执行和测试数据备份。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
RE.2.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RE.3.139	根据组织定义，定期执行完整、全面和有弹性的数据备份。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
RE.5.140	确保信息处理设施满足组织定义的信息安全连续性、冗余性和可用性要求。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
RM.2.142	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
RM.4.150	利用威胁情报为系统和安全架构的开发、安全解决方案的选择、监控、威胁搜寻以及响应和恢复活动提供信息。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
RM.4.151	通过组织的互联网网络边界和组织定义的其他边界，扫描周边网络边界上的未经授权端口。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
RM.4.151	通过组织的互联网网络边界和组织定义的其他边界，扫描周边网络边界上的未经授权端口。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
RM.4.151	通过组织的互联网网络边界和组织定义的其他边界，扫描周边网络边界上的未经授权端口。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
RM.4.151	通过组织的互联网网络边界和组织定义的其他边界，扫描周边网络边界上的未经授权端口。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SA.4.171	建立并维护网络威胁搜寻能力，以搜索组织系统中的漏洞指标，并检测、跟踪和破坏逃避现有控制的威胁。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.1.175	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.2.179	使用加密会话管理网络设备。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.2.179	使用加密会话管理网络设备。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC.2.179	使用加密会话管理网络设备。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC.2.179	使用加密会话管理网络设备。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.2.179	使用加密会话管理网络设备。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
SC.3.180	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.3.182	防止通过共享系统资源进行未经授权和非预期的信息传输。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.185	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.187	为组织系统中使用的密码技术建立和管理加密密钥。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.187	为组织系统中使用的密码技术建立和管理加密密钥。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC.3.190	保护通信会话的真实性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.190	保护通信会话的真实性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.190	保护通信会话的真实性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.3.190	保护通信会话的真实性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.3.190	保护通信会话的真实性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.190	保护通信会话的真实性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
SC.3.191	保护静态 CUI 的机密性。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC.3.191	保护静态 CUI 的机密性。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC.3.191	保护静态 CUI 的机密性。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.3.191	保护静态 CUI 的机密性。	sagemaker-notebook-instance-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.3.191	保护静态 CUI 的机密性。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.4.199	利用威胁情报主动阻止 DNS 请求到达恶意域。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.4.199	利用威胁情报主动阻止 DNS 请求到达恶意域。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SC.4.202	使用机制来分析穿越互联网网络边界或其他组织定义边界的可执行代码和脚本（例如沙箱）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.198	配置监控系统以记录通过组织的互联网网络边界和组织定义的其他边界的数据包。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.5.198	配置监控系统以记录通过组织的互联网网络边界和组织定义的其他边界的数据包。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SC.5.198	配置监控系统以记录通过组织的互联网网络边界和组织定义的其他边界的数据包。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.5.208	除了市售解决方案外，还采用组织定义和量身定制的边界保护。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.230	强制执行端口和协议合规性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.5.230	强制执行端口和协议合规性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC.5.230	强制执行端口和协议合规性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.230	强制执行端口和协议合规性。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.5.230	强制执行端口和协议合规性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.230	强制执行端口和协议合规性。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
SC.5.230	强制执行端口和协议合规性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.5.230	强制执行端口和协议合规性。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.5.230	强制执行端口和协议合规性。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.210	及时识别、报告和纠正信息及信息系统的缺陷。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.1.211	在组织信息系统的适当位置提供恶意代码防护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.1.213	定期扫描信息系统，并在下载、打开或执行来自外部来源的文件时实时扫描。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.2.214	监控系统安全警报和建议，并采取相应措施。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.214	监控系统安全警报和建议，并采取相应措施。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.216	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SI.2.217	识别对组织系统的未经授权使用。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SI.2.217	识别对组织系统的未经授权使用。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.2.217	识别对组织系统的未经授权使用。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
SI.2.217	识别对组织系统的未经授权使用。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
SI.2.217	识别对组织系统的未经授权使用。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
SI.2.217	识别对组织系统的未经授权使用。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.2.217	识别对组织系统的未经授权使用。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI.4.221	使用与受保护的信息和系统相关的威胁指标信息以及从外部组织获得的有效缓解措施，为入侵检测和威胁搜寻提供信息。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.5.222	分析系统行为，以检测和缓解表明恶意行为的正常系统命令和脚本的执行情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.5.223	持续监控个人和系统组件是否存在异常或可疑行为。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

模板

该模板可在以下网址获得 GitHub：CMMC 第 5 级运营最佳实践。

CMMC 2.0 Level 1 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了网络安全成熟度模型认证 (CMMC) 2.0 第 1 级与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CMMC 2.0 1 级控件相关。一个 CMMC 2.0 Level 1 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因

控制 ID	控制描述	AWS Config 规则	指南
			此需要对此类账户进行访问控制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI.L1-3.14.1	及时识别、报告和纠正信息及信息系统的缺陷。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.L1-3.14.1	及时识别、报告和纠正信息及信息系统的缺陷。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.L1-3.14.1	及时识别、报告和纠正信息及信息系统的缺陷。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.L1-3.14.2	在组织信息系统的适当位置提供恶意代码防护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.L1-3.14.5	定期扫描信息系统，并在下载、打开或执行来自外部来源的文件时实时扫描。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。

模板

该模板可在以下网址获得 GitHub：CMMC 2.0 第 1 级操作最佳实践。

CMMC 2.0 Level 2 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了网络安全成熟度模型认证 (CMMC) 2.0 第 2 级与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 CMMC 2.0 2 级控件相关。一个 CMMC 2.0 Level 2 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效

控制 ID	控制描述	AWS Config 规则	指南
			期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他信息系统）访问信息系统。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.L1-3.1.2	将信息系统的访问限制在授权用户获准执行的事务类型和功能范围内。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L1-3.1.20	验证和控制/限制外部信息系统的连接和使用。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC.L2-3.1.3	根据批准的授权控制 CUI 流。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AC.L2-3.1.7	防止非特权用户执行特权功能，并在审计日志中捕获此类功能的执行情况。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.12	监视和控制远程访问会话。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AC.L2-3.1.12	监视和控制远程访问会话。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.12	监视和控制远程访问会话。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AC.L2-3.1.12	监视和控制远程访问会话。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC.L2-3.1.13	使用加密机制来保护远程访问会话的机密性。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.1	根据需要创建并保留系统审计日志和记录，以便对非法或未经授权的系统活动进行监控、分析、调查和报告。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU.L2-3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU.L2-3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU.L2-3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU.L2-3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU.L2-3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU.L2-3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.4	在审计日志记录过程失败时发出警报。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU.L2-3.3.4	在审计日志记录过程失败时发出警报。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.4	在审计日志记录过程失败时发出警报。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU.L2-3.3.4	在审计日志记录过程失败时发出警报。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.5	关联审计记录审查、分析和报告流程，以便调查和应对非法、未授权、可疑或异常活动的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU.L2-3.3.5	关联审计记录审查、分析和报告流程，以便调查和应对非法、未授权、可疑或异常活动的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
AU.L2-3.3.8	保护审计信息和审计日志记录工具免遭未经授权的访问、修改和删除。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CA.L2-3.12.2	制定和实施旨在纠正缺陷并减少或消除组织系统漏洞的行动计划。	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。

控制 ID	控制描述	AWS Config 规则	指南
CA.L2-3.12.3	持续监控安全控制措施，以确保控制措施的持续有效性。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CA.L2-3.12.3	持续监控安全控制措施，以确保控制措施的持续有效性。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CA.L2-3.12.3	持续监控安全控制措施，以确保控制措施的持续有效性。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CM.L2-3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.L2-3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
CM.L2-3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.2	为组织系统中使用的信息技术产品建立并强制执行安全配置设置。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CM.L2-3.4.3	跟踪、审查、批准或不批准，并记录对组织系统的更改。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CM.L2-3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.7	限制、禁用或阻止使用不必要的程序、功能、端口、协议和服务。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CM.L2-3.4.9	控制和监控用户安装的软件。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM.L2-3.4.9	控制和监控用户安装的软件。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM.L2-3.4.9	控制和监控用户安装的软件。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
IA.L1-3.5.1	识别信息系统用户、代表用户行事的进程或设备。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.L1-3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织信息系统的先决条件。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA.L2-3.5.3	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA.L2-3.5.3	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.3	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA.L2-3.5.3	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.6	在规定的非活动时间后禁用标识符。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.6	在规定的非活动时间后禁用标识符。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.7	在创建新密码时，强制执行最低密码复杂度和更改字符的规定。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.8	禁止在指定的次数范围内重复使用密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
IA.L2-3.5.10	仅存储和传输受加密保护的密码。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IR.L2-3.6.1	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR.L2-3.6.1	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
IR.L2-3.6.1	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
IR.L2-3.6.1	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
IR.L2-3.6.3	测试组织的事件响应能力。	response-plan-tested（流程检查）	确保对事件响应和恢复计划进行测试。这有助于了解您的计划在事件期间是否有效，以及是否需要弥补任何不足或进行更新。

控制 ID	控制描述	AWS Config 规则	指南
MA.L2-3.7.5	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
MA.L2-3.7.5	需要多重身份验证才能通过外部网络连接建立非本地维护会话，并在非本地维护完成后终止此类连接。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
RA.L2-3.11.2	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
RA.L2-3.11.2	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
RA.L2-3.11.2	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
RA.L2-3.11.2	定期扫描组织系统和应用程序中的漏洞，并在发现影响这些系统和应用程序的新漏洞时进行扫描。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.L1-3.13.1	在信息系统的外部边界和关键内部边界监控、控制和保护组织通信（即组织信息系统传输或接收的信息）。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
SC.L2-3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC.L2-3.13.4	防止通过共享系统资源进行未经授权和非预期的信息传输。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L2-3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L2-3.13.10	为组织系统中使用的密码技术建立和管理加密密钥。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.10	为组织系统中使用的密码技术建立和管理加密密钥。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC.L2-3.13.15	保护通信会话的真实性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L2-3.13.15	保护通信会话的真实性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.15	保护通信会话的真实性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.L2-3.13.15	保护通信会话的真实性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC.L2-3.13.15	保护通信会话的真实性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.15	保护通信会话的真实性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC.L2-3.13.16	保护静态 CUI 的机密性。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC.L2-3.13.16	保护静态 CUI 的机密性。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
SC.L2-3.13.16	保护静态 CUI 的机密性。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.16	保护静态 CUI 的机密性。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.L2-3.13.16	保护静态 CUI 的机密性。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC.L2-3.13.16	保护静态 CUI 的机密性。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC.L2-3.13.16	保护静态 CUI 的机密性。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.16	保护静态 CUI 的机密性。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.L2-3.13.16	保护静态 CUI 的机密性。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.L2-3.13.16	保护静态 CUI 的机密性。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.16	保护静态 CUI 的机密性。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC.L2-3.13.16	保护静态 CUI 的机密性。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.L2-3.13.16	保护静态 CUI 的机密性。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC.L2-3.13.16	保护静态 CUI 的机密性。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SC.L2-3.13.16	保护静态 CUI 的机密性。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC.L2-3.13.16	保护静态 CUI 的机密性。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SI.L1-3.14.1	及时识别、报告和纠正信息及信息系统的缺陷。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.L1-3.14.1	及时识别、报告和纠正信息及信息系统的缺陷。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.L1-3.14.1	及时识别、报告和纠正信息及信息系统的缺陷。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.L1-3.14.2	在组织信息系统的适当位置提供恶意代码防护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.L1-3.14.5	定期扫描信息系统，并在下载、打开或执行来自外部来源的文件时实时扫描。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
SI.L2-3.14.3	监控系统安全警报和建议，并采取相应措施。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SI.L2-3.14.3	监控系统安全警报和建议，并采取相应措施。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.3	监控系统安全警报和建议，并采取相应措施。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI.L2-3.14.3	监控系统安全警报和建议，并采取相应措施。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.3	监控系统安全警报和建议，并采取相应措施。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.L2-3.14.3	监控系统安全警报和建议，并采取相应措施。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.3	监控系统安全警报和建议，并采取相应措施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.L2-3.14.3	监控系统安全警报和建议，并采取相应措施。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.3	监控系统安全警报和建议，并采取相应措施。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.L2-3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SI.L2-3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
SI.L2-3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI.L2-3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.L2-3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.7	识别对组织系统的未经授权使用。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SI.L2-3.14.7	识别对组织系统的未经授权使用。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SI.L2-3.14.7	识别对组织系统的未经授权使用。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.7	识别对组织系统的未经授权使用。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI.L2-3.14.7	识别对组织系统的未经授权使用。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.7	识别对组织系统的未经授权使用。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
SI.L2-3.14.7	识别对组织系统的未经授权使用。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.7	识别对组织系统的未经授权使用。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
SI.L2-3.14.7	识别对组织系统的未经授权使用。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.7	识别对组织系统的未经授权使用。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
SI.L2-3.14.7	识别对组织系统的未经授权使用。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI.L2-3.14.7	识别对组织系统的未经授权使用。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

模板

该模板可在以下网址获得 GitHub：CMMC 2.0 第 2 级操作最佳实践。

计算服务操作最佳实践

此一致性包包含基于计算服务的 AWS Config 规则。有关更多信息，请参阅适用于任何工作负载的计算。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：计算服务最佳运营实践。

数据弹性操作最佳实践

有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：数据弹性运营最佳实践。

数据库服务操作最佳实践

此一致性包包含基于数据库服务的 AWS Config 规则。有关更多信息，请参阅上的数据库 AWS。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：数据库服务最佳操作实践。

数据湖和分析服务操作最佳实践

此一致性包包含数据湖和分析服务的 AWS Config 规则。有关更多信息，请参阅上的 “数据湖和分析” AWS。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：数据湖和分析服务的运营最佳实践。

DevOps 操作最佳实践

此一致性包包含基于 DevOps 内部 AWS的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：的运营最佳实践 DevOps。

EC2 操作最佳实践

此一致性包包含基于 EC2 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：EC2 最佳运营实践。

加密和密钥管理操作最佳实践

有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：加密和密钥管理最佳操作实践。

适用于 SME 的 ENISA 网络安全指南操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了欧盟网络安全局 (ENISA) 中小企业网络安全指南与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 ENISA 中小企业网络安全控制指南相关。适用于 SME 的 ENISA 网络安全指南控制可以与多个 Config 规则有关。有关这些映射的更多详细信息和指导，请参阅下表。

此示例合规包模板包含改编自适用于 SME 的 ENISA 网络安全指南的控制映射。有关适用于 SME 的 ENISA 网络安全指南，请参阅适用于 SME 的网络安全指南 - 保护业务安全的 12 个步骤。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：发布网络安全政策	应概述明确而具体的网络安全规则	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工

控制 ID	控制描述	AWS Config 规则	指南
			如何保护其组织免受各种安全漏洞或事件的侵害。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Managemen t。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	elasticsearch-encrypted-at-rest	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elasticsearch Service (Amazon ES) 域启用了加密。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	elasticsearch-node-to-node-encryption-check	确保已启用亚马逊 Elasticsearch Service 的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
1_培养良好的网络安全文化：记住数据保护	根据《欧盟通用数据保护条例1》的规定，任何处理或存储欧盟/欧洲经济区居民个人数据的 SME 都必须确保采取适当的安全控制措施来保护这些数据。这包括确保任何代表 SME 工作的第三方都采取适当的安全措施。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
2_提供适当的培训	定期为所有员工提供网络安全意识培训，确保他们能够识别和应对各种网络安全威胁。这些培训应针对 SME 量身定制，并侧重于实际情景。为企业内部负责管理网络安全的人员提供专门的网络安全培训，以确保他们具备完成工作所需的技能和能力。	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。

控制 ID	控制描述	AWS Config 规则	指南
4_制定事件响应计划	制定正式的事件响应计划，其中包含明确的指导方针、角色和职责，以确保以及时、专业和适当的方式应对所有安全事件。要快速应对安全威胁，请调查可在发生可疑活动或安全漏洞时监控和创建警报的工具。	response-plan-exists-maintained（流程检查）	确保制定和维护事件响应计划，并将其分发给负责人。

控制 ID	控制描述	AWS Config 规则	指南
5_安全访问系统	鼓励每个人使用口令，口令是由至少三个随机的常用单词组合而成的短语，既容易记住，又很安全。如果您选择使用典型的密码：- 使用由小写和大写字符组成的长密码，可能还应包含数字和特殊字符。- 避免使用显而易见的字母或数字序列，例如“password”、“abc”或“123”。- 避免使用可在网上找到的个人信息。而且，无论您使用口令还是密码，都不要在其他地方重复使用它们。- 不要与同事共享。- 启用多重身份验证。- 使用专用的密码管理器。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5_安全访问系统	鼓励每个人使用口令，口令是由至少三个随机的常用单词组合而成的短语，既容易记住，又很安全。如果您选择使用典型的密码：- 使用由小写和大写字符组成的长密码，可能还应包含数字和特殊字符。- 避免使用显而易见的字母或数字序列，例如“passwor d”、“abc”或“123”。- 避免使用可在网上找到的个人信息。而且，无论您使用口令还是密码，都不要在其他地方重复使用它们。- 不要与同事共享。- 启用多重身份验证。- 使用专用的密码管理器。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
5_安全访问系统	鼓励每个人使用口令，口令是由至少三个随机的常用单词组合而成的短语，既容易记住，又很安全。如果您选择使用典型的密码：- 使用由小写和大写字符组成的长密码，可能还应包含数字和特殊字符。- 避免使用显而易见的字母或数字序列，例如“passwor d”、“abc”或“123”。- 避免使用可在网上找到的个人信息。而且，无论您使用口令还是密码，都不要在其他地方重复使用它们。- 不要与同事共享。- 启用多重身份验证。- 使用专用的密码管理器。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
5_安全访问系统	鼓励每个人使用口令，口令是由至少三个随机的常用单词组合而成的短语，既容易记住，又很安全。如果您选择使用典型的密码：- 使用由小写和大写字符组成的长密码，可能还应包含数字和特殊字符。- 避免使用显而易见的字母或数字序列，例如“password”、“abc”或“123”。- 避免使用可在网上找到的个人信息。而且，无论您使用口令还是密码，都不要在其他地方重复使用它们。- 不要与同事共享。- 启用多重身份验证。- 使用专用的密码管理器。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
5_安全访问系统	鼓励每个人使用口令，口令是由至少三个随机的常用单词组合而成的短语，既容易记住，又很安全。如果您选择使用典型的密码：- 使用由小写和大写字符组成的长密码，可能还应包含数字和特殊字符。- 避免使用显而易见的字母或数字序列，例如“password”、“abc”或“123”。- 避免使用可在网上找到的个人信息。而且，无论您使用口令还是密码，都不要在其他地方重复使用它们。- 不要与同事共享。- 启用多重身份验证。- 使用专用的密码管理器。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：对软件进行修补并及时更新软件	理想情况下，使用集中式平台来管理补丁。强烈建议 SME：- 定期更新所有软件。- 尽可能启用自动更新。- 确定需要手动更新的软件和硬件。- 将移动设备和物联网设备考虑在内。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
6_保护设备：对软件进行修补并及时更新软件	理想情况下，使用集中式平台来管理补丁。强烈建议 SME：- 定期更新所有软件。- 尽可能启用自动更新。- 确定需要手动更新的软件和硬件。- 将移动设备和物联网设备考虑在内。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：对软件进行修补并及时更新软件	理想情况下，使用集中式平台来管理补丁。强烈建议 SME：- 定期更新所有软件。- 尽可能启用自动更新。- 确定需要手动更新的软件和硬件。- 将移动设备和物联网设备考虑在内。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
6_保护设备：对软件进行修补并及时更新软件	理想情况下，使用集中式平台来管理补丁。强烈建议 SME：- 定期更新所有软件。- 尽可能启用自动更新。- 确定需要手动更新的软件和硬件。- 将移动设备和物联网设备考虑在内。	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。为了协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：对软件进行修补并及时更新软件	理想情况下，使用集中式平台来管理补丁。强烈建议 SME：- 定期更新所有软件。- 尽可能启用自动更新。- 确定需要手动更新的软件和硬件。- 将移动设备和物联网设备考虑在内。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
6_保护设备：对软件进行修补并及时更新软件	理想情况下，使用集中式平台来管理补丁。强烈建议 SME：- 定期更新所有软件。- 尽可能启用自动更新。- 确定需要手动更新的软件和硬件。- 将移动设备和物联网设备考虑在内。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：对软件进行修补并及时更新软件	理想情况下，使用集中式平台来管理补丁。强烈建议 SME：- 定期更新所有软件。- 尽可能启用自动更新。- 确定需要手动更新的软件和硬件。- 将移动设备和物联网设备考虑在内。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	elasticsearch-encrypted-at-rest	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elasticsearch Service (Amazon ES) 域启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	elasticsearch-node-to-node-encryption-check	确保已启用亚马逊 Elasticsearch Service 的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
6_保护设备：加密	通过加密数据来保护数据。SME 应确保存储在笔记本电脑、智能手机和平板电脑等移动设备上的数据经过加密。对于通过公共网络（例如酒店或机场 WiFi 网络）传输的数据，请确保使用虚拟专用网络 (VPN) 或使用 SSL/TLS 协议通过安全连接访问网站，对数据进行加密。确保他们自己的网站采用合适的加密技术来保护通过互联网传输的客户数据。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	netfw-policy-rule-group-associated	AWS Network Firewall 策略定义了您的防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来过滤数据包和流量，并定义默认流量处理方式。
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。
7_保护您的网络：使用防火墙	防火墙管理进出网络的流量，是保护 SME 系统的关键工具。应部署防火墙来保护所有关键系统，特别是应使用防火墙来保护 SME 的网络免受互联网的侵害。	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	[api-gw-execution-logging-enabled](#)	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	elasticsearch-logs-to-cloudwatch	确保 Amazon Elasticsearch 服务域启用错误日志，并将其流式传输到亚马逊 CloudWatch 日志以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
7_保护您的网络：查看远程访问解决方案	SME 应定期审查任何远程访问工具，以确保其安全，特别是：- 确保所有远程访问软件都已修补并处于最新状态。- 限制从可疑地理位置或某些 IP 地址进行远程访问。- 限制员工只能远程访问其工作所需的系统和计算机。- 强制使用强密码进行远程访问，并在可能的情况下启用多重身份验证。- 确保启用监控和警报，以警示可疑攻击或异常可疑活动。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
9_保护备份	为了能够恢复关键信息，应保留备份，因为它们是从勒索软件攻击等灾难中恢复的有效方法。应该应用以下备份规则：- 定期进行备份，并尽可能自动备份，- 备份保存位置与 SME 的生产环境分开，- 备份经过加密，尤其是在要在不同地点之间移动时，- 定期从备份中恢复数据的能力已经过测试。理想情况下，应该从头到尾对整个还原过程进行定期测试。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
11_保护在线网站	SME 必须确保以安全的方式配置和维护其在线网站，并确保任何个人数据或财务明细（例如信用卡数据）都得到适当保护。这将需要定期对网站进行安全测试，以发现任何潜在安全漏洞，并定期进行审查以确保网站得到正确维护和更新。	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。

模板

该模板可在以下网址获得 GitHub：ENISA运营最佳实践中小企业网络安全指南。

Esquema Nacional de Seguridad (ENS) Low 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了西班牙国家安全局 (ENS) 低框架控制和托管 Config 规则之间的映射示例。 AWS 每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个 Spain ENS Low 控制相关。一个 Spain ENS 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

此示例合规包模板包含 Spain ENS Low 框架内控制的映射，最新更新时间为 2020/10/23。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数

控制 ID	AWS Config 规则	指南
		据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
Anexo II 4.1.2.a); b); c)	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.b)	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
Anexo II 4.1.2.b)	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
Anexo II 4.1.2.b)	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.1.a)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
Anexo II 4.2.1.a); b)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
Anexo II 4.2.4	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
Anexo II 4.2.5	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.5.BAJO.a)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.5.BAJO.c)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
Anexo II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
Anexo II 4.3.1	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
Anexo II 4.3.1	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.1	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
Anexo II 4.3.1	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
Anexo II 4.3.2.b)	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
Anexo II 4.3.2.b)	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
Anexo II 4.3.2.b)	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
Anexo II 4.3.2.b)	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
Anexo II 4.3.2.b)	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
Anexo II 4.3.2.b)	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Anexo II 4.3.2.b)	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
Anexo II 4.3.4.c)	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
Anexo II 4.3.8.BAJO	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.BAJO	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.BAJO	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
Anexo II 4.3.8.BAJO	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrai l 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	AWS Config 规则	指南
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
Anexo II 5.2.3	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.3.BAJO.a)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	AWS Config 规则	指南
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
Anexo II 5.7.3	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Anexo II 5.7.3	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 5.7.3	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Anexo II 5.7.3	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
Anexo II 5.7.3	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 5.7.3	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
Anexo II 5.7.3	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
Anexo II 5.7.3	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	AWS Config 规则	指南
Anexo II 5.8.2	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
Anexo II 5.8.2	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
Art. 14.4	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
Art. 16	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	AWS Config 规则	指南
Art. 16	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
Art. 16	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	AWS Config 规则	指南
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
Art. 20.2	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
Art. 20.2	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。
Art. 21.1	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Art. 21.1	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
Art. 21.1	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	AWS Config 规则	指南
Art. 21.1	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
Art. 21.1	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Art. 21.1	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Art. 21.1	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
Art. 21.1	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
Art. 21.1	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Art. 21.1	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
Art. 21.1	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Art. 21.1	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
Art. 21.1	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
Art. 21.1	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
Art. 21.1	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
Art. 21.1	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
Art. 21.1	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Art. 21.1	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
Art. 22	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
Art. 22	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	AWS Config 规则	指南
Art. 22	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Art. 22	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
Art. 22	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Art. 22	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
Art. 22	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
Art. 22	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
Art. 22	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
Art. 22	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	AWS Config 规则	指南
Art. 22	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
Art. 22	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Art. 22	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Art. 22	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
Art. 22	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
Art. 22	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Art. 22	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
Art. 22	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Art. 22	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Art. 22	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
Art. 22	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
Art. 22	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
Art. 22	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
Art. 23	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
Art. 23	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
Art. 23	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
Art. 23	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Art. 23	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
Art. 23	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
Art. 23	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
Art. 23	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Art. 23	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Art. 23	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
Art. 23	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Art. 25	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
Art. 25	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Art. 25	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Art. 25	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
Art. 25	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
Art. 25	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
Art. 25	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
Art. 25	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	AWS Config 规则	指南
Art. 25	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
Art. 25	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
Art. 25	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

模板

该模板可在以下网址获得 GitHub：Esquema Nacional de Seguridad (ENS) 运营最佳实践 Low。

Esquema Nacional de Seguridad (ENS) Medium 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了西班牙国家安全局 (ENS) Medium 框架控件和托管 Config 规则之间的映射示例。 AWS 每条 Config 规则都适用于特定 AWS 资源，并与一个或多个西班牙 ENS Medium 控件相关。一个 Spain ENS 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

此示例合规包模板包含 Spain ENS Medium 框架内控制的映射，最新更新时间为 2020/10/23。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数

控制 ID	AWS Config 规则	指南
		据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
Anexo II 4.1.2.a); b); c)	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.b)	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
Anexo II 4.1.2.b)	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
Anexo II 4.1.2.b)	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.1.a)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
Anexo II 4.2.1.a); 4.2.1.b)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
Anexo II 4.2.4	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
Anexo II 4.2.5	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.5.a)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.5.c)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.c)	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
Anexo II 4.2.6.c)	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
Anexo II 4.2.6.c)	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.c)	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
Anexo II 4.2.6.c)	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Anexo II 4.2.6.c)	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
Anexo II 4.2.6.c)	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.c)	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
Anexo II 4.2.6.c)	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Anexo II 4.2.6.c)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.c)	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Anexo II 4.2.7	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
Anexo II 4.2.7	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
Anexo II 4.2.7	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
Anexo II 4.2.7	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
Anexo II 4.3.1	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
Anexo II 4.3.1	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.1	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
Anexo II 4.3.1	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
Anexo II 4.3.1	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
Anexo II 4.3.2.b)	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
Anexo II 4.3.2.b)	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
Anexo II 4.3.2.b)	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
Anexo II 4.3.2.b)	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
Anexo II 4.3.2.b)	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
Anexo II 4.3.2.b)	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
Anexo II 4.3.4.c)	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
Anexo II 4.3.7.a)	response-plan-exists-maintained（流程检查）	确保制定和维护事件响应计划，并将其分发给负责人。更新并正式记录响应计划，有助于确保响应人员了解自己的角色、责任以及在事件发生时应遵循的流程。
Anexo II 4.3.8	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
Anexo II 4.3.8	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
Anexo II 4.3.8	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Anexo II 4.3.8	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
Anexo II 4.3.8	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
Anexo II 4.3.8	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Anexo II 4.3.8	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
Anexo II 4.3.8	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
Anexo II 4.6.2	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector 、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
Anexo II 4.6.2	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
Anexo II 5.2.3	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
Anexo II 5.4.2	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.2	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.2	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.2	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.2	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 5.4.2	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 5.4.2	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.2	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
Anexo II 5.4.3	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.3	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.3	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.3	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.3	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 5.4.3	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 5.4.3	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.3	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.3.a)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	AWS Config 规则	指南
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
Anexo II 5.7.3	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Anexo II 5.7.3	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 5.7.3	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Anexo II 5.7.3	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
Anexo II 5.7.3	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 5.7.3	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
Anexo II 5.7.3	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
Anexo II 5.7.3	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	AWS Config 规则	指南
Anexo II 5.8.2	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
Anexo II 5.8.2	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
Anexo II 5.8.3.b)	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
Anexo II 5.8.3.b)	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
Anexo II 5.8.3.b)	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
Anexo II 5.8.3.b)	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
Anexo II 5.8.3.b)	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	AWS Config 规则	指南
Anexo II 5.8.3.b)	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
Anexo II 5.8.3.b)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
Anexo II 5.8.3.b)	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	AWS Config 规则	指南
Art. 14.4	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
Art. 16	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
Art. 16	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
Art. 16	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
Art. 20.2	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	AWS Config 规则	指南
Art. 20.2	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。
Art. 21.1	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Art. 21.1	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
Art. 21.1	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
Art. 21.1	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
Art. 21.1	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
Art. 21.1	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Art. 21.1	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Art. 21.1	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
Art. 21.1	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
Art. 21.1	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Art. 21.1	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
Art. 21.1	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Art. 21.1	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
Art. 21.1	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
Art. 21.1	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
Art. 21.1	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
Art. 21.1	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
Art. 21.1	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Art. 21.1	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
Art. 22	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
Art. 22	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
Art. 22	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
Art. 22	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
Art. 22	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Art. 22	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
Art. 22	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
Art. 22	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
Art. 22	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	AWS Config 规则	指南
Art. 22	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
Art. 22	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
Art. 22	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
Art. 22	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Art. 22	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Art. 22	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Art. 22	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
Art. 22	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
Art. 22	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
Art. 22	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Art. 22	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
Art. 22	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
Art. 22	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	AWS Config 规则	指南
Art. 22	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
Art. 23	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
Art. 23	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
Art. 23	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
Art. 23	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Art. 23	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	AWS Config 规则	指南
Art. 23	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
Art. 23	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
Art. 23	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Art. 23	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Art. 23	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
Art. 23	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
Art. 24.2	response-plan-exists-maintained（流程检查）	确保制定和维护事件响应计划，并将其分发给负责人。更新并正式记录响应计划，有助于确保响应人员了解自己的角色、责任以及在事件发生时应遵循的流程。

控制 ID	AWS Config 规则	指南
Art. 25	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Art. 25	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Art. 25	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
Art. 25	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Art. 25	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
Art. 25	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
Art. 25	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	AWS Config 规则	指南
Art. 25	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
Art. 25	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
Art. 25	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	AWS Config 规则	指南
Art. 25	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

模板

该模板可在以下网址获得 GitHub：国家安全学院 (ENS) Medium 的运营最佳实践。

Esquema Nacional de Seguridad (ENS) High 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了西班牙国家安全部署 (ENS) 高级框架控制和托管 Config 规则之间的映射示例。 AWS 每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 Spain ENS High 控制相关。一个 Spain ENS 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

此示例合规包模板包含 Spain ENS High 框架内控制的映射，最新更新时间为 2021/07/09。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.1.ALTO	annual-risk-assessment-performed（过程检查）	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。

控制 ID	AWS Config 规则	指南
4.2.1.b)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
4.2.5.ALTO.a)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
Anexo II 4.1.2.a); b); c)	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Anexo II 4.1.2.a); b); c)	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
Anexo II 4.1.2.a); b); c)	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 4.1.2.a); b); c)	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
Anexo II 4.1.2.a); b); c)	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Anexo II 4.1.2.a); b); c)	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
Anexo II 4.1.2.a); b); c)	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Anexo II 4.1.2.a); b); c)	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 4.1.2.a); b); c)	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
Anexo II 4.1.2.a); b); c)	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
Anexo II 4.1.2.a); b); c)	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
Anexo II 4.1.2.a); b); c)	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
Anexo II 4.1.2.a); b); c)	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
Anexo II 4.1.2.a); b); c)	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Anexo II 4.1.2.a); b); c)	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.a); b); c)	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
Anexo II 4.1.2.b)	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
Anexo II 4.1.2.b)	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
Anexo II 4.1.2.b)	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
Anexo II 4.1.2.b)	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
Anexo II 4.1.2.b)	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
Anexo II 4.1.2.b)	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.1.a)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
Anexo II 4.2.4	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
Anexo II 4.2.4	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
Anexo II 4.2.4	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.4	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
Anexo II 4.2.5	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.5.BAJO.a)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.5.BAJO.c)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
Anexo II 4.2.6.ALTO.b)	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.ALTO.b)	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
Anexo II 4.2.6.ALTO.b)	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
Anexo II 4.2.6.ALTO.b)	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
Anexo II 4.2.6.BAJO.c)	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.BAJO.c)	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
Anexo II 4.2.6.BAJO.c)	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
Anexo II 4.2.6.BAJO.c)	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.BAJO.c)	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Anexo II 4.2.6.BAJO.c)	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
Anexo II 4.2.6.BAJO.c)	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
Anexo II 4.2.6.BAJO.c)	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.BAJO.c)	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Anexo II 4.2.6.BAJO.c)	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
Anexo II 4.2.6.BAJO.c)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
Anexo II 4.2.6.BAJO.c)	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Anexo II 4.2.7.BAJO	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
Anexo II 4.2.7.BAJO	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
Anexo II 4.2.7.BAJO	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
Anexo II 4.2.7.BAJO	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
Anexo II 4.3.1	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
Anexo II 4.3.1	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
Anexo II 4.3.1	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.1	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
Anexo II 4.3.1	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
Anexo II 4.3.1	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
Anexo II 4.3.2.b)	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
Anexo II 4.3.2.b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
Anexo II 4.3.2.b)	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
Anexo II 4.3.2.b)	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
Anexo II 4.3.2.b)	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Anexo II 4.3.2.b)	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Anexo II 4.3.2.b)	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
Anexo II 4.3.2.b)	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
Anexo II 4.3.2.b)	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
Anexo II 4.3.2.b)	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
Anexo II 4.3.2.b)	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Anexo II 4.3.2.b)	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Anexo II 4.3.2.b)	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Anexo II 4.3.2.b)	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
Anexo II 4.3.2.b)	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Anexo II 4.3.2.b)	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Anexo II 4.3.2.b)	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.2.b)	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
Anexo II 4.3.2.b)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
Anexo II 4.3.2.b)	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
Anexo II 4.3.4.c)	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.6	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
Anexo II 4.3.7.MEDIA.a)	response-plan-exists-maintained（流程检查）	确保制定和维护事件响应计划，并将其分发给负责人。更新并正式记录响应计划，有助于确保响应人员了解自己的角色、责任以及在事件发生时应遵循的流程。
Anexo II 4.3.8.BAJO	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.BAJO	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
Anexo II 4.3.8.BAJO	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
Anexo II 4.3.8.BAJO	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.BAJO	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Anexo II 4.3.8.BAJO	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
Anexo II 4.3.8.BAJO	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
Anexo II 4.3.8.BAJO	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.BAJO	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Anexo II 4.3.8.BAJO	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
Anexo II 4.3.8.BAJO	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.BAJO	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Anexo II 4.3.8.MEDIO	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
Anexo II 4.3.8.MEDIO	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.MEDIO	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
Anexo II 4.3.8.MEDIO	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
Anexo II 4.3.8.MEDIO	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Anexo II 4.3.8.MEDIO	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.MEDIO	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
Anexo II 4.3.8.MEDIO	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
Anexo II 4.3.8.MEDIO	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Anexo II 4.3.8.MEDIO	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.8.MEDIO	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
Anexo II 4.3.8.MEDIO	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Anexo II 4.3.10.b)	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Anexo II 4.3.10.b)	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
Anexo II 4.3.10.d)	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
Anexo II 4.6.1	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
Anexo II 4.6.2.ALTO	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。
Anexo II 4.6.2.BASICA	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
Anexo II 4.6.2.MEDIA	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
Anexo II 5.2.3	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
Anexo II 5.2.4	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
Anexo II 5.2.5	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
Anexo II 5.4.2.MEDIO	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.2.MEDIO	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.2.MEDIO	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.2.MEDIO	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.2.MEDIO	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 5.4.2.MEDIO	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 5.4.2.MEDIO	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.2.MEDIO	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.2.MEDIO	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.3.BAJO.a)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
Anexo II 5.4.3.MEDIO	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.3.MEDIO	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 5.4.3.MEDIO	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.3.MEDIO	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.3.MEDIO	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 5.4.3.MEDIO	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	AWS Config 规则	指南
Anexo II 5.4.3.MEDIO	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
Anexo II 5.4.3.MEDIO	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.4.3.MEDIO	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.6.1.c)	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	AWS Config 规则	指南
Anexo II 5.6.1.c)	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
Anexo II 5.7.3	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Anexo II 5.7.3	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Anexo II 5.7.3	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Anexo II 5.7.3	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Anexo II 5.7.3	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
Anexo II 5.7.3	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Anexo II 5.7.3	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
Anexo II 5.7.3	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Anexo II 5.7.3	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
Anexo II 5.7.3	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Anexo II 5.7.3	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Anexo II 5.7.3	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Anexo II 5.7.4	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
Anexo II 5.7.4	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	AWS Config 规则	指南
Anexo II 5.8.2	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
Anexo II 5.8.2	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
Anexo II 5.8.3.MEDIO.b)	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
Anexo II 5.8.3.MEDIO.b)	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
Anexo II 5.8.3.MEDIO.b)	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
Anexo II 5.8.3.MEDIO.b)	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
Anexo II 5.8.3.MEDIO.b)	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	AWS Config 规则	指南
Anexo II 5.8.3.MEDIO.b)	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
Anexo II 5.8.3.MEDIO.b)	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
Anexo II 5.8.3.MEDIO.b)	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	AWS Config 规则	指南
Art. 14.4	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
Art. 16	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
Art. 16	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
Art. 16	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
Art. 16	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
Art. 20.2	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
Art. 20.2	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
Art. 20.2	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	AWS Config 规则	指南
Art. 20.2	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。
Art. 21.1	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Art. 21.1	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
Art. 21.1	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
Art. 21.1	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
Art. 21.1	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
Art. 21.1	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Art. 21.1	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
Art. 21.1	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
Art. 21.1	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Art. 21.1	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
Art. 21.1	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Art. 21.1	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
Art. 21.1	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Art. 21.1	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
Art. 21.1	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
Art. 21.1	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
Art. 21.1	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
Art. 21.1	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
Art. 21.1	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Art. 21.1	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Art. 21.1	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Art. 21.1	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Art. 21.1	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
Art. 22	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
Art. 22	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
Art. 22	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
Art. 22	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
Art. 22	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Art. 22	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
Art. 22	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Art. 22	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
Art. 22	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
Art. 22	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
Art. 22	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
Art. 22	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
Art. 22	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
Art. 22	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Art. 22	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Art. 22	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Art. 22	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
Art. 22	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
Art. 22	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Art. 22	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Art. 22	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
Art. 22	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
Art. 22	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
Art. 22	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
Art. 23	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
Art. 23	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
Art. 23	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
Art. 23	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
Art. 23	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Art. 23	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
Art. 23	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
Art. 23	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
Art. 23	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
Art. 23	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Art. 23	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
Art. 23	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Art. 24.2	response-plan-exists-maintained（流程检查）	确保制定和维护事件响应计划，并将其分发给负责人。更新并正式记录响应计划，有助于确保响应人员了解自己的角色、责任以及在事件发生时应遵循的流程。
Art. 24.1	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
Art. 25	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Art. 25	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Art. 25	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
Art. 25	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Art. 25	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
Art. 25	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
Art. 25	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	AWS Config 规则	指南
Art. 25	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
Art. 25	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
Art. 25	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	AWS Config 规则	指南
Art. 25	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

模板

该模板可在以下网址获得 GitHub：Esquema Nacional de Seguridad (ENS) High 运营最佳实践。

FDA 联邦法规第 21 篇第 11 部分操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了《联邦法规法典》(CFR) 第 11 部分第 21 章与 AWS 托管 Config 规则之间的映射示例。每 AWS Config 条规则都适用于特定的 AWS 资源，并与一项或多项FDA CFR第21章第11部分的控制措施有关。一个 FDA 联邦法规第 21 篇第 11 部分控制可以与多个 Config 规则关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例

控制 ID	控制描述	AWS Config 规则	指南
	适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：		的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
11.1	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
11.10(a)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(a) 对系统进行验证，以确保准确性、可靠性、一致的预期性能以及识别无效或被篡改记录的能力。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	ecr-private-lifecycle-policy-configured	Amazon Elastic Container Repository (ECR) 生命周期策略使您能够指定存储库中映像的生命周期管理。这允许自动清理未使用的映像，例如根据存在期限或计数使映像过期。
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
11.10(c)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(c) 保护记录，以便在整个记录保留期内能够准确、随时检索。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
11.10(d)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(d) 仅限获得授权的人员访问系统。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
11.10(e)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(e) 使用计算机生成的、带有时间戳的安全审计跟踪记录，来独立记录操作员输入以及创建、修改或删除电子记录的操作的日期和时间。记录变更不得掩盖先前记录的信息。此类审计跟踪记录文件的保留期限应至少与相关电子记录所需的期限相同，并应可供机构审查和复制。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(g)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(g) 使用权限检查来确保只有获得授权的个人才能使用系统、对记录进行电子签名、访问操作或计算机系统输入或输出设备、更改记录或执行手头的操作。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(h)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制措施应包括以下内容：(h) 使用设备（例如终端）检查来酌情确定数据输入来源或操作指令的有效性。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
11.10(h)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制措施应包括以下内容：(h) 使用设备（例如终端）检查来酌情确定数据输入来源或操作指令的有效性。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
11.10(h)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制措施应包括以下内容：(h) 使用设备（例如终端）检查来酌情确定数据输入来源或操作指令的有效性。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
11.10(i)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(i) 确定开发、维护或使用电子记录/电子签名系统的人员是否受过教育和培训并拥有相关经验，可以完成分配的任务。	security-awareness-program-exists（过程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
11.10(k)	使用封闭系统创建、修改、维护或传输电子记录的人员，应采用旨在确保电子记录真实性、完整性以及适当情况下的机密性的程序和控制措施，并确保签名者不能轻易否认所签名记录的不真实性。此类程序和控制应包括以下内容：(k) 对系统文档使用适当的控制措施，包括：(1) 对系统操作和维护文档的分发、获取和使用进行适当控制。(2) 修订和变更控制程序，以维护审计跟踪记录，按时间顺序记录系统文档的开发和修改。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
11.2	(a) 非基于生物识别技术的电子签名应：(1) 至少使用两个不同的识别组成部分，例如识别码和密码。(i) 当个人在单次、连续的受控系统访问期间执行一系列签名时，第一次签名应使用所有电子签名组成部分；随后的签名应使用至少一个电子签名组成部分，该组成部分只能由个人执行，且设计为仅供个人使用。(ii) 当个人执行一项或多项非在单次连续受控访问系统期间进行的签署时，每次签署均应使用所有电子签名组成部分执行。(2) 仅供其真正所有者使用；(3) 其管理和执行方式可确保当个人电子签名的真正所有者以外的任何人试图使用个人电子签名时，需要两个或两个以上人员的配合。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.2	(a) 非基于生物识别技术的电子签名应：(1) 至少使用两个不同的识别组成部分，例如识别码和密码。(i) 当个人在单次、连续的受控系统访问期间执行一系列签名时，第一次签名应使用所有电子签名组成部分；随后的签名应使用至少一个电子签名组成部分，该组成部分只能由个人执行，且设计为仅供个人使用。(ii) 当个人执行一项或多项非在单次连续受控访问系统期间进行的签署时，每次签署均应使用所有电子签名组成部分执行。(2) 仅供其真正所有者使用；(3) 其管理和执行方式可确保当个人电子签名的真正所有者以外的任何人试图使用个人电子签名时，需要两个或两个以上人员的配合。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.2	(a) 非基于生物识别技术的电子签名应：(1) 至少使用两个不同的识别组成部分，例如识别码和密码。(i) 当个人在单次、连续的受控系统访问期间执行一系列签名时，第一次签名应使用所有电子签名组成部分；随后的签名应使用至少一个电子签名组成部分，该组成部分只能由个人执行，且设计为仅供个人使用。(ii) 当个人执行一项或多项非在单次连续受控访问系统期间进行的签署时，每次签署均应使用所有电子签名组成部分执行。(2) 仅供其真正所有者使用；(3) 其管理和执行方式可确保当个人电子签名的真正所有者以外的任何人试图使用个人电子签名时，需要两个或两个以上人员的配合。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
11.2	(a) 非基于生物识别技术的电子签名应：(1) 至少使用两个不同的识别组成部分，例如识别码和密码。(i) 当个人在单次、连续的受控系统访问期间执行一系列签名时，第一次签名应使用所有电子签名组成部分；随后的签名应使用至少一个电子签名组成部分，该组成部分只能由个人执行，且设计为仅供个人使用。(ii) 当个人执行一项或多项非在单次连续受控访问系统期间进行的签署时，每次签署均应使用所有电子签名组成部分执行。(2) 仅供其真正所有者使用；(3) 其管理和执行方式可确保当个人电子签名的真正所有者以外的任何人试图使用个人电子签名时，需要两个或两个以上人员的配合。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
11.2	(a) 非基于生物识别技术的电子签名应：(1) 至少使用两个不同的识别组成部分，例如识别码和密码。(i) 当个人在单次、连续的受控系统访问期间执行一系列签名时，第一次签名应使用所有电子签名组成部分；随后的签名应使用至少一个电子签名组成部分，该组成部分只能由个人执行，且设计为仅供个人使用。(ii) 当个人执行一项或多项非在单次连续受控访问系统期间进行的签署时，每次签署均应使用所有电子签名组成部分执行。(2) 仅供其真正所有者使用；(3) 其管理和执行方式可确保当个人电子签名的真正所有者以外的任何人试图使用个人电子签名时，需要两个或两个以上人员的配合。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
11.2	(a) 非基于生物识别技术的电子签名应：(1) 至少使用两个不同的识别组成部分，例如识别码和密码。(i) 当个人在单次、连续的受控系统访问期间执行一系列签名时，第一次签名应使用所有电子签名组成部分；随后的签名应使用至少一个电子签名组成部分，该组成部分只能由个人执行，且设计为仅供个人使用。(ii) 当个人执行一项或多项非在单次连续受控访问系统期间进行的签署时，每次签署均应使用所有电子签名组成部分执行。(2) 仅供其真正所有者使用；(3) 其管理和执行方式可确保当个人电子签名的真正所有者以外的任何人试图使用个人电子签名时，需要两个或两个以上人员的配合。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
11.2	(a) 非基于生物识别技术的电子签名应：(1) 至少使用两个不同的识别组成部分，例如识别码和密码。(i) 当个人在单次、连续的受控系统访问期间执行一系列签名时，第一次签名应使用所有电子签名组成部分；随后的签名应使用至少一个电子签名组成部分，该组成部分只能由个人执行，且设计为仅供个人使用。(ii) 当个人执行一项或多项非在单次连续受控访问系统期间进行的签署时，每次签署均应使用所有电子签名组成部分执行。(2) 仅供其真正所有者使用；(3) 其管理和执行方式可确保当个人电子签名的真正所有者以外的任何人试图使用个人电子签名时，需要两个或两个以上人员的配合。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
11.3	使用开放系统创建、修改、维护或传输电子记录的人员应采用旨在确保电子记录从创建到接收的整个过程中的真实性、完整性和适当保密性的程序和控制措施。此类程序和控制措施应酌情包括 11.10 中确定的程序和控制措施，以及其他措施，例如文档加密和使用适当的数字签名标准，以便在必要时确保记录的真实性、完整性和保密性。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.300(b)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(b) 确保定期检查、撤回或修改识别码和密码签发（例如，以涵盖密码老化等事件）。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.300(b)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(b) 确保定期检查、撤回或修改识别码和密码签发（例如，以涵盖密码老化等事件）。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
11.300(b)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(b) 确保定期检查、撤回或修改识别码和密码签发（例如，以涵盖密码老化等事件）。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11.300(b)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(b) 确保定期检查、撤回或修改识别码和密码签发（例如，以涵盖密码老化等事件）。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
11.300(b)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(b) 确保定期检查、撤回或修改识别码和密码签发（例如，以涵盖密码老化等事件）。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
11.300(b)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(b) 确保定期检查、撤回或修改识别码和密码签发（例如，以涵盖密码老化等事件）。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
11.300(d)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(d) 使用交易保障措施，防止未经授权使用密码和/或识别码，发现任何未经授权使用密码和/或识别码的企图，并立即向系统安全部门报告，同时酌情向组织管理层报告。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
11.300(d)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(d) 使用交易保障措施，防止未经授权使用密码和/或识别码，发现任何未经授权使用密码和/或识别码的企图，并立即向系统安全部门报告，同时酌情向组织管理层报告。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
11.300(d)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(d) 使用交易保障措施，防止未经授权使用密码和/或识别码，发现任何未经授权使用密码和/或识别码的企图，并立即向系统安全部门报告，同时酌情向组织管理层报告。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
11.300(d)	使用基于识别码和密码的电子签名的人应采用控制措施来确保这些信息的安全性和完整性。此类控制措施应包括：(d) 使用交易保障措施，防止未经授权使用密码和/或识别码，发现任何未经授权使用密码和/或识别码的企图，并立即向系统安全部门报告，同时酌情向组织管理层报告。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

模板

该模板可在以下网址获得 GitHub：FDA CFR 第 21 章第 11 部分的操作最佳实践。

FedRAMP(Low) 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了联邦风险和授权管理计划 (FedRAMP) 低基准控制与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个 FedRAMP 控件相关。一个 FedRAMP 控制可以与多个配置规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
AC-2	账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatt erns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC-2	账户管理	iam-group-has-users-check	AWS Identity and Access Managemen

控制 ID	控制描述	AWS Config 规则	指南
			t (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
AC-2	账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC-2	账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC-2	账户管理	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-2	账户管理	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AC-2	账户管理	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC-2	账户管理	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AC-2	账户管理	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2	账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2	账户管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC-2	账户管理	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-2	账户管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
AC-2	账户管理	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC-2	账户管理	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC-3	强制访问权限	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC-3	强制访问权限	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
AC-3	强制访问权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC-3	强制访问权限	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC-3	强制访问权限	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-3	强制访问权限	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-3	强制访问权限	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-3	强制访问权限	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
AC-3	强制访问权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-3	强制访问权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-3	强制访问权限	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-3	强制访问权限	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-3	强制访问权限	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-3	强制访问权限	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-3	强制访问权限	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-3	强制访问权限	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-3	强制访问权限	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-17	远程访问	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17	远程访问	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-17	远程访问	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17	远程访问	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-17	远程访问	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-17	远程访问	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-17	远程访问	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-17	远程访问	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC-17	远程访问	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-17	远程访问	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-17	远程访问	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-17	远程访问	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-17	远程访问	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-17	远程访问	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-17	远程访问	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC-17	远程访问	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-17	远程访问	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-17	远程访问	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AU-2	审计事件	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	审计事件	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU-2	审计事件	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	审计事件	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-2	审计事件	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU-2	审计事件	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	审计事件	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-2	审计事件	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU-2	审计事件	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	审计事件	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	审计事件	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-2	审计事件	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
AU-3	审计记录的内容	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU-3	审计记录的内容	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-3	审计记录的内容	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-3	审计记录的内容	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-3	审计记录的内容	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU-3	审计记录的内容	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-3	审计记录的内容	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-6	审计审查、分析和报告	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
AU-6	审计审查、分析和报告	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
AU-6	审计审查、分析和报告	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-6	审计审查、分析和报告	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AU-6	审计审查、分析和报告	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU-6	审计审查、分析和报告	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU-6	审计审查、分析和报告	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-6	审计审查、分析和报告	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
AU-6	审计审查、分析和报告	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU-6	审计审查、分析和报告	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
AU-6	审计审查、分析和报告	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU-6	审计审查、分析和报告	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU-6	审计审查、分析和报告	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU-6	审计审查、分析和报告	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-6	审计审查、分析和报告	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-6	审计审查、分析和报告	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-9	保护审计信息	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
AU-9	保护审计信息	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
AU-9	保护审计信息	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
AU-9	保护审计信息	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
AU-9	保护审计信息	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
AU-11	审计记录保留	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计生成	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
AU-12	审计生成	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计生成	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU-12	审计生成	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-12	审计生成	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计生成	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-12	审计生成	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-12	审计生成	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计生成	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU-12	审计生成	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计生成	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-12	审计生成	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
CA-7	持续监控	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
CA-7	持续监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CA-7	持续监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CA-7	持续监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CA-7	持续监控	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
CA-7	持续监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CA-7	持续监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
CM-2	基线配置	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
CM-2	基线配置	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM-2	基线配置	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CM-2	基线配置	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CM-2	基线配置	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM-2	基线配置	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CM-2	基线配置	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM-2	基线配置	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM-2	基线配置	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM-2	基线配置	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM-2	基线配置	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM-2	基线配置	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CM-2	基线配置	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-2	基线配置	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
CM-2	基线配置	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CM-2	基线配置	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CM-2	基线配置	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
CM-2	基线配置	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM-7	最少功能	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
CM-7	最少功能	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-7	最少功能	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM-8	信息系统组件清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-8	信息系统组件清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM-8	信息系统组件清单	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM-8	信息系统组件清单	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CP-9	信息系统备份	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	信息系统备份	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	信息系统备份	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9	信息系统备份	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	信息系统备份	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9	信息系统备份	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	信息系统备份	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9	信息系统备份	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	信息系统备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CP-9	信息系统备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-9	信息系统备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	信息系统备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CP-9	信息系统备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	信息系统备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CP-10	信息系统恢复和重组	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	信息系统恢复和重组	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	信息系统恢复和重组	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-10	信息系统恢复和重组	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	信息系统恢复和重组	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-10	信息系统恢复和重组	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	信息系统恢复和重组	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CP-10	信息系统恢复和重组	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	信息系统恢复和重组	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-10	信息系统恢复和重组	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	信息系统恢复和重组	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-10	信息系统恢复和重组	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
CP-10	信息系统恢复和重组	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	信息系统恢复和重组	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CP-10	信息系统恢复和重组	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CP-10	信息系统恢复和重组	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	信息系统恢复和重组	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CP-10	信息系统恢复和重组	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	信息系统恢复和重组	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CP-10	信息系统恢复和重组	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
IA-2	识别和身份验证（组织用户）	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA-2	识别和身份验证（组织用户）	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
IA-2	识别和身份验证（组织用户）	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
IA-2	识别和身份验证（组织用户）	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA-2	识别和身份验证（组织用户）	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2	识别和身份验证（组织用户）	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA-5	身份验证器管理	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
IA-5	身份验证器管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IR-4	事件处理	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
IR-4	事件处理	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR-4	事件处理	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
IR-4	事件处理	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
IR-4	事件处理	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
IR-6	事件报告	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR-6	事件报告	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
IR-6	事件报告	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
IR-7	事件响应	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
IR-7	事件响应	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
IR-7	事件响应	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
RA-5	漏洞扫描	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
RA-5	漏洞扫描	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
RA-5	漏洞扫描	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SA-3	系统开发生命周期	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
SA-3	系统开发生命周期	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	控制描述	AWS Config 规则	指南
SA-3	系统开发生命周期	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SC-5	拒绝服务保护	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	拒绝服务保护	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
SC-5	拒绝服务保护	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	拒绝服务保护	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
SC-5	拒绝服务保护	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
SC-5	拒绝服务保护	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	拒绝服务保护	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SC-5	拒绝服务保护	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
SC-5	拒绝服务保护	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	拒绝服务保护	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
SC-5	拒绝服务保护	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	拒绝服务保护	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
SC-5	拒绝服务保护	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC-7	边界保护	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
SC-7	边界保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
SC-7	边界保护	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
SC-7	边界保护	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
SC-7	边界保护	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC-7	边界保护	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7	边界保护	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7	边界保护	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-7	边界保护	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
SC-7	边界保护	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7	边界保护	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-7	边界保护	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SC-7	边界保护	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-7	边界保护	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
SC-12	加密密钥的建立和管理	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
SC-12	加密密钥的建立和管理	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
SC-12	加密密钥的建立和管理	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC-13	加密保护	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13	加密保护	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
SC-13	加密保护	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13	加密保护	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI-2	缺陷修复	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SI-2	缺陷修复	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI-2	缺陷修复	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
SI-2	缺陷修复	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
SI-3	缺陷修复	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
SI-3	缺陷修复	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
SI-3	缺陷修复	ecs-task-definition-memory-hard-limit	限制 Amazon Elastic Container Service (ECS) 容器可用的最大内存可确保您的资源使用量不会在容器遭到恶意访问时被滥用。
SI-4	信息系统监控	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SI-4	信息系统监控	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SI-4	信息系统监控	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
SI-4	信息系统监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI-4	信息系统监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI-4	信息系统监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-4	信息系统监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
SI-4	信息系统监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI-4	信息系统监控	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
SI-4	信息系统监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI-4	信息系统监控	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
SI-4	信息系统监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-4	信息系统监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-5	安全警报、公告和指令	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI-5	安全警报、公告和指令	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-5	安全警报、公告和指令	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
SI-5	安全警报、公告和指令	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息处理和保留	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息处理和保留	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
SI-12	信息处理和保留	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息处理和保留	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	信息处理和保留	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息处理和保留	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	信息处理和保留	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息处理和保留	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	信息处理和保留	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息处理和保留	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
SI-12	信息处理和保留	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
SI-12	信息处理和保留	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息处理和保留	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SI-12	信息处理和保留	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
SI-16	内存保护	ecs-task-definition-memory-hard-limit	限制 Amazon Elastic Container Service (ECS) 容器可用的最大内存可确保您的资源使用量不会在容器遭到恶意访问时被滥用。

模板

该模板可在以下网址获得 GitHub：FedRAMP 操作最佳实践（低）。

FedRAMP(Moderate) 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了联邦风险和授权管理计划 (FedRAMP) 与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个 FedRAMP 控件相关。一个 FedRAMP 控制可以与多个配置规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

该合规包已通过 AWS 安全保障服务有限责任公司（AWS SAS）的验证，该公司由支付卡行业合格安全评估员（QSA）、HITRUST认证的通用安全框架从业人员（CCSFP）和经过认证的合规专业人员组成，可以为各种行业框架提供指导和评估。 AWS SAS 专业人员设计此一致性包是为了让客户能够与 FedRAMP 控制的子集保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和

控制 ID	控制描述	AWS Config 规则	指南
			软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC-2(3)	信息系统会在 90 天后自动禁用用户处于非活动状态的账户。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(3)	信息系统会在 90 天后自动禁用用户处于非活动状态的账户。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(7)	组织：(a) 根据基于角色的访问方案建立和管理特权用户，该方案将允许的信息系统访问权限和特权组织到角色中；(b) 监控特权角色分配；(c) 在特权角色分配不再合适时采取 [分配：组织定义的操作]。补充指南：特权角色是指分配给个人的组织定义角色，以允许这些个人执行普通用户无权执行的与安全相关的某些职能。例如，这些特权角色包括密钥管理、账户管理、网络和系统管理、数据库管理以及 Web 管理。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-2(7)	组织：(a) 根据基于角色的访问方案建立和管理特权用户，该方案将允许的信息系统访问权限和特权组织到角色中；(b) 监控特权角色分配；(c) 在特权角色分配不再合适时采取 [分配：组织定义的操作]。补充指南：特权角色是指分配给个人的组织定义角色，以允许这些个人执行普通用户无权执行的与安全相关的某些职能。例如，这些特权角色包括密钥管理、账户管理、网络和系统管理、数据库管理以及 Web 管理。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(7)	组织：(a) 根据基于角色的访问方案建立和管理特权用户，该方案将允许的信息系统访问权限和特权组织到角色中；(b) 监控特权角色分配；(c) 在特权角色分配不再合适时采取 [分配：组织定义的操作]。补充指南：特权角色是指分配给个人的组织定义角色，以允许这些个人执行普通用户无权执行的与安全相关的某些职能。例如，这些特权角色包括密钥管理、账户管理、网络和系统管理、数据库管理以及 Web 管理。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(7)	组织：(a) 根据基于角色的访问方案建立和管理特权用户，该方案将允许的信息系统访问权限和特权组织到角色中；(b) 监控特权角色分配；(c) 在特权角色分配不再合适时采取 [分配：组织定义的操作]。补充指南：特权角色是指分配给个人的组织定义角色，以允许这些个人执行普通用户无权执行的与安全相关的某些职能。例如，这些特权角色包括密钥管理、账户管理、网络和系统管理、数据库管理以及 Web 管理。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(7)	组织：(a) 根据基于角色的访问方案建立和管理特权用户，该方案将允许的信息系统访问权限和特权组织到角色中；(b) 监控特权角色分配；(c) 在特权角色分配不再合适时采取 [分配：组织定义的操作]。补充指南：特权角色是指分配给个人的组织定义角色，以允许这些个人执行普通用户无权执行的与安全相关的某些职能。例如，这些特权角色包括密钥管理、账户管理、网络和系统管理、数据库管理以及 Web 管理。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(7)	组织：(a) 根据基于角色的访问方案建立和管理特权用户，该方案将允许的信息系统访问权限和特权组织到角色中；(b) 监控特权角色分配；(c) 在特权角色分配不再合适时采取 [分配：组织定义的操作]。补充指南：特权角色是指分配给个人的组织定义角色，以允许这些个人执行普通用户无权执行的与安全相关的某些职能。例如，这些特权角色包括密钥管理、账户管理、网络和系统管理、数据库管理以及 Web 管理。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(12)(a)	组织：a. 监控 [分配：组织定义的非典型用途] 的信息系统账户。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-2(12)(a)	组织：a. 监控 [分配：组织定义的非典型用途] 的信息系统账户。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC-6(10)	信息系统可防止非特权用户执行特权功能，包括禁用、规避或更改已实施的安全保障措施/对策。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(10)	信息系统可防止非特权用户执行特权功能，包括禁用、规避或更改已实施的安全保障措施/对策。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6(10)	信息系统可防止非特权用户执行特权功能，包括禁用、规避或更改已实施的安全保障措施/对策。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-17(1)	信息系统监视和控制远程访问方法。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-17(1)	信息系统监视和控制远程访问方法。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-17(1)	信息系统监视和控制远程访问方法。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-17(1)	信息系统监视和控制远程访问方法。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-17(1)	信息系统监视和控制远程访问方法。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AC-17(1)	信息系统监视和控制远程访问方法。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
AC-17(1)	信息系统监视和控制远程访问方法。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-17(1)	信息系统监视和控制远程访问方法。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-17(1)	信息系统监视和控制远程访问方法。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-17(1)	信息系统监视和控制远程访问方法。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-17(1)	信息系统监视和控制远程访问方法。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-17(1)	信息系统监视和控制远程访问方法。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：成功和失败的账户登录事件、账户管理事件、对象访问、策略更改、特权功能、进程跟踪和系统事件。对于 Web 应用程序，则包括：所有管理员活动、身份验证检查、授权检查、数据删除、数据访问、数据更改和权限更改。d. 确定要在信息系统中审计以下事件：[AU-2 a 中定义的可审计事件的组织定义子集，以便对每个确定的事件进行持续审计]。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-7(1)	信息系统提供了根据 [分配：审计记录中组织定义的审计字段] 处理相关事件的审计记录的功能。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-7(1)	信息系统提供了根据 [分配：审计记录中组织定义的审计字段] 处理相关事件的审计记录的功能。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
AU-9(2)	信息系统至少每周将审计记录备份到与被审计的系统或组件实际不同的系统或系统组件上。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
AU-9(2)	信息系统至少每周将审计记录备份到与被审计的系统或组件实际不同的系统或系统组件上。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
AU-9	信息系统保护审计信息和审计工具免遭未经授权的访问、修改和删除。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
AU-9	信息系统保护审计信息和审计工具免遭未经授权的访问、修改和删除。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
AU-9	信息系统保护审计信息和审计工具免遭未经授权的访问、修改和删除。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
AU-11	该组织将审计记录保留至少 90 天，以便为安全事件的 after-the-fact 调查提供支持，并满足监管和组织信息保留要求。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-12(a)(c)	信息系统：a. 在部署/提供审计功能的所有信息系统和网络组件中，为 AU-2 a. 中定义的可审计事件提供审计记录生成功能。c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
CM-7(a)	组织：a. 将信息系统配置为仅提供基本功能。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
CM-7(a)	组织：a. 将信息系统配置为仅提供基本功能。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM-7(a)	组织：a. 将信息系统配置为仅提供基本功能。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM-8(1)	组织更新信息系统组件清单，作为组件安装、拆除和信息系统更新的组成部分。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM-8(1)	组织更新信息系统组件清单，作为组件安装、拆除和信息系统更新的组成部分。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM-8(3)(a)	组织：a. 持续采用自动化机制，使用最长延迟五分钟检测的自动化机制，检测信息系统内是否存在未经授权的硬件、软件和固件组件	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM-8(3)(a)	组织：a. 持续采用自动化机制，使用最长延迟五分钟检测的自动化机制，检测信息系统内是否存在未经授权的硬件、软件和固件组件	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM-8(3)(a)	组织：a. 持续采用自动化机制，使用最长延迟五分钟检测的自动化机制，检测信息系统内是否存在未经授权的硬件、软件和固件组件	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM-8(3)(a)	组织：a. 持续采用自动化机制，使用最长延迟五分钟检测的自动化机制，检测信息系统内是否存在未经授权的硬件、软件和固件组件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份（每日增量备份；每周完整备份）。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
IA-2(1)(2)	(1) 信息系统对特权账户的网络访问实施多重身份验证。(2) 信息系统对非特权账户的网络访问实施多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2(1)(2)	(1) 信息系统对特权账户的网络访问实施多重身份验证。(2) 信息系统对非特权账户的网络访问实施多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA-2(1)(2)	(1) 信息系统对特权账户的网络访问实施多重身份验证。(2) 信息系统对非特权账户的网络访问实施多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
IA-2(1)(2)	(1) 信息系统对特权账户的网络访问实施多重身份验证。(2) 信息系统对非特权账户的网络访问实施多重身份验证。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2(1)	(1) 信息系统对特权账户的网络访问实施多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA-2(1)	(1) 信息系统对特权账户的网络访问实施多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
IA-2(1)	(1) 信息系统对特权账户的网络访问实施多重身份验证。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2(1)	(1) 信息系统对特权账户的网络访问实施多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA-2	信息系统对组织用户（或代表组织用户行事的进程）进行唯一标识和身份验证。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA-2	信息系统对组织用户（或代表组织用户行事的进程）进行唯一标识和身份验证。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
IA-5(1)(a)(d)(e)	对于基于密码的身份验证，信息系统：a. 强制执行最低密码复杂度 [分配：组织定义的区分大小写、字符数、混合使用大写字母、小写字母、数字和特殊字符的要求，包括每种类型字符的最低数量要求]；d. 强制执行 [分配：组织定义的最短和最长使用期限] 的密码最短和最长使用期限限制；e. 禁止重复使用 24 代以内的密码	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA-5(4)	组织使用自动化工具来确定密码身份验证器是否足够强大，可以满足 [分配：组织定义的要求]。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA-5(7)	组织确保未加密的静态身份验证器不会嵌入应用程序或访问脚本中，也不会存储在功能密钥上。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
IR-4(1)	组织采用自动化机制来支持事件处理流程。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
IR-4(1)	组织采用自动化机制来支持事件处理流程。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
IR-4(1)	组织采用自动化机制来支持事件处理流程。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
IR-4(1)	组织采用自动化机制来支持事件处理流程。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
IR-4(1)	组织采用自动化机制来支持事件处理流程。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
IR-6(1)	组织采用自动化机制来协助报告安全事件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
IR-6(1)	组织采用自动化机制来协助报告安全事件。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
IR-6(1)	组织采用自动化机制来协助报告安全事件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
IR-7(1)	组织采用自动化机制来提高与事件响应相关的信息和支持的可用性。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
IR-7(1)	组织采用自动化机制来提高与事件响应相关的信息和支持的可用性。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
IR-7(1)	组织采用自动化机制来提高与事件响应相关的信息和支持的可用性。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
RA-5(1)	组织使用漏洞扫描工具，其中包括随时更新要扫描的信息系统漏洞的功能。补充指南：随着新漏洞的发现、公布和扫描方法的完善，需要随时更新要扫描的漏洞。这一更新过程有助于确保尽快发现和解决信息系统中的潜在漏洞。相关控制：SI-3、SI-7。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
RA-5(1)	组织使用漏洞扫描工具，其中包括随时更新要扫描的信息系统漏洞的功能。补充指南：随着新漏洞的发现、公布和扫描方法的完善，需要随时更新要扫描的漏洞。这一更新过程有助于确保尽快发现和解决信息系统中的潜在漏洞。相关控制：SI-3、SI-7。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
RA-5(1)	组织使用漏洞扫描工具，其中包括随时更新要扫描的信息系统漏洞的功能。补充指南：随着新漏洞的发现、公布和扫描方法的完善，需要随时更新要扫描的漏洞。这一更新过程有助于确保尽快发现和解决信息系统中的潜在漏洞。相关控制：SI-3、SI-7。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
RA-5	组织：a. 每月扫描一次信息系统和托管应用程序中的漏洞 [操作系统/基础设施；每月扫描一次 Web 应用程序和数据库]，并在发现和报告可能影响系统/应用程序的新漏洞时进行扫描；b. 采用漏洞扫描工具和技术，通过使用以下标准来促进工具之间的互操作性，并实现漏洞管理过程的自动化：1. 枚举平台、软件缺陷和不当配置；2. 设置清单和测试程序格式；以及 3. 衡量漏洞的影响；c. 分析漏洞扫描报告和安全控制评估结果；d. 修复合法漏洞：根据组织的风险评估，自发现之日起三十 (30) 天内缓解高风险漏洞；自发现之日起九十 (90) 天内缓解中等风险漏洞；自发现之日起一百八十 (180) 天内缓解低风险漏洞；e. 与 [分配：组织定义的人员或角色] 共享从漏洞扫描过程和安全控制评估中获得的信	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
	息，以帮助消除其他信息系统中的类似漏洞（即系统薄弱环节或缺陷）。		

控制 ID	控制描述	AWS Config 规则	指南
RA-5	组织：a. 扫描信息系统和托管应用程序中的漏洞 [分配：组织定义的频率和/或根据组织定义的流程随机进行]，以及在发现和报告可能影响系统/应用程序的新漏洞时进行扫描；b. 采用漏洞扫描工具和技术，通过使用以下标准来促进工具之间的互操作性，并实现漏洞管理过程的自动化：1. 枚举平台、软件缺陷和不当配置；2. 设置清单和测试程序格式；以及 3. 衡量漏洞的影响；c. 分析漏洞扫描报告和安全控制评估结果；d. 根据组织的风险评估，修复合法漏洞 [分配：组织定义的响应时间]；以及 e. 与 [分配：组织定义的人员或角色] 共享从漏洞扫描过程和安全控制评估中获得的信息，以帮助消除其他信息系统中的类似漏洞（即系统薄弱环节或缺陷）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SA-3(a)	组织：a. 使用包含信息安全注意事项的 [分配：组织定义的系统开发生命周期] 管理信息系统。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
SA-3(a)	组织：a. 使用包含信息安全注意事项的 [分配：组织定义的系统开发生命周期] 管理信息系统。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	控制描述	AWS Config 规则	指南
SA-3(a)	组织：a. 使用包含信息安全注意事项的 [分配：组织定义的系统开发生命周期] 管理信息系统。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
SA-10	组织要求信息系统、系统组件或信息系统服务的开发人员：a. 在系统、组件或服务开发、实施和运行期间执行配置管理；b. 记录、管理和控制[分配：组织定义的接受配置管理的配置项]的更改的完整性；c. 仅对系统、组件或服务实施组织批准的更改；d. 记录经批准的系统、组件或服务变更，以及此类变更的潜在安全影响；以及 e. 跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给[分配：组织定义的人员]。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
SA-10	组织要求信息系统、系统组件或信息系统服务的开发人员：a. 在系统、组件或服务开发、实施和运行期间执行配置管理；b. 记录、管理和控制[分配：组织定义的接受配置管理的配置项]的更改的完整性；c. 仅对系统、组件或服务实施组织批准的更改；d. 记录经批准的系统、组件或服务变更，以及此类变更的潜在安全影响；以及 e. 跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给[分配：组织定义的人员]。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SA-10	组织要求信息系统、系统组件或信息系统服务的开发人员：a. 在系统、组件或服务开发、实施和运行期间执行配置管理；b. 记录、管理和控制[分配：组织定义的接受配置管理的配置项]的更改的完整性；c. 仅对系统、组件或服务实施组织批准的更改；d. 记录经批准的系统、组件或服务变更，以及此类变更的潜在安全影响；以及 e. 跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给[分配：组织定义的人员]。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
SA-10	组织要求信息系统、系统组件或信息系统服务的开发人员：a. 在系统、组件或服务开发、实施和运行期间执行配置管理；b. 记录、管理和控制[分配：组织定义的接受配置管理的配置项]的更改的完整性；c. 仅对系统、组件或服务实施组织批准的更改；d. 记录经批准的系统、组件或服务变更，以及此类变更的潜在安全影响；以及 e. 跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给[分配：组织定义的人员]。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC-2	信息系统将用户功能（包括用户界面服务）与信息系统管理功能分开。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
SC-2	信息系统将用户功能（包括用户界面服务）与信息系统管理功能分开。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
SC-2	信息系统将用户功能（包括用户界面服务）与信息系统管理功能分开。	iam-user-no-policies-check	该规则可确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
SC-2	信息系统将用户功能（包括用户界面服务）与信息系统管理功能分开。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
SC-2	信息系统将用户功能（包括用户界面服务）与信息系统管理功能分开。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-7(4)	组织：(a) 为每项外部电信服务实施托管接口；(b) 为每个托管接口制定流量策略；(c) 保护通过每个接口传输的信息的机密性和完整性；(d) 记录流量政策的每个例外情况，并附上支持性任务/业务需求和需求持续时间；(e) 审查流量策略的例外情况 [分配：组织定义的频率] 并删除不再有明确任务/业务需求支持的例外情况。补充指南：相关控制：SC-8。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	组织：(a) 为每项外部电信服务实施托管接口；(b) 为每个托管接口制定流量策略；(c) 保护通过每个接口传输的信息的机密性和完整性；(d) 记录流量政策的每个例外情况，并附上支持性任务/业务需求和需求持续时间；(e) 审查流量策略的例外情况 [分配：组织定义的频率] 并删除不再有明确任务/业务需求支持的例外情况。补充指南：相关控制：SC-8。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	组织：(a) 为每项外部电信服务实施托管接口；(b) 为每个托管接口制定流量策略；(c) 保护通过每个接口传输的信息的机密性和完整性；(d) 记录流量政策的每个例外情况，并附上支持性任务/业务需求和需求持续时间；(e) 审查流量策略的例外情况 [分配：组织定义的频率] 并删除不再有明确任务/业务需求支持的例外情况。补充指南：相关控制：SC-8。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	组织：(a) 为每项外部电信服务实施托管接口；(b) 为每个托管接口制定流量策略；(c) 保护通过每个接口传输的信息的机密性和完整性；(d) 记录流量政策的每个例外情况，并附上支持性任务/业务需求和需求持续时间；(e) 审查流量策略的例外情况 [分配：组织定义的频率] 并删除不再有明确任务/业务需求支持的例外情况。补充指南：相关控制：SC-8。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	组织：(a) 为每项外部电信服务实施托管接口；(b) 为每个托管接口制定流量策略；(c) 保护通过每个接口传输的信息的机密性和完整性；(d) 记录流量政策的每个例外情况，并附上支持性任务/业务需求和需求持续时间；(e) 审查流量策略的例外情况 [分配：组织定义的频率] 并删除不再有明确任务/业务需求支持的例外情况。补充指南：相关控制：SC-8。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	组织：(a) 为每项外部电信服务实施托管接口；(b) 为每个托管接口制定流量策略；(c) 保护通过每个接口传输的信息的机密性和完整性；(d) 记录流量政策的每个例外情况，并附上支持性任务/业务需求和需求持续时间；(e) 审查流量策略的例外情况 [分配：组织定义的频率] 并删除不再有明确任务/业务需求支持的例外情况。补充指南：相关控制：SC-8。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-7(5)	默认情况下，托管接口上的信息系统拒绝网络通信流量，并在例外情况下允许网络通信流量（即全部拒绝，按例外情况允许）。补充指南：此控制增强适用于入站和出站网络通信流量。“全部拒绝” 的 permit-by-exception 网络通信流量策略可确保仅允许那些必不可少且经过批准的连接。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	信息系统保护所传输信息的机密性和完整性。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	信息系统保护所传输信息的机密性和完整性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC-8	信息系统保护所传输信息的机密性和完整性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	信息系统保护所传输信息的机密性和完整性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	信息系统保护所传输信息的机密性和完整性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC-8	信息系统保护所传输信息的机密性和完整性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8	信息系统保护所传输信息的机密性和完整性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-12	组织根据 [分配：组织定义的密钥生成、分发、存储、访问和销毁要求]，为信息系统中使用的所需加密技术建立和管理加密密钥。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
SC-12	组织根据 [分配：组织定义的密钥生成、分发、存储、访问和销毁要求]，为信息系统中使用的所需加密技术建立和管理加密密钥。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-12	组织根据 [分配：组织定义的密钥生成、分发、存储、访问和销毁要求]，为信息系统中使用的所需加密技术建立和管理加密密钥。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准，实施经过 FIPS 验证或国家安全局批准的加密技术。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准，实施经过 FIPS 验证或国家安全局批准的加密技术。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准，实施经过 FIPS 验证或国家安全局批准的加密技术。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准，实施经过 FIPS 验证或国家安全局批准的加密技术。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准，实施经过 FIPS 验证或国家安全局批准的加密技术。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准，实施经过 FIPS 验证或国家安全局批准的加密技术。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-23	信息系统保护通信会话的真实性。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23	信息系统保护通信会话的真实性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23	信息系统保护通信会话的真实性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-23	信息系统保护通信会话的真实性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC-23	信息系统保护通信会话的真实性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23	信息系统保护通信会话的真实性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的机密性和完整性。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI-2(2)	组织至少每月使用一次自动化机制来确定信息系统组件在缺陷修复方面的状态。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SI-2(2)	组织至少每月使用一次自动化机制来确定信息系统组件在缺陷修复方面的状态。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI-2(2)	组织至少每月使用一次自动化机制来确定信息系统组件在缺陷修复方面的状态。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
SI-2(2)	组织至少每月使用一次自动化机制来确定信息系统组件在缺陷修复方面的状态。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
SI-3	组织：a. 在信息系统入口和出口处使用恶意代码保护机制来检测和消除恶意代码；b. 根据组织的配置管理策略和程序，每当有新版本可用时，就会更新恶意代码保护机制；c. 将恶意代码保护机制配置为：1. 在根据组织的安全策略，定期扫描信息系统 [分配：组织定义的频率]，并在 [选择（一项或多项）；端点；网络入口/出口点] 下载、打开或执行来自外部来源的文件时实时扫描文件；以及 2. [选择（一项或多项）：阻止恶意代码；隔离恶意代码；向管理员发送警报；[分配：组织定义的操作]] 以响应检测到的恶意代码；以及 d. 解决恶意代码检测和清除过程中的误报问题，以及由此对信息系统可用性造成的潜在影响。补充指南：信息系统的入口和出口点包括防火墙、电子邮件服务器、Web	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
	服务器、代理服务器、远程访问服务器、工作站、笔记本电脑和移动设备。例如，恶意代码包括病毒、蠕虫、特洛伊木马和间谍软件。恶意代码也可以以各种格式（例如 UUENCODE、Unicode）编码，包含在压缩或隐藏文件中，或者使用隐写术隐藏在文件中。恶意代码可以通过不同的方式传输，例如，网络访问、电子邮件、电子邮件附件和便携式存储设备。恶意代码插入是通过利用信息系统漏洞进行的。例如，恶意代码保护机制包括防病毒签名定义和基于信誉的技术。有多种技术和方法可以限制或消除恶意代码的影响。无处不在的配置管理和全面的软件完整性控制可以有效防止未经授权的代码的执行。除商业 off-the-shelf 软件外，定制软件中也可能存在恶意代码。例如，这可能包括逻辑炸弹、后		

控制 ID	控制描述	AWS Config 规则	指南
	门以及其他可能影响组织任务/业务职能的网络攻击。传统的恶意代码保护机制无法始终检测到此类代码。在这些情况下，组织转而依赖其他保护措施，包括安全编码实践、配置管理和控制、可信采购流程和监控实践，以帮助确保软件不会执行预期功能以外的功能。组织可能会决定，为了应对检测到的恶意代码，可能需要采取不同的行动。例如，组织可以定义针对定期扫描期间检测到的恶意代码的操作、针对检测到恶意下载的操作，和/或针对在尝试打开或执行文件时检测到的恶意行为的操作。相关控制：CM-3、MP-2、SA-4、SA-8、SA-12、SA-13、SC-7、SC-26、SC-44、SI-2、SI-4、SI-7。参考文献：NIST 专题出版物 800-83。		

控制 ID	控制描述	AWS Config 规则	指南
SI-3	组织：a. 在信息系统入口和出口处使用恶意代码保护机制来检测和消除恶意代码；b. 根据组织的配置管理策略和程序，每当有新版本可用时，就会更新恶意代码保护机制；c. 将恶意代码保护机制配置为：1. 在根据组织的安全策略，定期扫描信息系统 [分配：组织定义的频率]，并在 [选择（一项或多项）；端点；网络入口/出口点] 下载、打开或执行来自外部来源的文件时实时扫描文件；以及 2. [选择（一项或多项）：阻止恶意代码；隔离恶意代码；向管理员发送警报；[分配：组织定义的操作]] 以响应检测到的恶意代码；以及 d. 解决恶意代码检测和清除过程中的误报问题，以及由此对信息系统可用性造成的潜在影响。补充指南：信息系统的入口和出口点包括防火墙、电子邮件服务器、Web	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	控制描述	AWS Config 规则	指南
	服务器、代理服务器、远程访问服务器、工作站、笔记本电脑和移动设备。例如，恶意代码包括病毒、蠕虫、特洛伊木马和间谍软件。恶意代码也可以以各种格式（例如 UUENCODE、Unicode）编码，包含在压缩或隐藏文件中，或者使用隐写术隐藏在文件中。恶意代码可以通过不同的方式传输，例如，网络访问、电子邮件、电子邮件附件和便携式存储设备。恶意代码插入是通过利用信息系统漏洞进行的。例如，恶意代码保护机制包括防病毒签名定义和基于信誉的技术。有多种技术和方法可以限制或消除恶意代码的影响。无处不在的配置管理和全面的软件完整性控制可以有效防止未经授权的代码的执行。除商业 off-the-shelf 软件外，定制软件中也可能存在恶意代码。例如，这可能包括逻辑炸弹、后		

控制 ID	控制描述	AWS Config 规则	指南
	门以及其他可能影响组织任务/业务职能的网络攻击。传统的恶意代码保护机制无法始终检测到此类代码。在这些情况下，组织转而依赖其他保护措施，包括安全编码实践、配置管理和控制、可信采购流程和监控实践，以帮助确保软件不会执行预期功能以外的功能。组织可能会决定，为了应对检测到的恶意代码，可能需要采取不同的行动。例如，组织可以定义针对定期扫描期间检测到的恶意代码的操作、针对检测到恶意下载的操作，和/或针对在尝试打开或执行文件时检测到的恶意行为的操作。相关控制：CM-3、MP-2、SA-4、SA-8、SA-12、SA-13、SC-7、SC-26、SC-44、SI-2、SI-4、SI-7。参考文献：NIST 专题出版物 800-83。		

控制 ID	控制描述	AWS Config 规则	指南
SI-3	组织：a. 在信息系统入口和出口处使用恶意代码保护机制来检测和消除恶意代码；b. 根据组织的配置管理策略和程序，每当有新版本可用时，就会更新恶意代码保护机制；c. 将恶意代码保护机制配置为：1. 在根据组织的安全策略，定期扫描信息系统 [分配：组织定义的频率]，并在 [选择（一项或多项）；端点；网络入口/出口点] 下载、打开或执行来自外部来源的文件时实时扫描文件；以及 2. [选择（一项或多项）：阻止恶意代码；隔离恶意代码；向管理员发送警报；[分配：组织定义的操作]] 以响应检测到的恶意代码；以及 d. 解决恶意代码检测和清除过程中的误报问题，以及由此对信息系统可用性造成的潜在影响。补充指南：信息系统的入口和出口点包括防火墙、电子邮件服务器、Web	ecs-task-definition-memory-hard-limit	限制 Amazon Elastic Container Service (ECS) 容器可用的最大内存可确保您的资源使用量不会在容器遭到恶意访问时被滥用。

控制 ID	控制描述	AWS Config 规则	指南
	服务器、代理服务器、远程访问服务器、工作站、笔记本电脑和移动设备。例如，恶意代码包括病毒、蠕虫、特洛伊木马和间谍软件。恶意代码也可以以各种格式（例如 UUENCODE、Unicode）编码，包含在压缩或隐藏文件中，或者使用隐写术隐藏在文件中。恶意代码可以通过不同的方式传输，例如，网络访问、电子邮件、电子邮件附件和便携式存储设备。恶意代码插入是通过利用信息系统漏洞进行的。例如，恶意代码保护机制包括防病毒签名定义和基于信誉的技术。有多种技术和方法可以限制或消除恶意代码的影响。无处不在的配置管理和全面的软件完整性控制可以有效防止未经授权的代码的执行。除商业 off-the-shelf 软件外，定制软件中也可能存在恶意代码。例如，这可能包括逻辑炸弹、后		

控制 ID	控制描述	AWS Config 规则	指南
	门以及其他可能影响组织任务/业务职能的网络攻击。传统的恶意代码保护机制无法始终检测到此类代码。在这些情况下，组织转而依赖其他保护措施，包括安全编码实践、配置管理和控制、可信采购流程和监控实践，以帮助确保软件不会执行预期功能以外的功能。组织可能会决定，为了应对检测到的恶意代码，可能需要采取不同的行动。例如，组织可以定义针对定期扫描期间检测到的恶意代码的操作、针对检测到恶意下载的操作，和/或针对在尝试打开或执行文件时检测到的恶意行为的操作。相关控制：CM-3、MP-2、SA-4、SA-8、SA-12、SA-13、SC-7、SC-26、SC-44、SI-2、SI-4、SI-7。参考文献：NIST 专题出版物 800-83。		

控制 ID	控制描述	AWS Config 规则	指南
SI-4(1)	组织将各个入侵检测工具连接起来并配置到信息系统范围的入侵检测系统中。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(4)	信息系统持续监控入站和出站通信流量，以发现异常或未经授权的活动或情况。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI-4(4)	信息系统持续监控入站和出站通信流量，以发现异常或未经授权的活动或情况。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(4)	信息系统持续监控入站和出站通信流量，以发现异常或未经授权的活动或情况。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI-4(4)	信息系统持续监控入站和出站通信流量，以发现异常或未经授权的活动或情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(5)	当出现以下感染或潜在感染迹象时，信息系统会提醒 [分配：组织定义的人员或角色]：[分配：组织定义的感染指标]。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI-4(5)	当出现以下感染或潜在感染迹象时，信息系统会提醒 [分配：组织定义的人员或角色]：[分配：组织定义的感染指标]。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(5)	当出现以下感染或潜在感染迹象时，信息系统会提醒 [分配：组织定义的人员或角色]：[分配：组织定义的感染指标]。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI-4(5)	当出现以下感染或潜在感染迹象时，信息系统会提醒 [分配：组织定义的人员或角色]：[分配：组织定义的感染指标]。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(16)	组织将来自整个信息系统中使用的监控工具的信息关联起来。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(16)	组织将来自整个信息系统中使用的监控工具的信息关联起来。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SI-4(16)	组织将来自整个信息系统中使用的监控工具的信息关联起来。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(16)	组织将来自整个信息系统中使用的监控工具的信息关联起来。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SI-4(16)	组织将来自整个信息系统中使用的监控工具的信息关联起来。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(16)	组织将来自整个信息系统中使用的监控工具的信息关联起来。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-5	组织：a. 持续接收来自 [分配：组织定义的外部组织] 的信息系统安全警报、公告和指令；b. 根据需要生成内部安全警报、公告和指令；c. 向以下对象发布安全警报、建议和指令：[选择（一项或多项）：[分配：组织定义的人员或角色]；[分配：组织定义的组织内要素]；[分配：组织定义的外部组织]]；以及 d. 根据既定的时间框架实施安全指令，或将违规程度通知发布组织。补充指南：美国计算机应急准备小组 (US-CERT) 生成安全警报和建议，让联邦政府能够了解态势。安全指令由 OMB 或其他指定组织发布，他们有责任和权力发布此类指令。遵守安全指令至关重要，因为其中许多指令都非常重要，如果不及时执行这些指令，可能会对组织业务和资产、个人、其他组织和国家造成直接不利影响。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
	例如，外部组织包括外部任务/业务合作伙伴、供应链合作伙伴、外部服务提供商和其他同行/支持组织。相关控制：SI-2。参考文献：NIST 专题出版物 800-40。		

控制 ID	控制描述	AWS Config 规则	指南
SI-5	组织：a. 持续接收来自 [分配：组织定义的外部组织] 的信息系统安全警报、公告和指令；b. 根据需要生成内部安全警报、公告和指令；c. 向以下对象发布安全警报、建议和指令：[选择（一项或多项）：[分配：组织定义的人员或角色]；[分配：组织定义的组织内要素]；[分配：组织定义的外部组织]]；以及 d. 根据既定的时间框架实施安全指令，或将违规程度通知发布组织。补充指南：美国计算机应急准备小组 (US-CERT) 生成安全警报和建议，让联邦政府能够了解态势。安全指令由 OMB 或其他指定组织发布，他们有责任和权力发布此类指令。遵守安全指令至关重要，因为其中许多指令都非常重要，如果不及时执行这些指令，可能会对组织业务和资产、个人、其他组织和国家造成直接不利影响。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
	例如，外部组织包括外部任务/业务合作伙伴、供应链合作伙伴、外部服务提供商和其他同行/支持组织。相关控制：SI-2。参考文献：NIST 专题出版物 800-40。		

控制 ID	控制描述	AWS Config 规则	指南
SI-5	组织：a. 持续接收来自 [分配：组织定义的外部组织] 的信息系统安全警报、公告和指令；b. 根据需要生成内部安全警报、公告和指令；c. 向以下对象发布安全警报、建议和指令：[选择（一项或多项）：[分配：组织定义的人员或角色]；[分配：组织定义的组织内要素]；[分配：组织定义的外部组织]]；以及 d. 根据既定的时间框架实施安全指令，或将违规程度通知发布组织。补充指南：美国计算机应急准备小组 (US-CERT) 生成安全警报和建议，让联邦政府能够了解态势。安全指令由 OMB 或其他指定组织发布，他们有责任和权力发布此类指令。遵守安全指令至关重要，因为其中许多指令都非常重要，如果不及时执行这些指令，可能会对组织业务和资产、个人、其他组织和国家造成直接不利影响。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
	例如，外部组织包括外部任务/业务合作伙伴、供应链合作伙伴、外部服务提供商和其他同行/支持组织。相关控制：SI-2。参考文献：NIST 专题出版物 800-40。		

控制 ID	控制描述	AWS Config 规则	指南
SI-5	组织：a. 持续接收来自 [分配：组织定义的外部组织] 的信息系统安全警报、公告和指令；b. 根据需要生成内部安全警报、公告和指令；c. 向以下对象发布安全警报、建议和指令：[选择（一项或多项）：[分配：组织定义的人员或角色]；[分配：组织定义的组织内要素]；[分配：组织定义的外部组织]]；以及 d. 根据既定的时间框架实施安全指令，或将违规程度通知发布组织。补充指南：美国计算机应急准备小组 (US-CERT) 生成安全警报和建议，让联邦政府能够了解态势。安全指令由 OMB 或其他指定组织发布，他们有责任和权力发布此类指令。遵守安全指令至关重要，因为其中许多指令都非常重要，如果不及时执行这些指令，可能会对组织业务和资产、个人、其他组织和国家造成直接不利影响。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
	例如，外部组织包括外部任务/业务合作伙伴、供应链合作伙伴、外部服务提供商和其他同行/支持组织。相关控制：SI-2。参考文献：NIST 专题出版物 800-40。		
SI-7(1)	信息系统至少每月对安全相关事件进行一次完整性检查。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(1)	信息系统至少每月对安全相关事件进行一次完整性检查。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SI-7(1)	信息系统至少每月对安全相关事件进行一次完整性检查。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
SI-7	组织使用完整性验证工具来检测对 [分配：组织定义的软件、固件和信息] 的未经授权的更改。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
SI-11	信息系统：a. 生成错误消息，提供纠正措施所必需的信息，而不会泄露可能被对手利用的信息；以及 b. 仅向 [分配：组织定义的人员或角色] 显示错误消息。补充指南：组织仔细考虑错误消息的结构/内容。信息系统能在多大程度上识别和处理错误情况，取决于组织政策和操作要求。可能被对手利用的信息包括：错误的登录尝试（密码被错误地输入为用户名）、可从所记录的信息（如果没有明确说明）中推导出的任务/业务信息，以及个人信息（如账号、社会保险号和信用卡号）。此外，错误消息可能为传输信息提供一个秘密渠道。相关控制：AU-2、AU-3、SC-31。控制增强功能：无。参考文献：无。	[api-gw-execution-logging-enabled](#)	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
SI-11	信息系统：a. 生成错误消息，提供纠正措施所必需的信息，而不会泄露可能被对手利用的信息；以及 b. 仅向 [分配：组织定义的人员或角色] 显示错误消息。补充指南：组织仔细考虑错误消息的结构/内容。信息系统能在多大程度上识别和处理错误情况，取决于组织政策和操作要求。可能被对手利用的信息包括：错误的登录尝试（密码被错误地输入为用户名）、可从所记录的信息（如果没有明确说明）中推导出的任务/业务信息，以及个人信息（如账号、社会保险号和信用卡号）。此外，错误消息可能为传输信息提供一个秘密渠道。相关控制：AU-2、AU-3、SC-31。控制增强功能：无。参考文献：无。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-11	信息系统：a. 生成错误消息，提供纠正措施所必需的信息，而不会泄露可能被对手利用的信息；以及 b. 仅向 [分配：组织定义的人员或角色] 显示错误消息。补充指南：组织仔细考虑错误消息的结构/内容。信息系统能在多大程度上识别和处理错误情况，取决于组织政策和操作要求。可能被对手利用的信息包括：错误的登录尝试（密码被错误地输入为用户名）、可从所记录的信息（如果没有明确说明）中推导出的任务/业务信息，以及个人信息（如账号、社会保险号和信用卡号）。此外，错误消息可能为传输信息提供一个秘密渠道。相关控制：AU-2、AU-3、SC-31。控制增强功能：无。参考文献：无。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

控制 ID	控制描述	AWS Config 规则	指南
SI-11	信息系统：a. 生成错误消息，提供纠正措施所必需的信息，而不会泄露可能被对手利用的信息；以及 b. 仅向 [分配：组织定义的人员或角色] 显示错误消息。补充指南：组织仔细考虑错误消息的结构/内容。信息系统能在多大程度上识别和处理错误情况，取决于组织政策和操作要求。可能被对手利用的信息包括：错误的登录尝试（密码被错误地输入为用户名）、可从所记录的信息（如果没有明确说明）中推导出的任务/业务信息，以及个人信息（如账号、社会保险号和信用卡号）。此外，错误消息可能为传输信息提供一个秘密渠道。相关控制：AU-2、AU-3、SC-31。控制增强功能：无。参考文献：无。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
SI-11	信息系统：a. 生成错误消息，提供纠正措施所必需的信息，而不会泄露可能被对手利用的信息；以及 b. 仅向 [分配：组织定义的人员或角色] 显示错误消息。补充指南：组织仔细考虑错误消息的结构/内容。信息系统能在多大程度上识别和处理错误情况，取决于组织政策和操作要求。可能被对手利用的信息包括：错误的登录尝试（密码被错误地输入为用户名）、可从所记录的信息（如果没有明确说明）中推导出的任务/业务信息，以及个人信息（如账号、社会保险号和信用卡号）。此外，错误消息可能为传输信息提供一个秘密渠道。相关控制：AU-2、AU-3、SC-31。控制增强功能：无。参考文献：无。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
SI-11	信息系统：a. 生成错误消息，提供纠正措施所必需的信息，而不会泄露可能被对手利用的信息；以及 b. 仅向 [分配：组织定义的人员或角色] 显示错误消息。补充指南：组织仔细考虑错误消息的结构/内容。信息系统能在多大程度上识别和处理错误情况，取决于组织政策和操作要求。可能被对手利用的信息包括：错误的登录尝试（密码被错误地输入为用户名）、可从所记录的信息（如果没有明确说明）中推导出的任务/业务信息，以及个人信息（如账号、社会保险号和信用卡号）。此外，错误消息可能为传输信息提供一个秘密渠道。相关控制：AU-2、AU-3、SC-31。控制增强功能：无。参考文献：无。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
SI-11	信息系统：a. 生成错误消息，提供纠正措施所必需的信息，而不会泄露可能被对手利用的信息；以及 b. 仅向 [分配：组织定义的人员或角色] 显示错误消息。补充指南：组织仔细考虑错误消息的结构/内容。信息系统能在多大程度上识别和处理错误情况，取决于组织政策和操作要求。可能被对手利用的信息包括：错误的登录尝试（密码被错误地输入为用户名）、可从所记录的信息（如果没有明确说明）中推导出的任务/业务信息，以及个人信息（如账号、社会保险号和信用卡号）。此外，错误消息可能为传输信息提供一个秘密渠道。相关控制：AU-2、AU-3、SC-31。控制增强功能：无。参考文献：无。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
SI-16	信息系统实施 [分配：组织定义的安全保护措施]，以保护其内存免受未经授权的代码执行的侵害。补充指南：一些对手发起攻击，目的是在内存的不可执行区域或被禁止的内存位置执行代码。例如，用于保护内存的安全措施包括数据执行防护和地址空间布局随机化。数据执行保护措施可以由硬件强制执行，也可以由软件强制执行，硬件提供的机制强度更大。相关控制：AC-25、SC-3。控制增强功能：无。参考文献：无。	ecs-task-definition-memory-hard-limit	限制 Amazon Elastic Container Service (ECS) 容器可用的最大内存可确保您的资源使用量不会在容器遭到恶意访问时被滥用。

模板

该模板可在以下网址获得 GitHub：FedRAMP 操作最佳实践（中级）。

FFIEC 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了联邦金融机构考试委员会 (FFIEC) 网络安全评估工具域和 AWS 托管 Config 规则之间的映射示例。每条 Confic 规则都适用于特定 AWS 资源，并与一个或多个 FFIEC 网络安全评估工具控件相

关。一个 FFIEC 网络安全评估工具控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
D1.G.IT.B.1	维护组织资产（例如，外部托管的硬件、软件、数据和系统）清单。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
D1.G.IT.B.1	维护组织资产（例如，外部托管的硬件、软件、数据和系统）清单。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
D1.G.IT.B.1	维护组织资产（例如，外部托管的硬件、软件、数据和系统）清单。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例

控制 ID	控制描述	AWS Config 规则	指南
			终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
D1.G.IT.B.1	维护组织资产（例如，外部托管的硬件、软件、数据和系统）清单。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
D1.RM.Rm.B.1	机构内设有信息安全和业务连续性风险管理职能。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
D1.RM.RA.B.2	风险评估可确定基于互联网的系统和需要进行额外身份验证控制的高风险事务。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
D1.RM.RA.B.2	风险评估可确定基于互联网的系统和需要进行额外身份验证控制的高风险事务。	annual-risk-assessment-performed（过程检查）	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。

控制 ID	控制描述	AWS Config 规则	指南
D1.TC.Tr.B.2	年度信息安全培训包括事件响应、当前的网络威胁（例如网络钓鱼、鱼叉式网络钓鱼、社交工程和移动安全）和新出现的问题。	security-awareness-program-exists（过程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
D2.IS.Is.B.1	收集信息安全威胁并与相应的内部员工共享。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
D2.IS.Is.B.1	收集信息安全威胁并与相应的内部员工共享。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
D2.IS.Is.B.1	收集信息安全威胁并与相应的内部员工共享。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	cw-loggroup-retent ion-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.1	审计日志记录和其他安全事件日志将以安全的方式进行审查和保存。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	redshift-cluster-c onfiguration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D2.MA.Ma.B.2	计算机事件日志用于在事件发生后进行调查。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
D2.TI.Ti.B.1	该机构属于或订阅提供威胁信息的威胁和漏洞信息共享来源（例如，FS-ISAC、US-CERT）。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
D2.TI.Ti.B.1	该机构属于或订阅提供威胁信息的威胁和漏洞信息共享来源（例如，FS-ISAC、US-CERT）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
D2.TI.Ti.B.2	威胁信息用于监控威胁和漏洞。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
D2.TI.Ti.B.2	威胁信息用于监控威胁和漏洞。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
D2.TI.Ti.B.2	威胁信息用于监控威胁和漏洞。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
D2.TI.Ti.B.3	威胁信息用于加强内部风险管理和控制。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
D2.TI.Ti.B.3	威胁信息用于加强内部风险管理和控制。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
D3.CC.PM.B.1	实施补丁管理程序，确保及时应用软件和固件补丁。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
D3.CC.PM.B.1	实施补丁管理程序，确保及时应用软件和固件补丁。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
D3.CC.PM.B.1	实施补丁管理程序，确保及时应用软件和固件补丁。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
D3.CC.PM.B.1	实施补丁管理程序，确保及时应用软件和固件补丁。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
D3.CC.PM.B.3	补丁管理报告会接受审查，并反映缺少的安全补丁。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
D3.CC.PM.B.3	补丁管理报告会接受审查，并反映缺少的安全补丁。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
D3.CC.PM.B.3	补丁管理报告会接受审查，并反映缺少的安全补丁。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
D3.CC.PM.B.3	补丁管理报告会接受审查，并反映缺少的安全补丁。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.1	机构能够通过监控整个环境来检测异常活动。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
D3.DC.An.B.1	机构能够通过监控整个环境来检测异常活动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.1	机构能够通过监控整个环境来检测异常活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
D3.DC.An.B.2	监控和审查生成异常活动警报的客户交易。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.2	监控和审查生成异常活动警报的客户交易。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.3	事件发生后，将审查物理和/或逻辑访问日志。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
D3.DC.An.B.4	监控第三方对关键系统的访问，以防未经授权或出现异常活动	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
D3.DC.An.B.5	监控提升的特权。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.An.B.5	监控提升的特权。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
D3.DC.Ev.B.1	建立了正常网络活动基线。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
D3.DC.Ev.B.1	建立了正常网络活动基线。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
D3.DC.Ev.B.1	建立了正常网络活动基线。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.Ev.B.1	建立了正常网络活动基线。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
D3.DC.Ev.B.1	建立了正常网络活动基线。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
D3.DC.Ev.B.1	建立了正常网络活动基线。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.Ev.B.1	建立了正常网络活动基线。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.Ev.B.1	建立了正常网络活动基线。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
D3.DC.Ev.B.1	建立了正常网络活动基线。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.Ev.B.2	已建立机制（例如防病毒警报、日志事件警报），以提醒管理层注意潜在的攻击。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
D3.DC.Ev.B.3	已制定流程来监控是否存在未经授权的用户、设备、连接和软件。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
D3.DC.Ev.B.3	已制定流程来监控是否存在未经授权的用户、设备、连接和软件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.Ev.B.3	已制定流程来监控是否存在未经授权的用户、设备、连接和软件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
D3.DC.Ev.B.3	已制定流程来监控是否存在未经授权的用户、设备、连接和软件。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.Th.B.1	独立测试（包括渗透测试和漏洞扫描）是根据面向外部的系统和内部网络的风险评估进行的。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
D3.DC.Th.B.1	独立测试（包括渗透测试和漏洞扫描）是根据面向外部的系统和内部网络的风险评估进行的。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
D3.DC.Th.B.1	独立测试（包括渗透测试和漏洞扫描）是根据面向外部的系统和内部网络的风险评估进行的。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
D3.PC.Am.B.1	根据工作职责和最低权限原则，向员工授予访问系统和机密数据的权限。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.10	生产环境和非生产环境是隔离的，以防止未经授权的访问或更改信息资产。（*如果机构或机构的第三方不存在生产环境，则不适用。）	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.10	生产环境和非生产环境是隔离的，以防止未经授权的访问或更改信息资产。（*如果机构或机构的第三方不存在生产环境，则不适用。）	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
D3.PC.Am.B.10	生产环境和非生产环境是隔离的，以防止未经授权的访问或更改信息资产。（*如果机构或机构的第三方不存在生产环境，则不适用。）	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.10	生产环境和非生产环境是隔离的，以防止未经授权的访问或更改信息资产。（*如果机构或机构的第三方不存在生产环境，则不适用。）	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
D3.PC.Am.B.12	所有密码在存储和传输过程中都经过加密。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.13	机密数据在通过公共或不可信网络（例如 Internet）传输时会被加密。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
D3.PC.Am.B.13	机密数据在通过公共或不可信网络（例如 Internet）传输时会被加密。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.13	机密数据在通过公共或不可信网络（例如 Internet）传输时会被加密。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.13	机密数据在通过公共或不可信网络（例如 Internet）传输时会被加密。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.13	机密数据在通过公共或不可信网络（例如 Internet）传输时会被加密。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.13	机密数据在通过公共或不可信网络（例如 Internet）传输时会被加密。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.13	机密数据在通过公共或不可信网络（例如 Internet）传输时会被加密。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
D3.PC.Am.B.15	员工、承包商和第三方对关键系统的远程访问使用加密连接和多重身份验证。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.15	员工、承包商和第三方对关键系统的远程访问使用加密连接和多重身份验证。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.15	员工、承包商和第三方对关键系统的远程访问使用加密连接和多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
D3.PC.Am.B.15	员工、承包商和第三方对关键系统的远程访问使用加密连接和多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
D3.PC.Am.B.15	员工、承包商和第三方对关键系统的远程访问使用加密连接和多重身份验证。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.15	员工、承包商和第三方对关键系统的远程访问使用加密连接和多重身份验证。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
D3.PC.Am.B.15	员工、承包商和第三方对关键系统的远程访问使用加密连接和多重身份验证。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
D3.PC.Am.B.16	管理、物理或技术控制措施已到位，以防止没有管理责任的用户安装未经授权的软件。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.16	管理、物理或技术控制措施已到位，以防止没有管理责任的用户安装未经授权的软件。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
D3.PC.Am.B.16	管理、物理或技术控制措施已到位，以防止没有管理责任的用户安装未经授权的软件。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
D3.PC.Am.B.16	管理、物理或技术控制措施已到位，以防止没有管理责任的用户安装未经授权的软件。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.2	员工对系统和机密数据的访问实行职责分离。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
D3.PC.Am.B.2	员工对系统和机密数据的访问实行职责分离。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
D3.PC.Am.B.2	员工对系统和机密数据的访问实行职责分离。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.3	提升的权限（例如管理员权限）受到限制和严格控制（例如，分配给个人，而不是共享，需要更严格的密码控制）	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
D3.PC.Am.B.3	提升的权限（例如管理员权限）受到限制和严格控制（例如，分配给个人，而不是共享，需要更严格的密码控制）	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
D3.PC.Am.B.3	提升的权限（例如管理员权限）受到限制和严格控制（例如，分配给个人，而不是共享，并且需要更严格的密码控制）。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.3	提升的权限（例如管理员权限）受到限制和严格控制（例如，分配给个人，而不是共享，需要更严格的密码控制）	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
D3.PC.Am.B.3	提升的权限（例如管理员权限）受到限制和严格控制（例如，分配给个人，而不是共享，需要更严格的密码控制）	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
D3.PC.Am.B.3	提升的权限（例如管理员权限）受到限制和严格控制（例如，分配给个人，而不是共享，需要更严格的密码控制）	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
D3.PC.Am.B.6	访问系统、应用程序和硬件需要进行身份识别和身份验证，并对其进行管理。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.7	访问控制包括密码复杂性以及密码尝试次数和重用的限制。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Am.B.8	在系统实施之前，所有默认密码和不必要的默认账户都已更改。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
D3.PC.Im.B.1	使用网络外围防御工具（例如边界路由器和防火墙）。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.IM.B.2	通过互联网或由外部各方访问的系统受到防火墙或其他类似设备的保护。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
D3.PC.IM.B.2	通过互联网或由外部各方访问的系统受到防火墙或其他类似设备的保护。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.IM.B.2	通过互联网或由外部各方访问的系统受到防火墙或其他类似设备的保护。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
D3.PC.IM.B.2	通过互联网或由外部各方访问的系统受到防火墙或其他类似设备的保护。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.IM.B.2	通过互联网或由外部各方访问的系统受到防火墙或其他类似设备的保护。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
D3.PC.IM.B.2	通过互联网或由外部各方访问的系统受到防火墙或其他类似设备的保护。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.IM.B.3	所有端口都受到监控。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
D3.PC.IM.B.3	所有端口都受到监控。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
D3.PC.IM.B.3	所有端口都受到监控。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.IM.B.3	所有端口都受到监控。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
D3.PC.IM.B.3	所有端口都受到监控。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.IM.B.3	所有端口都受到监控。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
D3.PC.Im.B.5	（服务器、台式机、路由器等的）系统配置遵循行业标准并强制执行	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.5	（服务器、台式机、路由器等的）系统配置遵循行业标准并强制执行	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
D3.PC.Im.B.5	（服务器、台式机、路由器等的）系统配置遵循行业标准并强制执行	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.IM.B.6	禁止使用业务目的不再需要的端口、功能、协议和服务。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
D3.PC.IM.B.6	禁止使用业务目的不再需要的端口、功能、协议和服务。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.IM.B.6	禁止使用业务目的不再需要的端口、功能、协议和服务。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
D3.PC.IM.B.6	禁止使用业务目的不再需要的端口、功能、协议和服务。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.7	对系统配置（包括虚拟机和虚拟机管理程序）进行更改的权限受到控制和监控。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
D3.PC.Im.B.7	对系统配置（包括虚拟机和虚拟机管理程序）进行更改的权限受到控制和监控。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
D3.PC.Im.B.7	对系统配置（包括虚拟机和虚拟机管理程序）进行更改的权限受到控制和监控。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.7	对系统配置（包括虚拟机和虚拟机管理程序）进行更改的权限受到控制和监控。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
D3.PC.Im.B.7	对系统配置（包括虚拟机和虚拟机管理程序）进行更改的权限受到控制和监控。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
D3.PC.Im.B.7	对系统配置（包括虚拟机和虚拟机管理程序）进行更改的权限受到控制和监控。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
D3.PC.Im.B.7	对系统配置（包括虚拟机和虚拟机管理程序）进行更改的权限受到控制和监控。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
D3.PC.Se.B.1	在该机构工作的开发人员遵循符合行业标准的安全程序编码实践，这是系统开发生命周期 (SDLC) 的一部分。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
D3.PC.Se.B.1	在该机构工作的开发人员遵循符合行业标准的安全程序编码实践，这是系统开发生命周期 (SDLC) 的一部分。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	控制描述	AWS Config 规则	指南
D4.C.Co.B.2	该机构确保第三方连接获得授权。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
D4.C.Co.B.2	该机构确保第三方连接获得授权。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
D4.C.Co.B.2	该机构确保第三方连接获得授权。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
D4.C.Co.B.2	该机构确保第三方连接获得授权。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.1	设置警报参数用于检测信息安全事件，从而提示采取缓解措施。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.1	设置警报参数用于检测信息安全事件，从而提示采取缓解措施。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
D5.DR.De.B.1	设置警报参数用于检测信息安全事件，从而提示采取缓解措施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.2	系统性能报告包含可用作风险指标以检测信息安全事件的信息	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
D5.DR.De.B.2	系统性能报告包含可用作风险指标以检测信息安全事件的信息	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
D5.DR.De.B.3	有工具和流程来检测、提醒和触发事件响应计划。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
D5.ER.Es.B.4	对事件进行分类、记录和跟踪。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.Pl.B.1	该机构记录了它将如何应对和响应网络事件。	response-plan-exists-maintained （过程检查）	确保制定和维护事件响应计划，并将其分发给负责人。
D5.IR.Pl.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
D5.IR.Pl.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
D5.IR.PI.B.6	该机构计划利用业务连续性、灾难恢复和数据备份计划在事件发生后恢复业务。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

模板

该模板可在以下网址获得 GitHub：FFIEC 运营最佳实践。

德国云计算合规性条件目录 (C5) 操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了德国云计算合规性标准目录 (C5) 和 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个德国 C5 控件相关。一个德国 C5 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	AWS Config 规则	指南
COS-01	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
COS-01	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	AWS Config 规则	指南
COS-01	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。
COS-01	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。
COS-01	waf-regional-webacl-not-empty	连接到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
COS-01	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
COS-03	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
COS-03	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
COS-03	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
COS-03	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
COS-03	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	AWS Config 规则	指南
COS-03	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
COS-03	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
COS-03	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
COS-03	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
COS-03	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
COS-03	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	AWS Config 规则	指南
COS-03	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
COS-03	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
COS-03	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
COS-03	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
COS-03	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
COS-03	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
COS-03	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
COS-03	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
COS-03	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
COS-03	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
COS-05	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
COS-05	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
COS-05	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
COS-05	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
COS-05	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
COS-05	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
COS-05	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
COS-05	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
COS-05	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
COS-05	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
COS-05	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
COS-05	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	AWS Config 规则	指南
COS-05	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
CRY-02	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CRY-02	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	AWS Config 规则	指南
CRY-02	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
CRY-02	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
CRY-02	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CRY-02	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CRY-02	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CRY-02	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CRY-02	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CRY-03	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CRY-03	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
CRY-03	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
CRY-03	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
CRY-03	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CRY-03	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
CRY-03	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
CRY-03	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CRY-03	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
CRY-03	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
CRY-03	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
CRY-03	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	AWS Config 规则	指南
CRY-03	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CRY-03	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
CRY-03	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CRY-03	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
CRY-03	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CRY-03	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
CRY-03	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
CRY-03	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
CRY-04	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
DEV-07	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
DEV-07	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
DEV-07	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
DEV-07	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
DEV-07	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
DEV-07	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
IDM-01	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
IDM-01	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	AWS Config 规则	指南
IDM-01	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
IDM-01	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
IDM-01	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
IDM-01	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IDM-01	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
IDM-01	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IDM-01	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IDM-01	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IDM-01	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	AWS Config 规则	指南
IDM-01	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
IDM-01	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
IDM-01	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
IDM-01	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	AWS Config 规则	指南
IDM-01	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。
IDM-01	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
IDM-01	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
IDM-01	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。

控制 ID	AWS Config 规则	指南
IDM-01	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。
IDM-01	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
IDM-01	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。 OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。 OpenSearch

控制 ID	AWS Config 规则	指南
IDM-01	rds-instance-iam-authentication-enabled	确保在亚马逊关系数据库服务 (Amazon RDS) 实例上启用 AWS 身份和访问管理 (IAM) 身份验证，以控制对系统和资产的访问。这会强制进出数据库的网络流量使用安全套接字层 (SSL) 进行加密。您无需将用户凭证存储在数据库中，因为身份验证在外部进行管理。
IDM-01	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。
IDM-03	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（ Config 默认值：90 ）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
IDM-03	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays （ Config 默认值：90 ）。实际值应反映贵组织的策略。
IDM-08	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters （ AWS 基础安全最佳实践值：true ）、 RequireLowercaseCharacters （ AWS 基础安全最佳实践值：true ）、 RequireSymbols （ AWS 基础安全最佳实践值：true ）、 RequireNumbers （ AWS 基础安全最佳实践值：true ）、 MinimumPasswordLength （ AWS 基础安全最佳实践值：14 ）、 PasswordReusePrevention （ AWS 基础安全最佳实践值：24 ）和 MaxPasswordAge （ AWS 基础安全最佳实践值：90 ）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
CRY-01	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
IDM-09	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
IDM-09	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IDM-09	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IDM-09	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
OPS-01	clb-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。

控制 ID	AWS Config 规则	指南
OPS-01	elbv2-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
OPS-01	lambda-vpc-multi-az-check	如果您的 AWS Lambda 函数配置为连接到您账户中的虚拟私有云 (VPC)，请在至少两个不同的可用区中部署 AWS Lambda 函数，以确保在单个区域发生服务中断的情况下，您的函数可用于处理事件。
OPS-01	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	AWS Config 规则	指南
OPS-01	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
OPS-01	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
OPS-01	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	AWS Config 规则	指南
OPS-01	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
OPS-02	clb-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
OPS-02	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	AWS Config 规则	指南
OPS-02	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
OPS-02	elbv2-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
OPS-02	lambda-vpc-multi-az-check	如果您的 AWS Lambda 函数配置为连接到您账户中的虚拟私有云 (VPC)，请在至少两个不同的可用区中部署 AWS Lambda 函数，以确保在单个区域发生服务中断的情况下，您的函数可用于处理事件。

控制 ID	AWS Config 规则	指南
OPS-02	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
OPS-02	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	AWS Config 规则	指南
OPS-02	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
OPS-02	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
OPS-02	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
OPS-07	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
OPS-07	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
OPS-07	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	AWS Config 规则	指南
OPS-07	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
OPS-07	opensearch-data-node-fault-tolerance	为了实现高可用性和容错能力，Amazon OpenSearch OpenSearch 服务（服务）至少需要三个数据节点。部署具有至少三个数据节点的 OpenSearch 服务域可确保在节点出现故障时集群运行。
OPS-07	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
OPS-07	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	AWS Config 规则	指南
OPS-07	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
OPS-07	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
OPS-07	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
OPS-07	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
OPS-07	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
OPS-07	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
OPS-07	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
OPS-07	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
OPS-12	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
OPS-12	s3-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	AWS Config 规则	指南
OPS-13	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
OPS-13	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
OPS-13	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
OPS-14	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
OPS-14	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
OPS-14	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
OPS-14	s3-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
OPS-15	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	AWS Config 规则	指南
OPS-15	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
OPS-15	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
OPS-15	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
OPS-15	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	AWS Config 规则	指南
OPS-15	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
OPS-15	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
OPS-15	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
OPS-15	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。

控制 ID	AWS Config 规则	指南
OPS-15	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
OPS-15	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
OPS-15	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
OPS-15	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
OPS-15	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
OPS-15	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	AWS Config 规则	指南
OPS-15	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
OPS-22	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
PSS-05	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
PSS-05	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
PSS-05	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
PSS-05	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	AWS Config 规则	指南
PSS-07	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

模板

该模板可在以下网址获得 GitHub：德国云计算合规标准目录 (C5)。

《格雷姆-里奇-布里利法案》(GLBA) 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

下面提供了《格雷姆-里奇-布里利法案》(GLBA) 与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 GLBA 控件相关。一个 GLBA 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云

控制 ID	控制描述	AWS Config 规则	指南
	行政、技术和物理保障措施有关的适当标准。		（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
GLBA-SEC.501(b)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(1)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (1) 以确保客户记录和信息的安全性和保密性；	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
GLBA-SEC.501(b)(2)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (2) 以保护这些记录的安全性或完整性免受任何预期的威胁或危害；以及	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(2)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (2) 以保护这些记录的安全性或完整性免受任何预期的威胁或危害；以及	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	opensearch-access-control-enabled	确保在您的亚马逊 OpenSearch 服务域上启用精细访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
GLBA-SEC.501(b)(3)	为了推进 (a) 款中的政策，第 505(a) 款中描述的每个机构或部门都应为其管辖范围内的金融机构制定与行政、技术和物理保障措施有关的适当标准 (3) 以防止未经授权访问或使用此类记录或信息，从而可能给任何客户造成重大伤害或不便；以及	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

模板

该模板可在以下网址获得 GitHub：《Gramm Leach Bliley Act》（GLBA）的运营最佳实践。

GxP 欧盟附件 11 操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保

遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

下面提供了 GxP EU 附录 11 和 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一项或多项 GxP EU 附录 11 控制措施相关。一个 GxP 欧盟附件 11 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
1. 风险管理	应在计算机化系统的整个生命周期中运用风险管理，同时考虑到患者安全、数据完整性和产品质量。作为风险管理系统的一部分，应基于对计算机化系统的合理和有据可查的风险评估，做出关于验证范围和数据完整性控制的决策。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
1. 风险管理	应在计算机化系统的整个生命周期中运用风险管理，同时考虑到患者安全、数据完整性和产品质量。作为风险管理系统的一部分，应基于对计算机化系统的合理和有据可查的风险评估，做出关于验证范围和数据完整性控制的决策。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及

控制 ID	控制描述	AWS Config 规则	指南
			AWS 合作伙伴解决方案。 AWS
4.2。验证 - 文档变更控制	验证文档应包括变更控制记录（如果适用）和关于在验证过程中观察到的任何偏差的报告。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
4.3。验证 - 清单	应提供所有相关系统及其 GMP 功能（清单）的最新清单。对于关键系统，应提供最新的系统描述，详细说明物理和逻辑安排、数据流以及与其他系统或流程的接口、任何硬件和软件先决条件以及安全措施。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
4.3。验证 - 清单	应提供所有相关系统及其 GMP 功能（清单）的最新清单。对于关键系统，应提供最新的系统描述，详细说明物理和逻辑安排、数据流以及与其他系统或流程的接口、任何硬件和软件先决条件以及安全措施。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
4.3。验证 - 清单	应提供所有相关系统及其 GMP 功能（清单）的最新清单。对于关键系统，应提供最新的系统描述，详细说明物理和逻辑安排、数据流以及与其他系统或流程的接口、任何硬件和软件先决条件以及安全措施。	ec2-security-group-attached-to-eni-periodic	为了帮助管理资产清单，此规则检查安全组是否附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或弹性网络接口。如果您的安全组未附加到这些资源类型，则它们可能未被使用且不再需要。

控制 ID	控制描述	AWS Config 规则	指南
4.3。验证 - 清单	应提供所有相关系统及其 GMP 功能（清单）的最新清单。对于关键系统，应提供最新的系统描述，详细说明物理和逻辑安排、数据流以及与其他系统或流程的接口、任何硬件和软件先决条件以及安全措施。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
4.3。验证 - 清单	应提供所有相关系统及其 GMP 功能（清单）的最新清单。对于关键系统，应提供最新的系统描述，详细说明物理和逻辑安排、数据流以及与其他系统或流程的接口、任何硬件和软件先决条件以及安全措施。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
4.3。验证 - 清单	应提供所有相关系统及其 GMP 功能（清单）的最新清单。对于关键系统，应提供最新的系统描述，详细说明物理和逻辑安排、数据流以及与其他系统或流程的接口、任何硬件和软件先决条件以及安全措施。	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
4.8。验证 - 数据传输	如果将数据传输到其他数据格式或系统，则验证应包括检查在此迁移过程中数据的值和/或含义是否没有改变。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
5. 数据	与其他系统以电子方式交换数据的计算机化系统应包括适当的内置检查，以正确、安全地输入和处理数据，从而最大限度地降低风险。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
7.1。数据存储 - 损坏保护	应通过物理和电子手段保护数据免受损坏。应检查存储的数据的可访问性、可读性和准确性。应确保在整个保留期内都能访问数据。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
7.2。数据存储 - 备份	应定期备份所有相关数据。在验证期间，应检查备份数据的完整性和准确性以及恢复数据的能力，并定期对其进行监控。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
9. 审计跟踪记录	应考虑在风险评估的基础上，在系统中创建所有与 GMP 相关的更改和删除的记录（系统生成的“审计跟踪记录”）。对于 GMP 相关数据的更改或删除，应记录原因。审计跟踪记录需要可用，可转换为普遍可理解的形式，并定期进行审查。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
10. 变更和配置管理	对计算机化系统的任何更改（包括系统配置）只能按照规定的程序以受控方式进行。	elb-deletion-prote ction-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
10. 变更和配置管理	对计算机化系统的任何更改（包括系统配置）只能按照规定的程序以受控方式进行。	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
10. 变更和配置管理	对计算机化系统的任何更改（包括系统配置）只能按照规定的程序以受控方式进行。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
11. 评估期	应定期对计算机化系统进行评估，确认其保持有效状态并符合 GMP 要求。适当时，此类评估应包括当前的功能范围、偏差记录、事件、问题、升级历史记录、性能、可靠性、安全性和验证状态报告。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	ecs-containers-non privileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	rds-instance-iam-authentication-enabled	确保在亚马逊关系数据库服务 (Amazon RDS) 实例上启用 AWS 身份和访问管理 (IAM) 身份验证，以控制对系统和资产的访问。这会强制进出数据库的网络流量使用安全套接字层 (SSL) 进行加密。您无需将用户凭证存储在数据库中，因为身份验证在外部进行管理。

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Managemen t。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
12.1。安全 - 授权人员	应采取物理和/或逻辑控制措施，仅允许授权人员访问计算机化系统。防止未经授权进入系统的适当方法可能包括使用钥匙、通行卡、带密码的个人代码、生物识别、限制进入计算机设备和数据存储区域。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
12.3。安全 - 授权审计跟踪记录	应记录访问授权的创建、更改和取消。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

控制 ID	控制描述	AWS Config 规则	指南
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REG ION_CLOUD _TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。

控制 ID	控制描述	AWS Config 规则	指南
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
12.4。安全 - 审计跟踪记录	数据和文档管理系统应设计为记录输入、更改、确认或删除数据的操作员的身份（包括日期和时间）。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
13. 事件管理	应报告和评估所有事件，而不仅仅是系统故障和数据错误。应查明重大事件的根本原因，并据此采取纠正和预防行动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
13. 事件管理	应报告和评估所有事件，而不仅仅是系统故障和数据错误。应查明重大事件的根本原因，并据此采取纠正和预防行动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays （配置默认值：35）参数。实际值应反映贵组织的需求。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	elbv2-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	lambda-vpc-multi-az-check	如果您的 AWS Lambda 函数配置为连接到您账户中的虚拟私有云 (VPC)，请在至少两个不同的可用区中部署 AWS Lambda 函数，以确保在单个区域发生服务中断的情况下，您的函数可用于处理事件。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	opensearch-data-node-fault-tolerance	为了实现高可用性和容错能力，Amazon OpenSearch OpenSearch 服务（服务）至少需要三个数据节点。部署具有至少三个数据节点的 OpenSearch 服务域可确保在节点出现故障时集群运行。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
16. 业务连续性	为了提供支持关键流程的计算机化系统，应作出规定，确保在系统出现故障（例如手动系统或替代系统）时继续为这些程序提供支持。实施替代安排所需的时间应以风险为依据，并适合特定系统及其所支持的业务流程。应充分记录和检验这些安排。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
17. 存档	数据可能会被存档。应检查这些数据的可访问性、可读性和完整性。如果要对系统（例如计算机设备或程序）进行相关更改，则应确保并测试检索数据的能力。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

模板

该模板可在以下网址获得 GitHub：GxP 运营最佳实践欧盟附录 11。

HIPAA 安全操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全

确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了《健康保险流通与责任法案》(HIPAA) 与托管 AWS Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 HIPAA 控件相关。一个 HIPAA 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

该合规包已通过 AWS 安全保障服务有限责任公司（AWS SAS）的验证，该公司由支付卡行业合格安全评估员（QSA）、HITRUST认证的通用安全框架从业人员（CCSFP）和经过认证的合规专业人员组成，可以为各种行业框架提供指导和评估。 AWS SAS 专业人员设计此一致性包是为了让客户能够与 HIPAA 的子集保持一致。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(A)	(A) 风险分析（必填）。对所涵盖实体持有的受保护电子健康信息的机密性、完整性和可用性方面的潜在风险和漏洞进行准确、彻底的评估。	annual-risk-assessment-performed （流程检查）	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维

控制 ID	控制描述	AWS Config 规则	指南
	164.306(a) 款的规定。		持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(1)(ii)(B)	(B) 风险管理（必填）。实施足够的安全措施，将风险和漏洞降低到合理适当的水平，以符合第 164.306(a) 款的规定。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(i)	(3)(i) 标准：工作人员安全。实施政策和程序，以确保其所有员工均可根据本节第 (a)(4) 段规定适当访问受保护电子健康信息，并防止本节第 (a)(4) 段未授予访问权限的员工访问受保护电子健康信息。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
164.308(a)(3)(ii)(A)	(A) 授权和/或监督（可处理）。实施相关程序，对使用受保护电子健康信息或在可能访问这些信息的地点工作的员工进行授权和/或监督。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
164.308(a)(3)(ii)(B)	(B) 劳动力许可程序（可处理）。实施相关程序，确定员工对受保护电子健康信息的访问权限是否适当。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(3)(ii)(C)	(C) 终止程序（可处理）。实施相关程序，在员工雇佣关系终止时或根据本款第 (a)(3)(ii)(B) 段规定的决议要求，终止访问受保护电子健康信息。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(i)	(4)(i) 标准：信息访问管理。实施符合本部分 E 小节适用要求的授权访问受保护电子健康信息的政策和程序。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。
164.308(a)(4)(ii)(A)	(A) 隔离医疗保健信息交换中心的职能（必填）。如果医疗保健信息交换中心是大型组织的一部分，则信息交换中心必须实施政策和程序，保护信息交换中心的受保护电子健康信息免遭大型组织未经授权的访问。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
164.308(a)(4)(ii)(B)	(B) 访问授权（可处理）。实施允许访问受保护的电子健康信息的政策和程序，例如，通过访问工作站、交易、程序、流程或其他机制。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。
164.308(a)(4)(ii)(C)	(C) 访问权限的建立和修改（可处理）。实施政策和程序，根据实体的访问授权策略，建立、记录、审查和修改用户访问工作站、交易、程序或流程的权利。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(5)(ii)(A)	(A) 安全提醒（可处理）。定期安全更新。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
164.308(a)(5)(ii)(A)	(A) 安全提醒（可处理）。定期安全更新。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(5)(ii)(A)	(A) 安全提醒（可处理）。定期安全更新。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
164.308(a)(5)(ii)(A)	(A) 安全提醒（可处理）。定期安全更新。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(5)(ii)(B)	(B) 防范恶意软件（可处理）。防御、检测和报告恶意软件的程序。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
164.308(a)(5)(ii)(B)	(B) 防范恶意软件（可处理）。防御、检测和报告恶意软件的程序。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(5)(ii)(B)	(B) 防范恶意软件（可处理）。防御、检测和报告恶意软件的程序。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
164.308(a)(5)(ii)(C)	(C) 登录监控（可处理）。监控登录尝试和报告差异的程序。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
164.308(a)(5)(ii)(C)	(C) 登录监控（可处理）。监控登录尝试和报告差异的程序。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(5)(ii)(C)	(C) 登录监控（可处理）。监控登录尝试和报告差异的程序。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(5)(ii)(D)	(D) 密码管理（可处理）。创建、更改和保护密码的程序。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(6)(i)	(6)(i) 标准：安全事件程序。实施应对安全事件的政策和程序。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
164.308(a)(6)(ii)	(ii) 实施规范：响应和报告（必需）。识别和响应可疑或已知的安全事件；在可行的范围内减轻所涵盖实体已知的安全事件的有害影响；并记录安全事件及其结果。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	rds-multi-az-support	Amazon Relationa l Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
164.308(a)(7)(i)	(7)(i) 标准：应急计划。制定（并根据需要实施）政策和程序，以应对破坏包含受保护电子健康信息的系统的紧急情况或其他事件（例如火灾、蓄意破坏、系统故障和自然灾害）。	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(A)	(A) 数据备份计划（必需）。制定并实施程序，以创建和维护受保护电子健康信息的可检索精确副本。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
164.308(a)(7)(ii)(B)	(B) 灾难恢复计划（必需）。建立（并根据需要实施）恢复任何数据丢失的程序。	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(C)	(C) 紧急模式操作计划（必需）。建立（并根据需要实施）程序，以便在应急模式下继续执行关键业务流程，保护受保护电子健康信息的安全。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
164.308(a)(7)(ii)(C)	(C) 紧急模式操作计划（必需）。建立（并根据需要实施）程序，以便在应急模式下继续执行关键业务流程，保护受保护电子健康信息的安全。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
164.308(a)(7)(ii)(C)	(C) 紧急模式操作计划（必需）。建立（并根据需要实施）程序，以便在应急模式下继续执行关键业务流程，保护受保护电子健康信息的安全。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(C)	(C) 紧急模式操作计划（必需）。建立（并根据需要实施）程序，以便在应急模式下继续执行关键业务流程，保护受保护电子健康信息的安全。	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
164.308(a)(7)(ii)(C)	(C) 紧急模式操作计划（必需）。建立（并根据需要实施）程序，以便在应急模式下继续执行关键业务流程，保护受保护电子健康信息的安全。	rds-multi-az-support	Amazon Relationa l Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(7)(ii)(C)	(C) 紧急模式操作计划（必需）。建立（并根据需要实施）程序，以便在应急模式下继续执行关键业务流程，保护受保护电子健康信息的安全。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
164.308(a)(8)	(8) 标准：评估。定期进行技术和非技术评估，首先基于根据本规则实施的标准，然后根据影响受保护电子健康信息安全的环境或运营变化，确定实体的安全政策和程序在多大程度上符合本子部分的要求。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
164.308(a)(8)	(8) 标准：评估。定期进行技术和非技术评估，首先基于根据本规则实施的标准，然后根据影响受保护电子健康信息安全的环境或运营变化，确定实体的安全政策和程序在多大程度上符合本子部分的要求。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(1)	(a)(1) 标准：访问控制。为维护受保护电子健康信息的电子信息系统实施技术政策和程序，仅允许那些已获得 ¤ 164.308(a)(4) 中规定的访问权限的人员或软件程序进行访问。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
164.312(a)(2)(i)	(2) 实施规范：(i) 唯一用户标识（必需）。分配一个唯一的名称和/或编号以识别和跟踪用户身份。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(ii)	(ii) 紧急访问程序（必需）。制定（并根据需要实施）程序，以便在紧急情况下获取必要的受保护电子健康信息。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(a)(2)(iv)	(iv) 加密和解密（可处理）。实施一种机制来加密和解密受保护电子健康信息。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	s3-event-notifications-enabled	Amazon S3 事件通知可以提醒相关人员注意对您的存储桶对象的任何意外或故意修改。示例警报包括：创建了新对象、对象移除、对象恢复、丢失和复制的对象。

控制 ID	控制描述	AWS Config 规则	指南
164.312(b)	(b) 标准：审计控制。实施硬件、软件和/或程序机制，记录和检查包含或使用受保护电子健康信息的信息系统中的活动。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
164.312(c)(1)	(c)(1) 标准：完整性。实施政策和程序，保护受保护的电子健康信息免遭不当更改或破坏。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(c)(1)	(c)(1) 标准：完整性。实施政策和程序，保护受保护的电子健康信息免遭不当更改或破坏。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
164.312(c)(1)	(c)(1) 标准：完整性。实施政策和程序，保护受保护的电子健康信息免遭不当更改或破坏。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
164.312(c)(1)	(c)(1) 标准：完整性。实施政策和程序，保护受保护的电子健康信息免遭不当更改或破坏。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
164.312(c)(1)	(c)(1) 标准：完整性。实施政策和程序，保护受保护的电子健康信息免遭不当更改或破坏。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(c)(2)	(2) 实施规范：受保护电子健康信息的认证机制（可处理）。实施电子机制，以证实受保护电子健康信息没有被以未经授权的方式更改或销毁。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
164.312(c)(2)	(2) 实施规范：受保护电子健康信息的认证机制（可处理）。实施电子机制，以证实受保护电子健康信息没有被以未经授权的方式更改或销毁。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(c)(2)	(2) 实施规范：受保护电子健康信息的认证机制（可处理）。实施电子机制，以证实受保护电子健康信息没有被以未经授权的方式更改或销毁。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
164.312(c)(2)	(2) 实施规范：受保护电子健康信息的认证机制（可处理）。实施电子机制，以证实受保护电子健康信息没有被以未经授权的方式更改或销毁。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(c)(2)	(2) 实施规范：受保护电子健康信息的认证机制（可处理）。实施电子机制，以证实受保护电子健康信息没有被以未经授权的方式更改或销毁。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
164.312(d)	(d) 标准：个人或实体身份验证。实施程序，以验证寻求访问受保护电子健康信息的个人或实体是否为所声称的个人或实体。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.312(d)	(d) 标准：个人或实体身份验证。实施程序，以验证寻求访问受保护电子健康信息的个人或实体是否为所声称的个人或实体。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
164.312(d)	(d) 标准：个人或实体身份验证。实施程序，以验证寻求访问受保护电子健康信息的个人或实体是否为所声称的个人或实体。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
164.312(d)	(d) 标准：个人或实体身份验证。实施程序，以验证寻求访问受保护电子健康信息的个人或实体是否为所声称的个人或实体。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
164.312(d)	(d) 标准：个人或实体身份验证。实施程序，以验证寻求访问受保护电子健康信息的个人或实体是否为所声称的个人或实体。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELBSecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
164.312(e)(1)	(e)(1) 标准：传输安全。实施技术安全措施，防止未经授权访问通过电子通信网络传输的受保护的电子健康信息。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
164.312(e)(2)(i)	(i) 完整性控制（可处理）。实施安全措施，确保以电子方式传输的受保护的电子健康信息在处置之前不会在未被发现的情况下被不当修改。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELBSecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.312(e)(2)(ii)	(ii) 加密（可处理）。实施一种机制，在适当时对受保护的电子健康信息进行加密。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(1)	(b)(1) 标准：团体健康计划的要求。除非根据 ¤ 164.504(f)(1)(ii) 或 (iii) 或者根据 ¤ 164.508 的授权，来披露已披露给计划发起人的唯一受保护电子健康信息，否则团体健康计划必须确保其计划文件规定计划发起人将合理而适当地保护计划发起人创建、接收、维护，或由计划发起人代表团体健康计划创建、接收、维护，或传输给计划发起人或由计划发起人传输的受保护电子健康信息。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；(ii) 确保通过合理和适当的安全措施来支持 ¤ 164.504(f)(2)(iii) 所要求的适当分离；(iii) 确保向其提供这些信息的任何代理人，包括分包商，同意采取合理和适当的安全措施来保护信息；以及 (iv) 向团体健康计划报告其发现的任何安全事件。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELBSecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
164.314(b)(2)(i)	(2) 实施规范（必填）。必须修改团体健康计划的计划文件，以纳入相关规定，要求计划发起人：(i) 实施管理、物理和技术保障措施，合理而适当地保护其代表团体健康计划创建、接收、维护或传输的受保护的电子健康信息的机密性、完整性和可用性；	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

模板

该模板可在以下网址获得 GitHub：HIPAA 安全最佳运营实践。

IRS 1075 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了 IRS 1075 和 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 IRS 1075 控制措施相关。一个 IRS 1075 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 d. 传输中数据加密	FTI 在云环境内传输时必须加密。用于加密 FTI 的所有机制都必须通过 FIPS 140 认证，并使用符合 FIPS 140 要求的最新模块运行。必须在 SLA 中包含此要求。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.3.1 云计算 d. 传输中数据加密	FTI 在云环境内传输时必须加密。用于加密 FTI 的所有机制都必须通过 FIPS 140 认证，并使用符合 FIPS 140 要求的最新模块运行。必须在 SLA 中包含此要求。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.3.1 云计算 d. 传输中数据加密	FTI 在云环境内传输时必须加密。用于加密 FTI 的所有机制都必须	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听

控制 ID	控制描述	AWS Config 规则	指南
	通过 FIPS 140 认证，并使用符合 FIPS 140 要求的最新模块运行。必须在 SLA 中包含此要求。		器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.3.1 云计算 d. 传输中数据加密	FTI 在云环境内传输时必须加密。用于加密 FTI 的所有机制都必须通过 FIPS 140 认证，并使用符合 FIPS 140 要求的最新模块运行。必须在 SLA 中包含此要求。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
3.3.1 云计算 d. 传输中数据加密	FTI 在云环境内传输时必须加密。用于加密 FTI 的所有机制都必须通过 FIPS 140 认证，并使用符合 FIPS 140 要求的最新模块运行。必须在 SLA 中包含此要求。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.3.1 云计算 d. 传输中数据加密	FTI 在云环境内传输时必须加密。用于加密 FTI 的所有机制都必须通过 FIPS 140 认证，并使用符合 FIPS 140 要求的最新模块运行。必须在 SLA 中包含此要求。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 d. 传输中数据加密	FTI 在云环境内传输时必须加密。用于加密 FTI 的所有机制都必须通过 FIPS 140 认证，并使用符合 FIPS 140 要求的最新模块运行。必须在 SLA 中包含此要求。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
3.3.1 云计算 e. 静态数据加密	静态数据加密：必须使用最新的 FIPS 140 认证加密机制对云端静态数据进行加密。必须在 SLA 中包含此要求。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.3.1 云计算 k. 多重身份验证	当机构的云解决方案可从互联网访问时（即从机构的可信网络之外访问云解决方案），机构必须实施充分的多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 k. 多重身份验证	当机构的云解决方案可从互联网访问时（即从机构的可信网络之外访问云解决方案），机构必须实施充分的多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
3.3.1 云计算 k. 多重身份验证	当机构的云解决方案可从互联网访问时（即从机构的可信网络之外访问云解决方案），机构必须实施充分的多重身份验证。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
3.3.1 云计算 k. 多重身份验证	当机构的云解决方案可从互联网访问时（即从机构的可信网络之外访问云解决方案），机构必须实施充分的多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
3.3.1 云计算 i. 风险评估：	该机构必须对用于接收、处理、存储、访问、保护和/或传输 FTI 的所有信息系统的安全和隐私控制措施进行年度评估。	annual-risk-assessment-performed（流程检查）	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	netfw-policy-rule-group-associated	AWS Network Firewall 策略定义了您的防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来过滤数据包和流量，并定义默认流量处理方式。
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	waf-regional-webacl-not-empty	连接到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
3.3.6 网络边界和基础设施	机构必须在其整个系统架构中部署边界保护设备，包括路由器、防火墙、交换机和入侵检测系统，以保护 FTI 和 FTI 系统。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
AC-2 账户管理 (f)	根据代理账户管理程序的先决条件创建、启用、修改、禁用和删除账户；	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (f)	根据代理账户管理程序的先决条件创建、启用、修改、禁用和删除账户；	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
AC-2 账户管理 (f)	根据代理账户管理程序的先决条件创建、启用、修改、禁用和删除账户；	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-2 账户管理 (f)	根据代理账户管理程序的先决条件创建、启用、修改、禁用和删除账户；	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (f)	根据代理账户管理程序的先决条件创建、启用、修改、禁用和删除账户；	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC-2 账户管理 (g)	监控账户的使用情况	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC-2 账户管理 (g)	监控账户的使用情况	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (g)	监控账户的使用情况	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
AC-2 账户管理 (g)	监控账户的使用情况	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (g)	监控账户的使用情况	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AC-2 账户管理 (g)	监控账户的使用情况	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (g)	监控账户的使用情况	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (g)	监控账户的使用情况	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	secretsmanager-secret-periodic-rotation	此规则可确保 S AWS ecrets Manager 密钥启用定期轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。默认值为 90 天。
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC-2 账户管理 (j)	审查账户是否符合账户管理要求	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
(CE-1) 自动化系统账户管理	支持使用自动化机制管理系统账户。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
(CE-1) 自动化系统账户管理	支持使用自动化机制管理系统账户。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
(CE-1) 自动化系统账户管理	支持使用自动化机制管理系统账户。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
(CE-3)：禁用账户	在 120 天内禁用账户，前提是这些账户：a. 已过期；b. 不再与用户或个人关联；c. 违反组织政策；或 d. 非特权账户 120 天内处于非活动状态，特权账户 60 天内处于非活动状态	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
(CE-12) 账户异常使用监控	监控系统账户中是否存在机构定义的异常使用情况；并向机构定义的人员或角色报告系统账户的异常使用情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	opensearch-access-control-enabled	确保在您的亚马逊 OpenSearch 服务域上启用精细访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。

控制 ID	控制描述	AWS Config 规则	指南
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC-6 最低权限	采用最低权限原则，只允许用户（或代表用户行事的进程）具有完成分配的组织任务所必需的授权访问权限。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
AC-17：远程访问	针对允许的每种远程访问类型，制定并记录使用限制、配置/连接要求和实施指南；并在允许此类连接之前，对系统的每种远程访问类型进行授权。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
AT-1：认知和培训	为系统用户（包括经理、高级管理人员和承包商）提供安全和隐私知识培训	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
AU-2：审计事件	确定系统为支持审计功能而能够记录的事件类型	audit-log-policy-exists（流程检查）	制定并维护审计日志管理策略，以定义贵组织的日志记录要求。这包括但不限于审查和保留审计日志。
AU-16：跨组织审计日志记录	在跨组织边界传输审计信息时，采用机构定义的方法在外部组织之间协调机构定义的审计信息。	audit-log-policy-exists（流程检查）	制定并维护审计日志管理策略，以定义贵组织的日志记录要求。这包括但不限于审查和保留审计日志。

控制 ID	控制描述	AWS Config 规则	指南
CA-7：持续监控	制定系统级持续监控策略，并根据组织级持续监控策略实施持续监控：制定机构定义的监控指标；根据持续监控策略进行持续控制评估；根据持续监控策略对系统和组织定义的指标进行持续监控；对控制评估和监控产生的信息进行关联和分析；针对控制评估和监控信息分析结果采取应对行动；每年至少向机构定义的人员报告系统的安全和隐私状况。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CP-9：系统备份	a. 每周对系统文档（包括安全相关文档）中包含的用户级别信息进行备份；b. 每周对系统中包含的系统级别信息进行备份；c. 每周备份系统文档，包括与安全和隐私相关的文档；d. 保护备份信息的机密性、完整性和可用性。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
IA-2：识别和身份验证（组织用户）(CE-1) 特权账户的多重身份验证	为访问特权账户实施多重身份验证	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2：识别和身份验证（组织用户）(CE-1) 特权账户的多重身份验证	为访问特权账户实施多重身份验证	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA-2：识别和身份验证（组织用户）(CE-2) 非特权账户的多重身份验证	为访问非特权账户实施多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
IA-5：身份验证器管理：(CE-1) 基于密码的身份验证：用于基于密码的身份验证	强制执行以下构成和复杂度规则：1. 强制要求密码的最小长度为十四 (14) 个字符。2. 强制实施最低密码复杂度，使其包含数字、大写字母、小写字母和特殊字符的组合。3. 在选择使用新密码时，必须至少更改一 (1) 个字符。4. 仅存储和传输受加密保护的密码。5. 强制执行密码有效期限制：i. 最少一 (1) 天，最多 90 天。ii. 服务账户密码应在 366 天（含）内过期。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PM-5：系统清单	不断开发和更新组织系统的清单。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
PM-5：系统清单	不断开发和更新组织系统的清单。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
PM-5：系统清单	不断开发和更新组织系统的清单。	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
PM-5：系统清单	不断开发和更新组织系统的清单。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
RA-5：漏洞监控和扫描	在机构网络上安装新的信息系统之前，每三十 (30) 天监控和扫描一次系统和托管应用程序中的漏洞，以确认补救措施，以及在发现和报告可能影响系统的新漏洞时进行扫描	vuln-scans-performed（流程检查）	确保根据您的合规要求执行漏洞扫描。扫描节奏、使用的工具和结果的使用应由您的组织定义。

控制 ID	控制描述	AWS Config 规则	指南
SA-10：开发人员配置管理 (e.)	跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给 [分配：组织定义的人员]。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SA-10：开发人员配置管理 (e.)	跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给 [分配：组织定义的人员]。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
SA-10：开发人员配置管理 (e.)	跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给 [分配：组织定义的人员]。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
SA-10：开发人员配置管理 (a) (c.)	在系统、组件或服务设计、开发、实施、运行期间执行配置管理；仅对系统、组件或服务实施组织批准的更改；	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
SC-4：共享系统资源中的信息	防止通过共享系统资源进行未经授权和非预期的信息传输	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7：边界保护	监控和控制系统外部边界和系统内关键内部边界的通信；为与内部组织网络分开的可公开访问的系统组件实施子网；仅通过托管接口连接到外部网络或信息系统，这些接口由按照组织安全架构布置的边界保护设备组成。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-7：边界保护 (CE-9) 限制威胁性传出通信流量	检测并拒绝对外部系统构成威胁的传出通信流量；以及审计与被拒绝的通信相关的内部用户的身份。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SC-7：边界保护 (CE-9) 限制威胁性传出通信流量	检测并拒绝对外部系统构成威胁的传出通信流量；以及审计与被拒绝的通信相关的内部用户的身份。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC-7：边界保护 (CE-9) 限制威胁性传出通信流量	检测并拒绝对外部系统构成威胁的传出通信流量；以及审计与被拒绝的通信相关的内部用户的身份。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
SC-7：边界保护（由 IRS 定义）	各机构应在信任边界实施和管理边界保护（通常使用防火墙）。应监控每个信任边界，并控制跨越每个边界的通信。	netfw-policy-rule-group-associated	AWS Network Firewall 策略定义了您的防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来过滤数据包和流量，并定义默认流量处理方式。

控制 ID	控制描述	AWS Config 规则	指南
SC-7：边界保护（由 IRS 定义）	各机构应在信任边界实施和管理边界保护（通常使用防火墙）。应监控每个信任边界，并控制跨越每个边界的通信。	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。
SC-8：传输机密性和完整性 (CE-1) 加密保护	实施加密机制以防止未经授权的信息泄露并检测传输过程中信息的变化。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8：传输机密性和完整性 (CE-1) 加密保护	实施加密机制以防止未经授权的信息泄露并检测传输过程中信息的变化。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8：传输机密性和完整性 (CE-1) 加密保护	实施加密机制以防止未经授权的信息泄露并检测传输过程中信息的变化。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8：传输机密性和完整性 (CE-1) 加密保护	实施加密机制以防止未经授权的信息泄露并检测传输过程中信息的变化。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
SC-8：传输机密性和完整性 (CE-1) 加密保护	实施加密机制以防止未经授权的信息泄露并检测传输过程中信息的变化。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8：传输机密性和完整性 (CE-1) 加密保护	实施加密机制以防止未经授权的信息泄露并检测传输过程中信息的变化。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8：传输机密性和完整性 (CE-1) 加密保护	实施加密机制以防止未经授权的信息泄露并检测传输过程中信息的变化。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-12：加密密钥的建立和管理	在系统中使用加密技术时，机构必须根据以下密钥管理要求建立和管理加密密钥：NIST SP 800-57《密钥管理建议》，涉及密钥生成、分发、存储、访问和销毁。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
SC-12：加密密钥的建立和管理	在系统中使用加密技术时，机构必须根据以下密钥管理要求建立和管理加密密钥：NIST SP 800-57《密钥管理建议》，涉及密钥生成、分发、存储、访问和销毁。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13：加密保护	实施每种指定加密用途所需的以下加密类型：经过 FIPS-140 验证的最新加密机制；NIST 800-52；传输层安全性协议 (TLS) 实施的选择、配置和使用指南；传输中加密（有效载荷加密）。禁止使用 SHA-1 进行数字签名。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-23：会话真实性	保护通信会话的真实性。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SC-28：静态信息保护 (CE-1) 加密保护	实施加密机制，防止终端用户计算系统（即台式电脑、笔记本电脑、移动设备、便携式和可移动存储设备）非易失性存储中的静态 FTI 在未经授权的情况下被泄露和修改。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI-2：缺陷修复（IRS 定义）	该机构应确保在每天开机并连接到该机构的网络后，检查工作站（根据政策的定义，包括使用GFE工作站的远程连接），以确保已应用最新的机构批准的补丁，并确保在必要时应用任何缺失的补丁或新的补丁或不少于每24小时（不包括周末、节假日等）以其他方式检查一次	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SI-2：缺陷修复（IRS 定义）	该机构应确保在每天开机并连接到该机构的网络后，检查工作站（根据政策的定义，包括使用GFE工作站的远程连接），以确保已应用最新的机构批准的补丁，并确保在必要时应用任何缺失的补丁或新的补丁或不少于每24小时（不包括周末、节假日等）以其他方式检查一次	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI-2：缺陷修复（IRS 定义）	该机构应确保在每天开机并连接到该机构的网络后，检查工作站（根据政策的定义，包括使用GFE工作站的远程连接），以确保已应用最新的机构批准的补丁，并确保在必要时应用任何缺失的补丁或新的补丁或不少于每24小时（不包括周末、节假日等）以其他方式检查一次	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
SI-2：缺陷修复（IRS 定义）	该机构应确保在每天开机并连接到该机构的网络后，检查工作站（根据政策的定义，包括使用GFE工作站的远程连接），以确保已应用最新的机构批准的补丁，并确保在必要时应用任何缺失的补丁或新的补丁或不少于每24小时（不包括周末、节假日等）以其他方式检查一次	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。为了协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。

控制 ID	控制描述	AWS Config 规则	指南
SI-2：缺陷修复（IRS 定义）	该机构应确保在每天开机并连接到该机构的网络后，检查工作站（根据政策的定义，包括使用GFE工作站的远程连接），以确保已应用最新的机构批准的补丁，并确保在必要时应用任何缺失的补丁或新的补丁或不少于每24小时（不包括周末、节假日等）以其他方式检查一次	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
SI-2：缺陷修复（IRS 定义）	该机构应确保在每天开机并连接到该机构的网络后，检查工作站（根据政策的定义，包括使用GFE工作站的远程连接），以确保已应用最新的机构批准的补丁，并确保在必要时应用任何缺失的补丁或新的补丁或不少于每24小时（不包括周末、节假日等）以其他方式检查一次	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控	组织：a. 监视信息系统以便：1. 根据 [分配：组织定义的监控目标] 检测攻击和潜在攻击的指标；以及 2. 检测未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. 部署监控设备：1. 战略性地在信息系统内收集组织确定的基本信息；以及 2. 在系统内的临时位置跟踪组织感兴趣的特定类型的交易；d. 保护从入侵监控工具获得的信息免遭未经授权的访问、修改和删除；	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控	组织：a. 监视信息系统以便：1. 根据 [分配：组织定义的监控目标] 检测攻击和潜在攻击的指标；以及 2. 检测未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. 部署监控设备：1. 战略性地在信息系统内收集组织确定的基本信息；以及 2. 在系统内的临时位置跟踪组织感兴趣的特定类型的交易；d. 保护从入侵监控工具获得的信息免遭未经授权的访问、修改和删除；	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控	组织：a. 监视信息系统以便：1. 根据 [分配：组织定义的监控目标] 检测攻击和潜在攻击的指标；以及 2. 检测未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. 部署监控设备：1. 战略性地在信息系统内收集组织确定的基本信息；以及 2. 在系统内的临时位置跟踪组织感兴趣的特定类型的交易；d. 保护从入侵监控工具获得的信息免遭未经授权的访问、修改和删除；	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控	组织：a. 监视信息系统以便：1. 根据 [分配：组织定义的监控目标] 检测攻击和潜在攻击的指标；以及 2. 检测未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. 部署监控设备：1. 战略性地在信息系统内收集组织确定的基本信息；以及 2. 在系统内的临时位置跟踪组织感兴趣的特定类型的交易；d. 保护从入侵监控工具获得的信息免遭未经授权的访问、修改和删除；	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控	组织：a. 监视信息系统以便：1. 根据 [分配：组织定义的监控目标] 检测攻击和潜在攻击的指标；以及 2. 检测未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. 部署监控设备：1. 战略性地在信息系统内收集组织确定的基本信息；以及 2. 在系统内的临时位置跟踪组织感兴趣的特定类型的交易；d. 保护从入侵监控工具获得的信息免遭未经授权的访问、修改和删除；	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
SI-4：系统监控（IRS 定义）	所有互联网接入点/门户都应捕获入站和出站流量标头信息并并保留至少一年，但不包括经机构 CISO 批准的互联网“匿名”连接。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
SI-7：软件、固件和信息完整性	使用完整性验证工具来检测对以下软件、固件和信息的未经授权的更改：系统内核、驱动程序、固件（例如 BIOS、UEFI）、软件（例如操作系统、应用程序、中间件）和安全属性。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SI-7：软件、固件和信息完整性	使用完整性验证工具来检测对以下软件、固件和信息的未经授权的更改：系统内核、驱动程序、固件（例如 BIOS、UEFI）、软件（例如操作系统、应用程序、中间件）和安全属性。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
SI-7：软件、固件和信息完整性	使用完整性验证工具来检测对以下软件、固件和信息的未经授权的更改：系统内核、驱动程序、固件（例如 BIOS、UEFI）、软件（例如操作系统、应用程序、中间件）和安全属性。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	dynamodb-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 资源。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	ebs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	efs-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	rds-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 资源包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	s3-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
SI-12：信息管理和保留	根据适用的法律、行政令、指令、法规、政策、标准、指导方针和操作要求，管理和保留系统内的信息以及系统输出的信息。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

模板

该模板可在以下网址获得 GitHub：IRS 1075 最佳运营实践。

K-ISMS 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了韩国信息安全管理系统 (ISMS) 和 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个韩国 ISMS 控制相关。一个韩国 ISMS 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	AWS Config 规则	指南
1.2.1	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置

控制 ID	AWS Config 规则	指南
		以及有关您的环境的其他详细信息的基准。
1.2.1	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
2.1.3	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
2.1.3	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
2.3.3	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	AWS Config 规则	指南
2.3.3	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
2.5.1	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
2.5.1	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
2.5.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略

控制 ID	AWS Config 规则	指南
2.5.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
2.5.1	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
2.5.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
2.5.1	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
2.5.1	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
2.5.1	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
2.5.1	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	AWS Config 规则	指南
2.5.1	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
2.5.1	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
2.5.1	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	AWS Config 规则	指南
2.5.1	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2.5.3	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
2.5.3	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
2.5.3	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	AWS Config 规则	指南
2.5.4	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
2.5.5	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	AWS Config 规则	指南
2.5.5	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
2.5.5	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
2.6	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
2.6	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
2.6	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
2.6	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
2.6	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
2.6	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
2.6	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	AWS Config 规则	指南
2.6	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
2.6	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
2.6	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
2.6	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
2.6	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
2.6	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
2.6	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	AWS Config 规则	指南
2.6	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
2.6	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
2.6	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
2.6	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
2.6	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
2.6	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
2.6.6	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
2.6.6	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
2.6.6	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
2.6.6	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
2.6.6	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
2.6.6	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
2.6.6	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
2.6.6	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
2.6.6	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
2.6.6	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
2.6.6	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	AWS Config 规则	指南
2.6.6	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
2.6.7	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
2.7	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （ AWS 基础安全最佳实践值：90 ）。实际值应反映贵组织的策略。
2.7	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2.7	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.7	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
2.7	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
2.7	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
2.7	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	AWS Config 规则	指南
2.7	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2.7	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
2.7	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
2.7	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2.7	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
2.7	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.7	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
2.7	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2.7	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2.7	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
2.7	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.7	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2.7	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.7	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
2.7	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
2.7	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2.7	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
2.7	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.7.1	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	AWS Config 规则	指南
2.7.1	elb-predefined-security-policy-ssl-check	为了帮助保护传输中数据，请确保您的经典 Elastic Load Balancing SSL 侦听器使用预定义的安全策略。Elastic Load Balancing 将提供预定义的 SSL 协商配置，在客户端与您的负载均衡器之间建立连接时，这些配置用于进行 SSL 协商。SSL 协商配置提供了广泛的客户端兼容性，并使用高强度加密算法。此规则要求您为 SSL 侦听器设置预定义安全策略。默认的安全策略是：ELB SecurityPolicy-TLS-1-2-2017-0。实际值应反映贵组织的策略
2.7.2	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
2.7.2	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	AWS Config 规则	指南
2.8.5	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
2.8.5	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
2.8.6	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
2.8.6	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	AWS Config 规则	指南
2.9.1	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
2.9.1	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
2.9.1	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrai l 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	AWS Config 规则	指南
2.9.1	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
2.9.2	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	AWS Config 规则	指南
2.9.2	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
2.9.2	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
2.9.2	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
2.9.2	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
2.9.2	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
2.9.3	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	AWS Config 规则	指南
2.9.3	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
2.9.3	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2.9.3	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
2.9.3	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2.9.3	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
2.9.3	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
2.9.3	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	AWS Config 规则	指南
2.9.3	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
2.9.3	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2.9.3	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	AWS Config 规则	指南
2.9.3	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
2.9.3	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
2.9.3	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	AWS Config 规则	指南
2.9.3	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
2.9.3	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2.9.3	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
2.9.4	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
2.9.4	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
2.9.4	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
2.9.4	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
2.9.4	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	AWS Config 规则	指南
2.9.4	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
2.9.4	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
2.9.4	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
2.9.4	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
2.9.4	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
2.9.4	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
2.10.3	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
2.10.3	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
2.10.3	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。

控制 ID	AWS Config 规则	指南
2.10.3	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
2.10.3	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
2.10.5	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.10.5	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2.10.5	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.10.5	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
2.10.5	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.10.5	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2.10.5	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.10.5	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.10.8	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
2.10.8	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
2.11.2	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。
2.11.3	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
2.11.3	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	AWS Config 规则	指南
2.11.3	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
2.11.3	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
2.11.3	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	AWS Config 规则	指南
2.11.3	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
2.12	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
2.12	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	AWS Config 规则	指南
2.12	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2.12	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2.12	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
2.12	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
2.12	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
2.12	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
2.12	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	AWS Config 规则	指南
2.12	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2.12	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	AWS Config 规则	指南
2.12	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
2.12	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
2.12	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	AWS Config 规则	指南
2.12	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
2.12	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
2.12	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
2.12	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

模板

该模板可在以下网址获得 GitHub：K-ISMS 运营最佳实践。

负载平衡操作最佳实践

此一致性包包含基于内部 AWS负载平衡的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：负载平衡最佳操作实践。

日志记录操作最佳实践

此一致性包包含基于内部 AWS登录的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：日志操作最佳实践。

管理和治理服务操作最佳实践

此一致性包包含基于管理和治理服务的 AWS Config 规则。有关更多信息，请参阅上的 “管理和治理” AWS。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：管理和治理服务最佳运营实践。

MAS 第 655 号通知操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下是新加坡金融管理局 (MAS) 第 655 号通知 — 网络卫生与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 MAS 通知 655 — 网络卫生控制措施有关。一个 MAS 第 655 号通知 – 网络卫生控制可能与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	AWS Config 规则	指南
4.1	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
4.1	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认

控制 ID	AWS Config 规则	指南
		值：90）。实际值应反映贵组织的策略。
4.1	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
4.1	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
4.1	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	AWS Config 规则	指南
4.1	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
4.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
4.1	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
4.1	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
4.1	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
4.1	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
4.1	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
4.1	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
4.1	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
4.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
4.1	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
4.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
4.1	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
4.1	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	AWS Config 规则	指南
4.1	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
4.2	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
4.2	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
4.2	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
4.2	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
4.2	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
4.2	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	AWS Config 规则	指南
4.2	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
4.2	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
4.3	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
4.3	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector 、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
4.3	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
4.3	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	AWS Config 规则	指南
4.4	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
4.4	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
4.4	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
4.4	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
4.4	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。

控制 ID	AWS Config 规则	指南
4.4	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
4.4	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
4.4	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
4.4	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
4.4	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
4.4	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
4.4	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	AWS Config 规则	指南
4.4	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
4.4	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
4.4	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
4.4	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。

控制 ID	AWS Config 规则	指南
4.4	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。
4.4	waf-regional-webacl-not-empty	连接到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
4.4	netfw-policy-default-action-fragment-packets	AWS Network Firewall 策略定义了您的防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来过滤数据包和流量。默认为“通过”操作可能会允许意外流量。
4.4	netfw-policy-default-action-full-packets	AWS Network Firewall 策略定义了您的防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来过滤数据包和流量。默认为“通过”操作可能会允许意外流量。
4.4	netfw-policy-rule-group-associated	AWS Network Firewall 策略定义了您的防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来过滤数据包和流量，并定义默认流量处理方式。

控制 ID	AWS Config 规则	指南
4.4	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。
4.4	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
4.4	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
4.4	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
4.4	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
4.4	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	AWS Config 规则	指南
4.4	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
4.4	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
4.4	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
4.4	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	AWS Config 规则	指南
4.4	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
4.4	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
4.4	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
4.4	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	AWS Config 规则	指南
4.4	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
4.4	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
4.4	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
4.5	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
4.5	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
4.5	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
4.5	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
4.6	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
4.6	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
4.6	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
4.6	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
4.6	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
4.6	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

模板

该模板可在以下网址获得 GitHub：新加坡金融管理局655号通知的运营最佳实践。

MAS TRMG 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下是新加坡金融管理局 (MAS) 2021 年 1 月《技术风险管理指南》(TRMG) 与托管 AWS Config 规则之间的映射示例。每条 AWS Config 规则都适用于特定的 AWS 资源，并与一个或多个 MAS TRMG 控件相关。一个 MAS TRMG 2021 年 1 月控制可能与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	AWS Config 规则	指南
3.3.1	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
5.4.3	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据

控制 ID	AWS Config 规则	指南
		AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
5.4.3	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
6.1.1	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
6.1.2	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。 AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	AWS Config 规则	指南
6.1.4	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
6.1.4	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
6.1.4	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
6.2.1	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	AWS Config 规则	指南
6.3.1	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
6.4.5	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
6.4.5	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
6.4.5	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
6.4.5	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	AWS Config 规则	指南
6.4.5	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
6.4.5	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
6.4.5	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
6.4.5	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	AWS Config 规则	指南
6.4.5	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
6.4.5	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
6.4.5	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
6.4.5	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
6.4.6	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	AWS Config 规则	指南
6.4.6	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
6.4.6	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
6.4.6	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrai l 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	AWS Config 规则	指南
6.4.6	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
6.4.6	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
6.4.6	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
6.4.6	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
6.4.6	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
6.4.6	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
6.4.7	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
6.4.7	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
6.4.7	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
6.4.7	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
6.4.7	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
6.4.7	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
6.4.7	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	AWS Config 规则	指南
6.4.7	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
6.4.7	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
6.4.7	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
6.4.7	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
6.4.7	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
6.4.7	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
6.4.7	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
6.4.7	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
6.4.8	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	AWS Config 规则	指南
6.4.8	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
6.4.8	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
6.4.8	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
6.4.8	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	AWS Config 规则	指南
6.4.8	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
6.4.8	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	AWS Config 规则	指南
6.4.8	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
7.2.1	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
7.2.1	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
7.4.1	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
7.4.1	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
7.4.1	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
7.4.1	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	AWS Config 规则	指南
7.4.1	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
7.4.1	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
7.5.5	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	AWS Config 规则	指南
7.5.5	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.5.5	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
7.5.5	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
7.5.5	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
7.5.5	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
7.5.5	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
7.5.5	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
7.5.5	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
7.5.5	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
7.5.7	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	AWS Config 规则	指南
7.5.7	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
7.5.7	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
7.5.7	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
7.5.7	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
7.5.7	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
7.5.7	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
7.5.7	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	AWS Config 规则	指南
7.5.7	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
7.5.7	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
7.5.7	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	AWS Config 规则	指南
7.5.7	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
8.1.1	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
8.1.1	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	AWS Config 规则	指南
8.1.1	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
8.1.1	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
8.1.1	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
8.1.1	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	AWS Config 规则	指南
8.1.1	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
8.1.1	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	AWS Config 规则	指南
8.1.2	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
8.1.2	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
8.1.2	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	AWS Config 规则	指南
8.1.2	opensearch-data-node-fault-tolerance	为了实现高可用性和容错能力，Amazon OpenSearch OpenSearch 服务（服务）至少需要三个数据节点。部署具有至少三个数据节点的 OpenSearch 服务域可确保在节点出现故障时集群运行。
8.1.2	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
8.1.3	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	AWS Config 规则	指南
8.1.3	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
8.1.3	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
8.1.3	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
8.4.1	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	AWS Config 规则	指南
8.4.1	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.4.1	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
8.4.1	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.4.1	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	AWS Config 规则	指南
8.4.1	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.4.1	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.4.1	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	AWS Config 规则	指南
8.4.1	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
8.4.1	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
8.4.1	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
8.4.2	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	AWS Config 规则	指南
8.4.2	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.4.2	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
8.4.2	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.4.2	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	AWS Config 规则	指南
8.4.2	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.4.2	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
8.4.2	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
8.4.2	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
8.4.2	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
8.4.2	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	AWS Config 规则	指南
8.4.4	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
8.5.4	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
8.5.4	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	AWS Config 规则	指南
9.1.1	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
9.1.1	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
9.1.1	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	AWS Config 规则	指南
9.1.1	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
9.1.1	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
9.1.1	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
9.1.1	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
9.1.1	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
9.1.1	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
9.1.1	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
9.1.1	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
9.1.1	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
9.1.1	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
9.1.1	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
9.1.1	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
9.1.1	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
9.1.1	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
9.1.1	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
9.1.1	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	AWS Config 规则	指南
9.1.1	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
9.1.1	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
9.1.1	secretsmanager-secret-periodic-rotation	此规则可确保 S AWS ecrets Manager 密钥启用定期轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。默认值为 90 天。
9.1.1	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays （ Config 默认值：90 ）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
9.1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
9.1.2	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
9.1.2	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
9.1.2	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
9.1.2	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
9.1.2	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
9.1.3	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
9.1.3	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
9.1.3	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
9.1.3	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
9.1.3	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
9.1.3	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
9.1.3	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	AWS Config 规则	指南
9.1.3	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
9.1.3	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
9.1.3	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
9.1.3	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
9.1.3	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
9.1.3	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
9.1.3	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
9.1.3	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
9.1.3	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
9.1.3	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
9.1.3	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
9.1.4	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
9.1.5	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
9.1.5	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
9.1.5	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
9.1.5	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	AWS Config 规则	指南
9.1.6	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
9.1.7	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	AWS Config 规则	指南
9.1.7	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
9.1.7	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
9.1.7	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
9.1.7	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
9.1.7	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
9.2.1	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
9.2.1	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
9.2.1	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
9.2.1	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
9.2.1	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
9.2.1	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
9.2.1	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
9.2.1	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。

控制 ID	AWS Config 规则	指南
9.2.1	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
9.2.1	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
9.2.1	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector 、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
9.2.2	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
9.2.2	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
9.2.2	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
9.2.2	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
9.2.2	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrai l 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
9.2.2	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
9.2.2	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
9.2.2	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
9.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
9.2.2	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
9.2.2	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
9.3.1	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
9.3.1	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
9.3.1	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
9.3.1	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
9.3.1	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
9.3.1	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
9.3.1	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
9.3.1	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
9.3.1	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
9.3.1	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
9.3.1	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
9.3.1	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
9.3.1	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
9.3.1	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
9.3.1	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
10.1.1	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （ AWS 基础安全最佳实践值：90 ）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
10.1.1	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
10.1.1	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
10.1.1	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
10.1.1	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
10.1.1	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
10.1.1	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	AWS Config 规则	指南
10.1.1	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.1.1	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
10.1.1	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
10.1.1	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
10.1.1	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-n ode 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
10.1.1	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
10.1.1	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
10.1.1	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
10.1.1	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	AWS Config 规则	指南
10.1.1	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
10.1.1	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.1.1	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.1.1	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
10.1.1	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.1.1	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
10.1.1	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
10.1.1	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
10.1.1	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.1.1	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
10.1.1	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
10.1.1	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
10.1.1	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.2.1	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （ AWS 基础安全最佳实践值：90 ）。实际值应反映贵组织的策略。
10.2.1	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
10.2.1	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	AWS Config 规则	指南
10.2.2	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
10.2.3	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
10.2.3	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
10.2.3	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	AWS Config 规则	指南
11.1.1 (a)	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
11.1.1 (a)	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
11.1.1 (a)	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
11.1.1 (a)	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
11.1.1 (a)	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
11.1.1 (a)	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
11.1.1 (a)	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
11.1.1 (a)	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
11.1.1 (a)	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
11.1.1 (a)	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
11.1.1 (b)	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
11.1.1 (b)	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
11.1.1 (b)	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
11.1.1 (b)	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
11.1.1 (b)	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
11.1.1 (b)	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
11.1.1 (b)	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.1 (b)	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
11.1.1 (b)	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
11.1.1 (b)	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
11.1.1 (b)	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
11.1.1 (b)	opensearch-in-vpc-only	通过确保亚马逊 OpenSearc h 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
11.1.1 (b)	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
11.1.1 (b)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
11.1.1 (b)	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
11.1.1 (b)	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
11.1.1 (b)	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.1.1 (b)	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.1 (b)	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.1 (b)	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
11.1.1 (b)	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.1.1 (b)	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
11.1.1 (b)	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
11.1.1 (b)	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
11.1.1 (b)	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
11.1.1 (b)	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.1 (b)	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
11.1.1 (b)	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
11.1.1 (b)	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.1 (b)	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.1 (b)	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	AWS Config 规则	指南
11.1.1 (b)	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
11.1.3	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
11.1.3	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
11.1.3	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
11.1.3	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	AWS Config 规则	指南
11.1.3	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
11.1.3	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.3	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
11.1.3	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
11.1.3	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
11.1.3	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
11.1.3	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
11.1.3	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	AWS Config 规则	指南
11.1.3	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
11.1.3	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
11.1.3	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
11.1.3	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
11.1.3	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
11.1.3	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
11.1.3	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
11.1.3	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
11.1.3	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
11.1.3	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
11.1.3	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
11.1.3	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
11.1.3	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.3	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.3	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
11.1.3	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.3	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
11.1.3	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
11.1.3	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
11.1.3	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.1.3	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
11.1.3	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
11.1.3	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
11.1.3	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
11.2.1	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
11.2.2	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
11.2.2	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
11.2.2	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
11.2.2	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
11.2.2	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
11.2.2	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
11.2.2	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
11.2.2	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
11.2.2	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
11.2.2	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
11.2.2	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
11.2.2	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	AWS Config 规则	指南
11.2.2	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.2.2	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.2.2	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.2.2	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
11.2.2	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
11.2.2	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
11.2.2	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
11.2.2	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
11.2.2	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
11.2.2	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
11.2.2	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	AWS Config 规则	指南
11.2.2	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
11.2.4	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
11.2.4	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
11.2.4	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
11.2.4	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
11.2.4	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
11.2.4	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
11.2.4	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
11.2.4	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
11.2.4	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	AWS Config 规则	指南
11.2.4	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
11.2.4	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
11.2.4	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.2.4	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
11.2.4	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11.2.4	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
11.2.4	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
11.2.4	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
11.2.4	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
11.2.4	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
11.2.4	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	AWS Config 规则	指南
11.2.4	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
11.2.4	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
11.3.1	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	AWS Config 规则	指南
11.3.5	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
11.3.5	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
11.3.5	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
11.3.5	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
11.4.2	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
11.4.2	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
11.4.2	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
11.4.2	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
11.5.2	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
12.1.1	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
12.1.1	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
12.1.1	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
12.1.1	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
12.2.2	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
12.2.2	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
12.2.2	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	AWS Config 规则	指南
12.2.2	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
12.2.2	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
12.2.2	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
12.2.2	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	AWS Config 规则	指南
12.2.2	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
12.2.2	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
12.2.2	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
12.2.2	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
12.2.2	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
12.2.2	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	AWS Config 规则	指南
12.2.2	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
12.2.2	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
12.2.2	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
12.2.4	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
12.2.4	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
12.2.5	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
12.2.5	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
12.2.5	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	AWS Config 规则	指南
12.2.5	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
12.3.2	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
12.3.2	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
12.3.2	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	AWS Config 规则	指南
14.1.2	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
14.1.2	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
14.1.2	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
14.1.2	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
14.1.2	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
14.1.2	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
14.1.2	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
14.1.2	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
14.1.2	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
14.1.3	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
14.1.3	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
14.1.3	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
14.1.3	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
14.2.2	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
14.2.2	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
14.2.2	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
14.2.2	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
14.2.2	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
14.2.2	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
14.2.2	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
14.2.2	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
14.2.2	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
14.2.2	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
14.2.2	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	AWS Config 规则	指南
14.2.2	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
14.2.6	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
14.2.6	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
14.2.6	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	AWS Config 规则	指南
14.2.6	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
14.2.6	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
14.2.6	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
14.2.6	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	AWS Config 规则	指南
14.2.6	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

模板

该模板可在以下网址获得 GitHub：M AS TRMG 运营最佳实践。

监控操作最佳实践

此一致性包包含基于内部 AWS监控的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：最佳监控操作实践。

NBC TRMG 操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了柬埔寨国家银行 (NBC) 的《技术风险管理 (TRM) 指南》框架与 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 NBC TRM 指南相关。一个 NBC TRM 指南可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

此示例合规包模板包含与柬埔寨国家银行 (NBC) 的《技术风险管理 (TRM) 指南》框架内的控制措施的映射，可在此处访问该框架：柬埔寨国家银行：技术风险管理指南。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方

控制 ID	控制描述	AWS Config 规则	指南
	问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID		式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(d)	d) 需要考虑的重要控制措施包括：- 申请和授权创建用户 ID 和访问控制矩阵的系统流程 - 进行风险评估并根据风险评估授予访问权限。- 实施基于角色的访问控制，旨在确保有效的职责分离 - 更改系统的默认用户名和/或密码，禁止共享普通账户的用户 ID 和密码 - 在角色或职责发生变化时修改访问权限，在离职/合同终止时取消访问权限 - 及时通知信息安全职能部门有关用户添加、删除和角色变更的流程 - 定期核对系统中的用户 ID 和需要访问的实际用户，删除不必要的 ID（如有）- 审计、记录和监控所有用户访问 IT 资产的情况；以及 - 考虑停用长期休假的关键应用程序用户的用户 ID	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(f)	f) 出于问责目的，确保对用户和 IT 资产进行唯一标识，并确保他们的行为是可审计的。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
3.1.1(f)	f) 出于问责目的，确保对用户和 IT 资产进行唯一标识，并确保他们的行为是可审计的。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(f)	f) 出于问责目的，确保对用户和 IT 资产进行唯一标识，并确保他们的行为是可审计的。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
3.1.1(f)	f) 出于问责目的，确保对用户和 IT 资产进行唯一标识，并确保他们的行为是可审计的。	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
3.1.1(f)	f) 出于问责目的，确保对用户和 IT 资产进行唯一标识，并确保他们的行为是可审计的。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(f)	f) 出于问责目的，确保对用户和 IT 资产进行唯一标识，并确保他们的行为是可审计的。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
3.1.1(f)	f) 出于问责目的，确保对用户和 IT 资产进行唯一标识，并确保他们的行为是可审计的。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据“需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含“效果”：“允许”和“操作”：“*”而不是“资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		

控制 ID	控制描述	AWS Config 规则	指南
3.1.1(h)	h) 系统管理员、安全人员、程序员和执行关键操作的工作人员，由于其工作职能和特权访问权限，必然拥有对其维护或操作的金融系统造成严重破坏的能力。对拥有较高系统访问权限的人员应严加监管，并记录他们的所有系统活动，因为他们掌握内幕消息和资源，可以规避系统控制和安全程序。需要考虑下面列举的一些控制和安全实践：- 对特权用户实施双重验证 - 对特权用户的远程访问实施强有力的控制 - 限制特权用户的数量 - 根据 “需要拥有”或“需要执行”原则授予特权访问 - 对特权用户执行的系统活动保持审计日志记录 - 确保特权用户无法访问记录有其活动的系统日志 - 对日志进行定期审计或管理审查 - 禁止共享特权 ID 及其访问代码 - 禁止供应商和承包商在没有密切监督和监控的情况下获得系统访	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
	问特权 - 保护备份数据免遭未经授权的访问		
3.1.2(a)	a) BFI 应在其 IT 基础设施的关键节点安装网络安全设备，如防火墙、防病毒/防恶意软件以及入侵检测和防御系统，以保护网络外围。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
3.1.2(a)	a) BFI 应在其 IT 基础设施的关键节点安装网络安全设备，如防火墙、防病毒/防恶意软件以及入侵检测和防御系统，以保护网络外围。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(a)	a) BFI 应在其 IT 基础设施的关键节点安装网络安全设备，如防火墙、防病毒/防恶意软件以及入侵检测和防御系统，以保护网络外围。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则基于您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	[api-gw-execution-logging-enabled](#)	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(c)	c) 应实施控制措施，确保网络中信息的安全，并保护联网服务免遭未经授权的访问。特别是，应考虑以下各项：- 应制定管理网络设备的责任和程序 - 在适当情况下，网络的运营责任应与计算机操作分开 - 应制定特别的控制措施，来保障通过公共网络或无线网络传递的数据的保密性和完整性，并保护所连接的系统和应用程序（在连接到不受信任的系统/网络时，还包括网络加密协议）。- 应进行适当的记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作 - 应密切协调管理活动，以优化为组织提供的服务，并确保在整个信息处理基础设施中始终如一地实施控制措施 - 网络上的系统应经过身份验证 - 应限制不受信任的系统与网络的连接	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2(e)	e) 网络服务的范围可以从简单的非托管带宽到复杂的服务，例如 VPN、IP 语音、VSAT 等。网络服务的安全功能应是：- 用于确保网络服务安全的技术，例如身份验证、加密和网络连接控制 - 根据安全和网络连接规则与网络服务进行安全连接所需的技术参数，以及 - 必要时使用网络服务限制访问网络服务或应用程序的程序	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(e)	e) 使用加密来保护远程访问设备与机构之间的通信渠道，以限制与网络欺骗相关的风险。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
3.1.3(g)	g) 维护远程访问通信日志。日志应包括所有远程访问的日期、时间、用户、用户位置、持续时间和目的，包括通过远程访问进行的所有活动	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
3.1.3(i)	i) 对远程访问强制执行双因素身份验证流程（例如，带有一次性随机密码生成器的基于 PIN 的令牌卡，或基于令牌的 PKI）	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3(i)	i) 对远程访问强制执行双因素身份验证流程（例如，带有一次性随机密码生成器的基于 PIN 的令牌卡，或基于令牌的 PKI）	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
3.1.3(i)	i) 对远程访问强制执行双因素身份验证流程（例如，带有一次性随机密码生成器的基于 PIN 的令牌卡，或基于令牌的 PKI）	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
3.1.3(i)	i) 对远程访问强制执行双因素身份验证流程（例如，带有一次性随机密码生成器的基于 PIN 的令牌卡，或基于令牌的 PKI）	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
3.1.4(c)(e)	c) 补丁管理流程应包括以下方面：-确定获取和验证补丁的方法以确保补丁来自授权来源-识别适用于组织使用的应用程序和系统的漏洞-评估实施补丁（或不实施特定补丁）的业务影响-确保补丁经过测试-描述自动部署补丁的方法-报告整个组织的补丁部署状态以及-包括方法用于处理补丁部署失败（例如，补丁的重新部署）。e) BFI 应为所有可用且安全的自动补丁管理工具和软件更新工具的系统部署自动补丁管理工具和软件更新工具	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4(c)(e)	c) 补丁管理流程应包括以下方面：-确定获取和验证补丁的方法以确保补丁来自授权来源-识别适用于组织使用的应用程序和系统的漏洞-评估实施补丁（或不实施特定补丁）的业务影响-确保补丁经过测试-描述自动部署补丁的方法-报告整个组织的补丁部署状态以及-包括方法用于处理补丁部署失败（例如，补丁的重新部署）。e) BFI 应为所有可用且安全的自动补丁管理工具和软件更新工具的系统部署自动补丁管理工具和软件更新工具	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4(c)(e)	c) 补丁管理流程应包括以下方面：-确定获取和验证补丁的方法以确保补丁来自授权来源-识别适用于组织使用的应用程序和系统的漏洞-评估实施补丁（或不实施特定补丁）的业务影响-确保补丁经过测试-描述自动部署补丁的方法-报告整个组织的补丁部署状态以及-包括方法用于处理补丁部署失败（例如，补丁的重新部署）。e) BFI 应为所有可用且安全的自动补丁管理工具和软件更新工具的系统部署自动补丁管理工具和软件更新工具	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4(c)(e)	c) 补丁管理流程应包括以下方面：-确定获取和验证补丁的方法以确保补丁来自授权来源-识别适用于组织使用的应用程序和系统的漏洞-评估实施补丁（或不实施特定补丁）的业务影响-确保补丁经过测试-描述自动部署补丁的方法-报告整个组织的补丁部署状态以及-包括方法用于处理补丁部署失败（例如，补丁的重新部署）。e) BFI 应为所有可用且安全的自动补丁管理工具和软件更新工具的系统部署自动补丁管理工具和软件更新工具	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4(c)(e)	c) 补丁管理流程应包括以下方面：-确定获取和验证补丁的方法以确保补丁来自授权来源-识别适用于组织使用的应用程序和系统的漏洞-评估实施补丁（或不实施特定补丁）的业务影响-确保补丁经过测试-描述自动部署补丁的方法-报告整个组织的补丁部署状态以及-包括方法用于处理补丁部署失败（例如，补丁的重新部署）。e) BFI 应为所有可用且安全的自动补丁管理工具和软件更新工具的系统部署自动补丁管理工具和软件更新工具	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4(c)(e)	c) 补丁管理流程应包括以下方面：-确定获取和验证补丁的方法以确保补丁来自授权来源-识别适用于组织使用的应用程序和系统的漏洞-评估实施补丁（或不实施特定补丁）的业务影响-确保补丁经过测试-描述自动部署补丁的方法-报告整个组织的补丁部署状态以及-包括方法用于处理补丁部署失败（例如，补丁的重新部署）。e) BFI 应为所有可用且安全的自动补丁管理工具和软件更新工具的系统部署自动补丁管理工具和软件更新工具	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
3.1.5(d)(e)	d) 适当的密钥管理需要生成、存储、存档、检索、分发、停用和销毁加密密钥的安全流程 e) 应保护所有加密密钥免遭修改和丢失。此外，还需要保护密钥和私钥免遭未经授权的使用和泄露。用于生成、存储和存档密钥的设备应受到物理保护	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5(d)(e)	d) 适当的密钥管理需要生成、存储、存档、检索、分发、停用和销毁加密密钥的安全流程 e) 应保护所有加密密钥免遭修改和丢失。此外，还需要保护密钥和私钥免遭未经授权的使用和泄露。用于生成、存储和存档密钥的设备应受到物理保护	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
3.1.5(d)(e)	d) 适当的密钥管理需要生成、存储、存档、检索、分发、停用和销毁加密密钥的安全流程 e) 应保护所有加密密钥免遭修改和丢失。此外，还需要保护密钥和私钥免遭未经授权的使用和泄露。用于生成、存储和存档密钥的设备应受到物理保护	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
3.1.5(d)(e)	d) 适当的密钥管理需要生成、存储、存档、检索、分发、停用和销毁加密密钥的安全流程 e) 应保护所有加密密钥免遭修改和丢失。此外，还需要保护密钥和私钥免遭未经授权的使用和泄露。用于生成、存储和存档密钥的设备应受到物理保护	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5(f)	f) 密钥管理系统应基于一套商定的标准、程序和安全方法，用于：-为不同的加密系统和不同的应用程序生成密钥-颁发和获取公钥证书-向目标实体分发密钥，包括在收到密钥时应如何激活密钥-存储密钥，包括授权用户如何访问密钥-更改或更新密钥，包括何时应更改密钥以及如何更改的规则-处理泄露的密钥-撤销密钥包括如何按键应撤回或停用，例如当密钥被盗或用户离开组织时（在这种情况下，密钥也应存档）——恢复丢失或损坏的密钥——备份或存档密钥——销毁密钥以及——记录和审计与密钥管理相关的活动。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5(f)	f) 密钥管理系统应基于一套商定的标准、程序和安全方法，用于：-为不同的加密系统和不同的应用程序生成密钥-颁发和获取公钥证书-向目标实体分发密钥，包括在收到密钥时应如何激活密钥-存储密钥，包括授权用户如何访问密钥-更改或更新密钥，包括何时应更改密钥以及如何更改的规则-处理泄露的密钥-撤销密钥包括如何按键应撤回或停用，例如当密钥被盗或用户离开组织时（在这种情况下，密钥也应存档）——恢复丢失或损坏的密钥——备份或存档密钥——销毁密钥以及——记录和审计与密钥管理相关的活动。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5(f)	f) 密钥管理系统应基于一套商定的标准、程序和安全方法，用于：-为不同的加密系统和不同的应用程序生成密钥-颁发和获取公钥证书-向目标实体分发密钥，包括在收到密钥时应如何激活密钥-存储密钥，包括授权用户如何访问密钥-更改或更新密钥，包括何时应更改密钥以及如何更改的规则-处理泄露的密钥-撤销密钥包括如何按键应撤回或停用，例如当密钥被盗或用户离开组织时（在这种情况下，密钥也应存档）——恢复丢失或损坏的密钥——备份或存档密钥——销毁密钥以及——记录和审计与密钥管理相关的活动。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5(f)	f) 密钥管理系统应基于一套商定的标准、程序和安全方法，用于：-为不同的加密系统和不同的应用程序生成密钥-颁发和获取公钥证书-向目标实体分发密钥，包括在收到密钥时应如何激活密钥-存储密钥，包括授权用户如何访问密钥-更改或更新密钥，包括何时应更改密钥以及如何更改的规则-处理泄露的密钥-撤销密钥包括如何按键应撤回或停用，例如当密钥被盗或用户离开组织时（在这种情况下，密钥也应存档）——恢复丢失或损坏的密钥——备份或存档密钥——销毁密钥以及——记录和审计与密钥管理相关的活动。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5(f)	f) 密钥管理系统应基于一套商定的标准、程序和安全方法，用于：-为不同的加密系统和不同的应用程序生成密钥-颁发和获取公钥证书-向目标实体分发密钥，包括在收到密钥时应如何激活密钥-存储密钥，包括授权用户如何访问密钥-更改或更新密钥，包括何时应更改密钥以及如何更改的规则-处理泄露的密钥-撤销密钥包括如何按键应撤回或停用，例如当密钥被盗或用户离开组织时（在这种情况下，密钥也应存档）——恢复丢失或损坏的密钥——备份或存档密钥——销毁密钥以及——记录和审计与密钥管理相关的活动。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5(f)	f) 密钥管理系统应基于一套商定的标准、程序和安全方法，用于：-为不同的加密系统和不同的应用程序生成密钥-颁发和获取公钥证书-向目标实体分发密钥，包括在收到密钥时应如何激活密钥-存储密钥，包括授权用户如何访问密钥-更改或更新密钥，包括何时应更改密钥以及如何更改的规则-处理泄露的密钥-撤销密钥包括如何按键应撤回或停用，例如当密钥被盗或用户离开组织时（在这种情况下，密钥也应存档）——恢复丢失或损坏的密钥——备份或存档密钥——销毁密钥以及——记录和审计与密钥管理相关的活动。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5(f)	f) 密钥管理系统应基于一套商定的标准、程序和安全方法，用于：-为不同的加密系统和不同的应用程序生成密钥-颁发和获取公钥证书-向目标实体分发密钥，包括在收到密钥时应如何激活密钥-存储密钥，包括授权用户如何访问密钥-更改或更新密钥，包括何时应更改密钥以及如何更改的规则-处理泄露的密钥-撤销密钥包括如何按键应撤回或停用，例如当密钥被盗或用户离开组织时（在这种情况下，密钥也应存档）——恢复丢失或损坏的密钥——备份或存档密钥——销毁密钥以及——记录和审计与密钥管理相关的活动。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
3.1.6(a)	a) BFI 应部署自动化工具和手动技术的组合，定期进行全面的漏洞评估。对于基于 Web 的外部系统，漏洞评估的范围应包括常见的 Web 漏洞，例如 SQL 注入和跨站点脚本。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.1.6(a)	a) BFI 应部署自动化工具和手动技术的组合，定期进行全面的漏洞评估。对于基于 Web 的外部系统，漏洞评估的范围应包括常见的 Web 漏洞，例如 SQL 注入和跨站点脚本。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
3.1.6(a)	a) BFI 应部署自动化工具和手动技术的组合，定期进行全面的漏洞评估。对于基于 Web 的外部系统，漏洞评估的范围应包括常见的 Web 漏洞，例如 SQL 注入和跨站点脚本。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则基于您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
3.1.6(c)	c) BFI 应制定程序来补救漏洞评估和 PT 中发现的问题，并随后对补救措施进行重新验证，以验证差距是否已得到充分解决。	vuln-mitigated-accepted（流程检查）	确保新发现的漏洞得到补救或记录为可接受的风险。应根据贵组织的合规要求对漏洞进行补救或将其作为风险接受。
3.1.6(f)	f) 安全职能部门应定期向高级管理层提供有关每个部门/分部未缓解的严重漏洞数量的最新状态以及缓解计划	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
3.1.8	用户培训和意识	security-awareness-program-exists（流程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。

控制 ID	控制描述	AWS Config 规则	指南
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.1.10(b)	b) 系统文档、应用程序源代码和生产交易数据等敏感信息应有更广泛的控制措施以防篡改（例如，完整性检查器、加密哈希）。此外，政策应尽量减少敏感信息的分发，包括包含信息的打印件。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(h)	h) 为了最大限度地降低与变更相关的风险，BFI 应在变更之前对受影响的系统或应用程序进行备份。BFI 应制定回滚计划，以便在部署期间或部署之后遇到问题时恢复到系统或应用程序的先前版本。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
3.2.1(k)	k) 审计和安全日志是有用的信息，有助于调查和故障排除。BFI 应确保启用日志记录功能，以记录迁移过程中执行的活动。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
3.2.3(a)	a) 制定和实施预防、检测、分析和应对信息安全事件的流程。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.2.3(a)	a) 制定和实施预防、检测、分析和应对信息安全事件的流程。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
3.3.1(a)	a) 在系统设计中，考虑与保持高系统可用性、足够容量、可靠性能、快速响应时间和可扩展性相关的重要因素。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.4(a)(b)(c)(f)(j)	a) 确保对用户访问记录进行唯一地标识和记录，以便进行审计和审查。b) 对未经授权的访问进行问责和识别，并记录在案。c) 启用对特权用户执行的系统活动的审计日志记录。f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。j) 确保事件日志记录为自动监控系统奠定了基础，该系统能够生成有关系统安全的综合报告和警报。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.4(f)	f) 确保应用适当的日志记录和监控，以记录和检测可能影响信息安全或与信息安全相关的操作。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.4(g)	g) 确保事件日志在相关时包括：-用户 ID-系统活动-关键事件的日期、时间和详细信息，例如登录和注销-设备身份或位置（如果可能）和系统标识符-成功和拒绝的系统访问尝试的记录-成功和拒绝的数据和其他资源访问尝试的记录-系统配置的更改-权限的使用-系统实用程序和应用程序的使用-访问的文件和访问的类型-网络地址和协议-警报由门禁系统引起，而且-用户在应用程序和在线客户交易中执行的交易记录	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
3.6.1(a)(h)	a) BFI 需要确保为其 Web 应用程序采取适当的安全措施，并针对各种 Web 安全风险采取合理的缓解措施。h) BFI 需要确保为其 Web 应用程序采取适当的安全措施，并针对各种 Web 安全风险采取合理的缓解措施	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
3.6.1(a)(h)	a) BFI 需要确保为其 Web 应用程序采取适当的安全措施，并针对各种 Web 安全风险采取合理的缓解措施。h) BFI 需要确保为其 Web 应用程序采取适当的安全措施，并针对各种 Web 安全风险采取合理的缓解措施	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则基于您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
3.6.1(b)	b) BFI 需要评估与其网上银行系统和其他相关系统相关的安全要求，并根据所需的保密性和完整性程度采用加密解决方案。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
3.6.1(d)	d) 提供网上银行业务的 BFI 应对异常的网络流量状况/系统性能以及系统资源利用率的突然激增（这可能表明存在 DDoS 攻击）做出反应。因此，任何先发制人和被动反应行动的成功与否，都取决于是否部署了适当的工具来有效检测、监控和分析网络和系统中的异常情况。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
3.6.1(d)	d) 提供网上银行业务的 BFI 应对异常的网络流量状况/系统性能以及系统资源利用率的突然激增（这可能表明存在 DDoS 攻击）做出反应。因此，任何先发制人和被动反应行动的成功与否，都取决于是否部署了适当的工具来有效检测、监控和分析网络和系统中的异常情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.6.1(d)	d) 提供网上银行业务的 BFI 应对异常的网络流量状况/系统性能以及系统资源利用率的突然激增（这可能表明存在 DDoS 攻击）做出反应。因此，任何先发制人和被动反应行动的成功与否，都取决于是否部署了适当的工具来有效检测、监控和分析网络和系统中的异常情况。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.6.1(d)	d) 提供网上银行业务的 BFI 应对异常的网络流量状况/系统性能以及系统资源利用率的突然激增（这可能表明存在 DDoS 攻击）做出反应。因此，任何先发制人和被动反应行动的成功与否，都取决于是否部署了适当的工具来有效检测、监控和分析网络和系统中的异常情况。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
3.6.1(d)	d) 提供网上银行业务的 BFI 应对异常的网络流量状况/系统性能以及系统资源利用率的突然激增（这可能表明存在 DDoS 攻击）做出反应。因此，任何先发制人和被动反应行动的成功与否，都取决于是否部署了适当的工具来有效检测、监控和分析网络和系统中的异常情况。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则基于您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
3.6.1(e)	e) BFI 需要定期评估信息安全漏洞，评估现有 IT 安全风险管理框架的有效性，进行必要的调整，以确保及时解决新出现的漏洞。这种评估也应作为任何重大变更的一部分进行。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.6.4(a)(b)	a) 限制互联网访问并将关键系统与通用 IT 环境隔离开来。b) 减少攻击面和漏洞。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

模板

该模板可在以下网址获得 GitHub：NBC TRMG 运营最佳实践。

NERC CIP BCSI 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了北美电力可靠性公司的 BES 网络系统信息 (BCSI) 关键基础设施保护标准 (NERC CIP)、CIP-004-7 和 CIP-011-3 与托管规则之间的映射示例。 AWS Config 每条 AWS Config 规则都适用于特定 AWS 资源，并与一个或多个适用于 BCSI 的 NERC CIP 控制相关。一个 NERC CIP 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon 域名的最低权限访问。 OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 仪表板多租户，以及对和 Kibana 的 HTTP 基本身份验证。 OpenSearch

控制 ID	控制描述	AWS Config 规则	指南
	访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限		

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
CIP-004-7-R6-Part 6.1	每个责任实体均应实施一个或多个记录在案的访问管理计划，以授权、验证和撤销与 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中确定的“适用系统”有关的 BCSI 的预置访问权限，这些计划共同包括 CIP-004-7 表 R6“BES 网络系统信息的访问管理”中的每个适用要求部分。根据这一要求，个人必须同时具备获取和使用 BCSI 的能力，才能被视为能够访问 BCSI。预配置访问应被视为为向个人提供访问 BCSI 的途径而采取的具体措施的结果（例如，可能包括物理密钥或门禁卡、用户和相关的权限和权限、加密密钥）。第 6.1 部分：在配置之前，根据责任实体确定的需要进行授权（除非已根据第 4.1 部分授权），但“CIP 特殊情况：6.1.1”除外。提供对电子 BCSI 的电子访问权限	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	ecr-private-tag-immutability-enabled	启用 Elastic Container Repository (ECR) 标签不可变性，以防止 ECR 映像上的映像标签被覆盖。以前，标签可能会被覆盖，需要手动方法来唯一识别映像。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	s3-event-notifications-enabled	Amazon S3 事件通知可以提醒相关人员注意对您的存储桶对象的任何意外或故意修改。示例警报包括：创建了新对象、对象移除、对象恢复、丢失和复制的对象。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	s3-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	rds-cluster-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Relational Database Service (Amazon RDS) 数据库集群的攻击面。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	rds-instance-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Relational Database Service (Amazon RDS) 数据库实例的攻击面。

控制 ID	控制描述	AWS Config 规则	指南
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	redshift-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Redshift 集群的攻击面。
CIP-011-3-R1-Part 1.2	每个责任实体应实施一个或多个记录在案的信息保护计划，这些计划共同包括 CIP-011-3 表 R1“信息保护”中的每个适用要求部分。第 1.2 部分：保护和安全处理 BCSI 以降低泄密风险的方法。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。

模板

该模板可在以下网址获得 GitHub：NERC CIP BCSI 操作最佳实践。

NCSC 云安全原则操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保

遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了英国国家网络安全中心 (NCSC) 云安全原则和托管 C AWS onfig 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一项或多项英国 NCSC 云安全原则控制措施相关。一个英国 NCSC 云安全原则控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

此示例合规包模板包含英国 NCSC 云安全原则（国家网络安全中心 | 云安全指南）中控制的映射，此类公共部门信息根据开放式政府许可证 v3.0 获得许可。应在此处访问开放式政府许可证：公共部门信息的开放式政府许可证。

控制 ID	控制描述	AWS Config 规则	指南
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1. 传输中数据保护	应充分保护通过网络传输的用户数据免遭篡改和窃听。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保为您的 Amazon S OpenSearch ervice 域启用加密。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
2. 资产保护和复原力	您的数据（以及存储或处理数据的资产）应得到充分保护。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
5. 运营安全	必须以阻碍、检测或防止攻击的方式运营和管理服务。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
7. 安全开发	云服务的设计、开发和部署应最大限度地减少和缓解其安全威胁。	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。

控制 ID	控制描述	AWS Config 规则	指南
7. 安全开发	云服务的设计、开发和部署应最大限度地减少和缓解其安全威胁。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
7. 安全开发	云服务的设计、开发和部署应最大限度地减少和缓解其安全威胁。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
9. 安全的用户管理	提供商应提供工具，以安全地管理您对其服务的使用。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	rds-instance-iam-authentication-enabled	确保在亚马逊关系数据库服务 (Amazon RDS) 实例上启用 AWS 身份和访问管理 (IAM) 身份验证，以控制对系统和资产的访问。这会强制进出数据库的网络流量使用安全套接字层 (SSL) 进行加密。您无需将用户凭证存储在数据库中，因为身份验证在外部进行管理。

控制 ID	控制描述	AWS Config 规则	指南
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
10. 身份和身份验证	访问服务接口的权限应仅限于经过身份验证和授权的个人。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	ecs-container-insights-enabled	监控是维护 Amazon 弹性容器服务 (ECS) 和您的 AWS 解决方案的可靠性、可用性和性能的重要组成部分。Container Insights 还提供诊断信息（如容器重新启动失败），以帮助您查明问题并快速解决问题。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
11. 外部接口保护	应识别和防御服务的所有外部接口或不太可信的接口。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
12. 安全的服务管理	云提供商应认识到管理系统的高价值。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
13. 为用户提供的审计信息	提供商应提供监控服务访问权限所需的日志，以及其中保存的数据。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
13. 为用户提供的审计信息	提供商应提供监控服务访问权限所需的日志，以及其中保存的数据。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
13. 为用户提供的审计信息	提供商应提供监控服务访问权限所需的日志，以及其中保存的数据。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
13. 为用户提供的审计信息	提供商应提供监控服务访问权限所需的日志，以及其中保存的数据。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

模板

该模板可在以下网址获得 GitHub：NCSC 云安全原则最佳运营实践。

NCSC 网络评估框架操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保

遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了英国国家网络安全中心 (NCSC) 网络评估框架 (CAF) 控制和托管 C AWS onfig 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个英国 NCSC CAF 控件相关。一个英国 NCSC CAF 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

此示例合规包模板包含与英国 NCSC CAF（国家网络安全中心 | NCSC CAF 指南）内部控制的映射，此类公共部门信息根据开放政府许可证 v3.0 获得许可。应在此处访问开放式政府许可证：公共部门信息的开放式政府许可证。

控制 ID	控制描述	AWS Config 规则	指南
A3.a 资产管理	确定并了解交付、维护或支持基本功能运行所需的网络和信息系统所需的一切。这包括数据、人员和系统，以及任何支持性基础设施（例如电源或冷却）。	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
A3.a 资产管理	确定并了解交付、维护或支持基本功能运行所需的网络和信息系统所需的一切。这包括数据、人员和系统，以及任何支持性基础设施（例如电源或冷却）。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
A3.a 资产管理	确定并了解交付、维护或支持基本功能运行所需的网络和信息系统所需的一切。这包括数据、人员和系统，以及任何支持性基础设施（例如电源或冷却）。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
A3.a 资产管理	确定并了解交付、维护或支持基本功能运行所需的网络和信息系统所需的一切。这包括数据、人员和系统，以及任何支持性基础设施（例如电源或冷却）。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
A3.a 资产管理	确定并了解交付、维护或支持基本功能运行所需的网络和信息系统所需的一切。这包括数据、人员和系统，以及任何支持性基础设施（例如电源或冷却）。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。

控制 ID	控制描述	AWS Config 规则	指南
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	opensearch-access-control-enabled	确保在您的亚马逊 OpenSearch 服务域上启用精细访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch

控制 ID	控制描述	AWS Config 规则	指南
B2.a 身份核实、验证和授权	您严格核实、验证和授权访问支持您的基本功能的网络和信息系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
B2.b 设备管理	您完全了解并信任用于访问您的网络、信息系统和支持您的基本功能的数据的设备。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
B2.b 设备管理	您完全了解并信任用于访问您的网络、信息系统和支持您的基本功能的数据的设备。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays（Config 默认值：90）。实际值应反映贵组织的策略。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
B2.c 特权用户管理	您可以严格管理特权用户对支持基本功能的网络和信息系统的访问。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
B2.d#Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
B2.d Identity and Access Management (IdAM)	您可以确保对支持基本功能的网络和信息系统的身份和访问控制进行良好的管理和维护。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
B3.a 了解数据	您非常了解对基本功能的运行至关重要的数据、数据的存储位置、数据的传输位置，以及数据不可用或未经授权的访问、修改或删除将如何对基本功能产生不利影响。这也适用于存储或访问对基本功能运行非常重要的数据的第三方。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
B3.b 传输中数据	您已经保护了对基本功能的运行至关重要的数据的传输。这包括向第三方传输数据。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
B3.c 存储的数据	您已经保护了对基本功能的运行至关重要的存储数据。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
B4.a 从设计上确保安全	您在网络和信息系统中设计安全性，以支持基本功能的运行。您可以最大限度地减少他们的攻击面，并确保基本功能的运行不会受到任何单个漏洞利用的影响。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
B4.b 安全配置	您可以安全地配置支持基本功能运行的网络和信息系统。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
B4.b 安全配置	您可以安全地配置支持基本功能运行的网络和信息系统。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
B4.b 安全配置	您可以安全地配置支持基本功能运行的网络和信息系统。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
B4.b 安全配置	您可以安全地配置支持基本功能运行的网络和信息系统。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
B4.c#安全管理	您管理组织的网络和信息系统，这些系统支持基本功能的运行，以实现和维护安全。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
B4.c#安全管理	您管理组织的网络和信息系统，这些系统支持基本功能的运行，以实现和维护安全。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
B4.c#安全管理	您管理组织的网络和信息系统，这些系统支持基本功能的运行，以实现和维护安全。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
B4.d. 漏洞管理	您管理网络和信息系统中的已知漏洞，以防止对基本功能产生不利影响。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
B4.d. 漏洞管理	您管理网络和信息系统中的已知漏洞，以防止对基本功能产生不利影响。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
B4.d. 漏洞管理	您管理网络和信息系统中的已知漏洞，以防止对基本功能产生不利影响。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
B4.d. 漏洞管理	您管理网络和信息系统中的已知漏洞，以防止对基本功能产生不利影响。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
B4.d. 漏洞管理	您管理网络和信息系统中的已知漏洞，以防止对基本功能产生不利影响。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
B4.d. 漏洞管理	您管理网络和信息系统中的已知漏洞，以防止对基本功能产生不利影响。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
B5.b 复原力设计	您要设计支持基本职能的网络和信息系统，使其能够抵御网络安全事件。系统经过适当隔离，资源限制得到缓解。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
B5.b 复原力设计	您要设计支持基本职能的网络和信息系统，使其能够抵御网络安全事件。系统经过适当隔离，资源限制得到缓解。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
B5.b 复原力设计	您要设计支持基本职能的网络和信息系统，使其能够抵御网络安全事件。系统经过适当隔离，资源限制得到缓解。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
B5.c 备份	您拥有恢复基本功能运行所需的数据和信息的可访问和安全的当前备份	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。

控制 ID	控制描述	AWS Config 规则	指南
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
C1.a 监控覆盖范围	您在监控中包含的数据源可以及时识别可能影响基本功能运行的安全事件。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
C1.b 保护日志	您可以安全地保存日志数据，并且仅向有业务需求的账户授予读取权限。在约定的保留期限内，任何员工都不得修改或删除日志数据，保留期后应予以删除。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	s3-event-notifications-enabled	Amazon S3 事件通知可以提醒相关人员注意对您的存储桶对象的任何意外或故意修改。示例警报包括：创建了新对象、对象移除、对象恢复、丢失和复制的对象。

控制 ID	控制描述	AWS Config 规则	指南
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	cw-loggroup-retent ion-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
C1.c 生成警报	可以可靠地识别监控数据中包含的潜在安全事件的证据，并触发警报。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
C1.d 识别安全事件	您可以根据对威胁和系统的了解来对警报进行情境化，以识别那些需要某种形式响应的安全事件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
C1.d 识别安全事件	您可以根据对威胁和系统的了解来对警报进行情境化，以识别那些需要某种形式响应的安全事件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
C1.e 监控工具和技能	监控人员的技能、工具和角色，包括任何外包的技能、工具和角色，应反映治理和报告要求、预期威胁以及他们需要使用的网络或系统数据的复杂性。监控人员了解他们需要保护的基本功能。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
C1.e 监控工具和技能	监控人员的技能、工具和角色，包括任何外包的技能、工具和角色，应反映治理和报告要求、预期威胁以及他们需要使用的网络或系统数据的复杂性。监控人员了解他们需要保护的基本功能。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
C1.e 监控工具和技能	监控人员的技能、工具和角色，包括任何外包的技能、工具和角色，应反映治理和报告要求、预期威胁以及他们需要使用的网络或系统数据的复杂性。监控人员了解他们需要保护的基本功能。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
C2.a 用于攻击检测的系统异常	您可以定义系统行为异常的示例，这些示例提供了检测原本难以识别的恶意活动的实用方法。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
C2.a 用于攻击检测的系统异常	您可以定义系统行为异常的示例，这些示例提供了检测原本难以识别的恶意活动的实用方法。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
D1.c 测试和演习	贵组织使用过去影响您（和其他）组织的事件，并根据威胁情报和风险评估情景，开展演习以测试响应计划。	response-plan-exists-maintained （流程检查）	确保制定和维护事件响应计划，并将其分发给负责人。更新并正式记录响应计划，有助于确保响应人员了解自己的角色、责任以及在事件发生时应遵循的流程。
D1.c 测试和演习	贵组织使用过去影响您（和其他）组织的事件，并根据威胁情报和风险评估情景，开展演习以测试响应计划。	response-plan-tested （流程检查）	确保对事件响应和恢复计划进行测试。这有助于了解您的计划在事件期间是否有效，以及是否需要弥补任何不足或进行更新。

模板

该模板可在以下网址获得 GitHub：NCSC 网络评估框架的运营最佳实践。

联网和内容交付服务操作最佳实践

此一致性包包含基于网络和内容分发服务的 AWS Config 规则。有关更多信息，请参阅上的 “联网和内容交付” AWS。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：网络和内容分发服务的运营最佳实践。

NIST 800-53 rev 4 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了 NIST 800-53 和托管 C AWS onfig 规则之间的映射示例。每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个 NIST 800-53 控件相关。一个 NIST 800-53 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

该合规包已通过 AWS 安全保障服务有限责任公司（AWS SAS）的验证，该公司由支付卡行业合格安全评估员（QSA）、HITRUST认证的通用安全框架从业人员（CCSFP）和经过认证的合规专业人员组成，可以为各种行业框架提供指导和评估。 AWS SAS 专业人员设计此一致性包是为了让客户能够与 NIST 800-53 的子集保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	secretsmanager-scheduled-rotation-success-检查	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-user-group-membership-检查	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可

控制 ID	控制描述	AWS Config 规则	指南
			能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了NIST SP 800-63 和互联网安全中心 (CIS) AWS 基金会基准对密码强度的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政

控制 ID	控制描述	AWS Config 规则	指南
			策。实际值应反映贵组织的策略。
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	iam-user-unused-credentials-检查	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-2(1)	组织采用自动化机制来支持信息系统账户的管理。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(3)	在 [分配：组织定义的时间段] 之后，信息系统会自动禁用非活动账户。	iam-user-unused-credentials-检查	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有日志文件传送 AWS 区域 到你的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	信息系统会自动审计账户的创建、修改、启用、禁用和删除操作，并通知 [分配：组织定义的人员或角色]。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(12)(a)	组织：a. 监控 [分配：组织定义的非典型用途] 的信息系统账户。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
AC-2(12)(a)	组织：a. 监控 [分配：组织定义的非典型用途] 的信息系统账户。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-user-unused-credentials-检查	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了NIST SP 800-63 和互联网安全中心 (CIS) AWS 基金会基准对密码强度的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政

控制 ID	控制描述	AWS Config 规则	指南
			策。实际值应反映贵组织的策略。
AC-2(f)	组织：f. 根据 [分配：组织定义的程序或条件] 创建、启用、修改、禁用和删除信息系统账户。	iam-root-access-key-检查	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户 信息、IP 地址和事件时间。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AC-2(g)	组织：g. 监控信息系统账户的使用情况。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	secretsmanager-scheduled-rotation-success-检查	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-user-group-membership-检查	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了NIST SP 800-63 和互联网安全中心 (CIS) AWS 基金会基准对密码强度的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政

控制 ID	控制描述	AWS Config 规则	指南
			策。实际值应反映贵组织的策略。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-root-access-key-检查	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-group-has-users-检查	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(j)	组织：j. [分配：组织定义的频率]审查账户是否符合账户管理要求。	iam-user-no-policies-检查	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-user-no-policies-检查	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-user-unused-cr edentials-检查	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCreden tialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	lambda-function-pu blic-access-禁止	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	redshift-cluster-public-access-检查	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-user-group-membership-检查	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	s3-account-level-public-access-blocks	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-root-access-key-检查	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	ebs-snapshot-public-restorable-检查	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-group-has-users-检查	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-3	信息系统根据适用的访问控制策略，对信息和系统资源的逻辑访问强制实施经批准的授权。	sagemaker-notebook-no-direct-互联网接入	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	lambda-function-public-access-禁止	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	redshift-cluster-public-access-检查	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	rds-instance-public-access-检查	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	s3-account-level-public-access-blocks	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	sagemaker-notebook-no-direct-互联网接入	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	vpc-default-security-group-已关闭	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	ebs-snapshot-public-restorable-检查	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4	信息系统根据 [分配：组织定义的信息流控制策略] 强制执行经批准的授权，以控制系统内部和互连系统之间的信息流。	internet-gateway-authorized-vpc-只有	确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），从而管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-group-has-users-检查	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-5c	组织：c. 定义信息系统访问授权，以支持职责分离。	iam-user-no-policies-检查	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	rds-instance-public-access-检查	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	redshift-cluster-public-access-检查	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	s3-account-level-public-access-blocks	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	sagemaker-notebook-no-direct-互联网接入	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	lambda-function-public-access-禁止	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	codebuild-project-envvar-awscred-检查	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	ebs-snapshot-public-restorable-检查	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-user-unused-credentials-检查	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-group-has-users-检查	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-root-access-key-检查	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-user-group-membership-检查	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-user-no-policies-检查	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC-6	组织采用最低权限原则，只允许用户（或代表用户行事的进程）进行授权访问，这是根据组织使命和业务职能完成分配的任务所必需的。	iam-no-inline-policy-检查	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(10)	信息系统可防止非特权用户执行特权功能，包括禁用、规避或更改已实施的安全保障措施/对策。	iam-root-access-key-检查	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-17(1)	信息系统监视和控制远程访问方法。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AC-17(1)	信息系统监视和控制远程访问方法。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	alb-http-to-https-重定向检查	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	alb-http-drop-invalid-已启用标题	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17(2)	信息系统采用加密机制来保护远程访问会话的机密性和完整性。	elb-tls-https-listeners-只有	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17(3)	信息系统通过 [分配：组织定义的数字] 个托管网络访问控制点路由所有远程访问。	internet-gateway-authorized-vpc-只有	确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），从而管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	ebs-snapshot-public-restorable-检查	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	lambda-function-public-access-禁止	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	rds-instance-public-access-检查	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	redshift-cluster-public-access-检查	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	s3-account-level-public-access-blocks	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-21(b)	组织：b. 采用 [分配：组织定义的自动化机制或手动流程] 来帮助用户做出信息共享/协作决策。	sagemaker-notebook-no-direct-互联网接入	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	api-gw-execution-logging-已启用	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户 信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有日志文件传送 AWS 区域 到你的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU-2(a)(d)	组织：a. 确定信息系统是否能够审计以下事件：[分配：组织定义的可审计事件]；d. 确定要在信息系统中审计以下事件：[分配：组织定义的已审计事件（AU-2 a. 中定义的可审计事件的子集）以及每个已识别事件的审计频率（或需要审计的情况）]。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	api-gw-execution-logging-已启用	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户 信息、IP 地址和事件时间。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有日志文件传送 AWS 区域 到你的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
AU-3	信息系统生成审计记录，其中包含以下信息：事件类型、事件发生时间、事件发生地点、事件来源、事件结果以及与该事件相关的任何个人或主体的身份。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU-6(1)(3)	(1) 组织采用自动化机制来整合审计审查、分析和报告流程，以支持组织调查和应对可疑活动的程序。(3) 组织对不同存储库的审计记录进行分析和关联，以获得整个组织的态势感知。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU-7(1)	信息系统提供了根据 [分配：审计记录中组织定义的审计字段] 处理相关事件的审计记录的功能。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU-7(1)	信息系统提供了根据 [分配：审计记录中组织定义的审计字段] 处理相关事件的审计记录的功能。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-9	信息系统保护审计信息和审计工具免遭未经授权的访问、修改和删除。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
AU-9	信息系统保护审计信息和审计工具免遭未经授权的访问、修改和删除。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
AU-9(2)	信息系统将审计记录 [分配：组织定义的频率] 备份到与被审计的系统或组件实际不同的系统或系统组件。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
AU-11	该组织保留 [任务：符合记录保留政策的组织定义的时间段] 的审计记录，以为安全事件的 after-the-fact 调查提供支持并满足监管和组织信息保留要求。	cw-loggroup-retention-period-检查	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	api-gw-execution-logging-已启用	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户 信息、IP 地址和事件时间。
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有日志文件传送 AWS 区域 到你的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-12(a)(c)	信息系统：a. 在 [分配：组织定义的信息系统组件] 中为 AU-2 中定义的可审计事件提供审计记录生成功能；c. 为 AU-2 d. 中定义的事件生成审计记录，内容在 AU-3 中定义。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
CA-7(a)(b)	组织制定持续监控策略并实施持续监控计划，其中包括：a. 建立要监控的 [分配：组织定义的指标]；b. 建立监控 [分配：组织定义的频率] 和用于支持此类监控的评估 [分配：组织定义的频率]。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CM-2	组织在配置控制下开发、记录和维护信息系统的当前基线配置。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
CM-7(a)	组织：a. 将信息系统配置为仅提供基本功能。	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-7(a)	组织：a. 将信息系统配置为仅提供基本功能。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM-8(1)	组织更新信息系统组件清单，作为组件安装、拆除和信息系统更新的组成部分。	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-8(3)(a)	组织：a. 采用自动化机制 [分配：组织定义的频率] 来检测信息系统中是否存在未经授权的硬件、软件和固件组件	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM-8(3)(a)	组织：a. 采用自动化机制 [分配：组织定义的频率] 来检测信息系统中是否存在未经授权的硬件、软件和固件组件	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM-8(3)(a)	组织：a. 采用自动化机制 [分配：组织定义的频率] 来检测信息系统中是否存在未经授权的硬件、软件和固件组件	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份 [分配：与恢复时间和恢复点目标一致的组织定义的频率]。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份 [分配：与恢复时间和恢复点目标一致的组织定义的频率]。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份 [分配：与恢复时间和恢复点目标一致的组织定义的频率]。	elasticache-redis-cluster-automatic-备份检查	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份 [分配：与恢复时间和恢复点目标一致的组织定义的频率]。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份 [分配：与恢复时间和恢复点目标一致的组织定义的频率]。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份 [分配：与恢复时间和恢复点目标一致的组织定义的频率]。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份 [分配：与恢复时间和恢复点目标一致的组织定义的频率]。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9(b)	组织：b. 对信息系统中包含的系统级信息进行备份 [分配：与恢复时间和恢复点目标一致的组织定义的频率]。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	elasticache-redis-cluster-automatic-备份检查	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	elb-cross-zone-load-启用平衡	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CP-10	组织规定在发生中断、泄露或故障后恢复和重建信息系统，使其恢复到已知状态。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
IA-2	信息系统对组织用户（或代表组织用户行事的进程）进行唯一标识和身份验证。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了NIST SP 800-63 和互联网安全中心 (CIS) AWS 基金会基准对密码强度的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政

控制 ID	控制描述	AWS Config 规则	指南
			策。实际值应反映贵组织的策略。
IA-2(1)(11)	(1) 信息系统对特权账户的网络访问实施多重身份验证。(11) 信息系统为特权和非特权账户的远程访问实施多重身份验证，其中一个因素由独立于访问系统的设备提供，且该设备符合 [分配：组织定义的机制强度要求]。	root-account-hardware-mfa-已启用	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2(1)(11)	(1) 信息系统对特权账户的网络访问实施多重身份验证。(11) 信息系统为特权和非特权账户的远程访问实施多重身份验证，其中一个因素由独立于访问系统的设备提供，且该设备符合 [分配：组织定义的机制强度要求]。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA-2(1)(2)(11)	(1) 信息系统对特权账户的网络访问实施多重身份验证。(2) 信息系统对非特权账户的网络访问实施多重身份验证。(11) 信息系统为特权和非特权账户的远程访问实施多重身份验证，其中一个因素由独立于访问系统的设备提供，且该设备符合 [分配：组织定义的机制强度要求]。	mfa-enabled-for-iam-控制台访问权限	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA-2(1)(2)(11)	(1) 信息系统对特权账户的网络访问实施多重身份验证。(2) 信息系统对非特权账户的网络访问实施多重身份验证。(11) 信息系统为特权和非特权账户的远程访问实施多重身份验证，其中一个因素由独立于访问系统的设备提供，且该设备符合 [分配：组织定义的机制强度要求]。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
IA-5(1)(a)(d)(e)	对于基于密码的身份验证，信息系统：a. 强制执行最低密码复杂度 [分配：组织定义的区分大小写、字符数、混合使用大写字母、小写字母、数字和特殊字符的要求，包括每种类型字符的最低数量要求]；d. 强制执行 [分配：组织定义的最短和最长使用期限] 的密码最短和最长使用期限限制；e. 禁止重复使用 [分配：组织定义的数字] 代以内的密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了NIST SP 800-63 和互联网安全中心 (CIS) AWS 基金会基准对密码强度的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政

控制 ID	控制描述	AWS Config 规则	指南
			策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA-5(4)	组织使用自动化工具来确定密码身份验证器是否足够强大，可以满足 [分配：组织定义的要求]。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了NIST SP 800-63 和互联网安全中心 (CIS) AWS 基金会基准对密码强度的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政

控制 ID	控制描述	AWS Config 规则	指南
			策。实际值应反映贵组织的策略。
IA-5(7)	组织确保未加密的静态身份验证器不会嵌入应用程序或访问脚本中，也不会存储在功能密钥上。	codebuild-project-envvar-awscred-检查	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
IR-4(1)	组织采用自动化机制来支持事件处理流程。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
IR-4(1)	组织采用自动化机制来支持事件处理流程。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
IR-6(1)	组织采用自动化机制来协助报告安全事件。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
IR-7(1)	组织采用自动化机制来提高与事件响应相关的信息和支持的可用性。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
RA-5	组织：a. 扫描信息系统和托管应用程序中的漏洞 [分配：组织定义的频率和/或根据组织定义的流程随机进行]，以及在发现和报告可能影响系统/应用程序的新漏洞时进行扫描；b. 采用漏洞扫描工具和技术，通过使用以下标准来促进工具之间的互操作性，并实现漏洞管理过程的自动化：1. 枚举平台、软件缺陷和不当配置；2. 设置清单和测试程序格式；以及 3. 衡量漏洞的影响；c. 分析漏洞扫描报告和安全控制评估结果；d. 根据组织的风险评估，修复合法漏洞 [分配：组织定义的响应时间]；以及 e. 与 [分配：组织定义的人员或角色] 共享从漏洞扫描过程和安全控制评估中获得的信息，以帮助消除其他信息系统中的类似漏洞（即系统薄弱环节或缺陷）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
RA-5	组织：a. 扫描信息系统和托管应用程序中的漏洞 [分配：组织定义的频率和/或根据组织定义的流程随机进行]，以及在发现和报告可能影响系统/应用程序的新漏洞时进行扫描；b. 采用漏洞扫描工具和技术，通过使用以下标准来促进工具之间的互操作性，并实现漏洞管理过程的自动化：1. 枚举平台、软件缺陷和不当配置；2. 设置清单和测试程序格式；以及 3. 衡量漏洞的影响；c. 分析漏洞扫描报告和安全控制评估结果；d. 根据组织的风险评估，修复合法漏洞 [分配：组织定义的响应时间]；以及 e. 与 [分配：组织定义的人员或角色] 共享从漏洞扫描过程和安全控制评估中获得的信息，以帮助消除其他信息系统中的类似漏洞（即系统薄弱环节或缺陷）。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
SA-3(a)	组织：a. 使用包含信息安全注意事项的 [分配：组织定义的系统开发生命周期] 管理信息系统。	codebuild-project-envvar-awscred-检查	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
SA-3(a)	组织：a. 使用包含信息安全注意事项的 [分配：组织定义的系统开发生命周期] 管理信息系统。	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
SA-3(a)	组织：a. 使用包含信息安全注意事项的 [分配：组织定义的系统开发生命周期] 管理信息系统。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
SA-10	组织要求信息系统、系统组件或信息系统服务的开发人员：a. 在系统、组件或服务的 [选择（一项或多项）：设计；开发；实施；操作] 期间执行配置管理；b. 记录、管理和控制 [分配：组织定义的接受配置管理的配置项] 的更改的完整性；c. 仅对系统、组件或服务实施组织批准的更改；d. 记录经批准的系统、组件或服务变更，以及此类变更的潜在安全影响；以及 e. 跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给 [分配：组织定义的人员]。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SA-10	组织要求信息系统、系统组件或信息系统服务的开发人员：a. 在系统、组件或服务的 [选择（一项或多项）：设计；开发；实施；操作] 期间执行配置管理；b. 记录、管理和控制 [分配：组织定义的接受配置管理的配置项] 的更改的完整性；c. 仅对系统、组件或服务实施组织批准的更改；d. 记录经批准的系统、组件或服务变更，以及此类变更的潜在安全影响；以及 e. 跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给 [分配：组织定义的人员]。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
SA-10	组织要求信息系统、系统组件或信息系统服务的开发人员：a. 在系统、组件或服务的 [选择（一项或多项）：设计；开发；实施；操作] 期间执行配置管理；b. 记录、管理和控制 [分配：组织定义的接受配置管理的配置项] 的更改的完整性；c. 仅对系统、组件或服务实施组织批准的更改；d. 记录经批准的系统、组件或服务变更，以及此类变更的潜在安全影响；以及 e. 跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给 [分配：组织定义的人员]。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SA-10	组织要求信息系统、系统组件或信息系统服务的开发人员：a. 在系统、组件或服务的 [选择（一项或多项）：设计；开发；实施；操作] 期间执行配置管理；b. 记录、管理和控制 [分配：组织定义的接受配置管理的配置项] 的更改的完整性；c. 仅对系统、组件或服务实施组织批准的更改；d. 记录经批准的系统、组件或服务变更，以及此类变更的潜在安全影响；以及 e. 跟踪系统、组件或服务中的安全漏洞和漏洞解决方法，并将发现结果报告给 [分配：组织定义的人员]。	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
SC-2	信息系统将用户功能（包括用户界面服务）与信息系统管理功能分开。	iam-group-has-users-检查	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
SC-2	信息系统将用户功能（包括用户界面服务）与信息系统管理功能分开。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
SC-4	信息系统可防止通过共享系统资源进行未经授权和意外的信息传输。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	autoscaling-group-elb-healthcheck-必填项	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	elb-cross-zone-load-启用平衡	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
SC-5	信息系统通过采用 [分配：组织定义的安全保护措施] 来防范或限制以下类型的拒绝服务攻击的影响：[分配：组织定义的拒绝服务攻击类型或对此类信息来源的引用]。	rds-instance-deletion-protection-已启用	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	alb-http-to-https-重定向检查	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	elb-tls-https-listeners-只有	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	internet-gateway-authorized-vpc-只有	确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），从而管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	ebs-snapshot-public-restorable-检查	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	lambda-function-public-access-禁止	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	rds-instance-public-access-检查	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	redshift-cluster-public-access-检查	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	sagemaker-notebook-no-direct-互联网接入	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	vpc-default-security-group-已关闭	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	s3-account-level-public-access-blocks	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	alb-http-drop-invalid-已启用标题	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	信息系统：a. 监视和控制系统外部边界及系统内关键内部边界的通信；b. 为 [选择：物理上；逻辑上] 与内部组织网络分开的可公开访问的系统组件实现子网；c. 仅通过由边界保护设备组成的受管接口连接外部网络或信息系统，边界保护设备按照组织安全架构进行布置。	elasticsearch-node-to-node-加密检查	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	internet-gateway-authorized-vpc-只有	确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），从而管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	ebs-snapshot-public-restorable-检查	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	lambda-function-public-access-禁止	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	rds-instance-public-access-检查	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	redshift-cluster-public-access-检查	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	s3-account-level-public-access-blocks	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	sagemaker-notebook-no-direct-互联网接入	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	vpc-default-security-group-已关闭	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	该组织限制与信息系统的外部网络连接数量。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-8	信息系统保护所传输信息的 [选择（一项或多项）：机密性；完整性]。	alb-http-to-https-重定向检查	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	信息系统保护所传输信息的 [选择（一项或多项）：机密性；完整性]。	alb-http-drop-invalid-已启用标题	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8	信息系统保护所传输信息的 [选择（一项或多项）：机密性；完整性]。	elasticsearch-node-to-node-加密检查	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	信息系统保护所传输信息的 [选择（一项或多项）：机密性；完整性]。	elb-tls-https-listeners-只有	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	信息系统保护所传输信息的 [选择（一项或多项）：机密性；完整性]。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8	信息系统保护所传输信息的 [选择（一项或多项）：机密性；完整性]。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	信息系统保护所传输信息的 [选择（一项或多项）：机密性；完整性]。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	alb-http-to-https-重定向检查	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	alb-http-drop-invalid-已启用标题	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	elasticsearch-node-to-node-加密检查	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	elb-tls-https-listeners-只有	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	信息系统在传输过程中实现加密机制，以便 [选择（一项或多项）：防止未经授权披露信息；检测信息的变化]，除非以其他方式受到 [分配：组织定义的备选物理保护措施] 的保护。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC-12	组织根据 [分配：组织定义的密钥生成、分发、存储、访问和销毁要求]，为信息系统中使用的所需加密技术建立和管理加密密钥。	cmk-backing-key-rotation-已启用	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。
SC-12	组织根据 [分配：组织定义的密钥生成、分发、存储、访问和销毁要求]，为信息系统中使用的所需加密技术建立和管理加密密钥。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
SC-12	组织根据 [分配：组织定义的密钥生成、分发、存储、访问和销毁要求]，为信息系统中使用的所需加密技术建立和管理加密密钥。	kms-cmk-not-scheduled-用于删除	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	alb-http-to-https-重定向检查	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	api-gw-cache-enabled 并已加密	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	s3-已bucket-server-side-encryption启用	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	sagemaker-endpoint-configuration-kms-密钥已配置	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	sagemaker-notebook-instance-kms-密钥已配置	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准实施 [分配：组织定义的加密用途和每种用途所需的加密类型]。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	信息系统根据适用的联邦法律、行政令、指令、政策、法规和标准，实施经过 FIPS 验证或国家安全局批准的加密技术。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
SC-23	信息系统保护通信会话的真实性。	alb-http-to-https-重定向检查	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23	信息系统保护通信会话的真实性。	alb-http-drop-invalid-已启用标题	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-23	信息系统保护通信会话的真实性。	elb-tls-https-listeners-只有	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	api-gw-cache-enabled 并已加密	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	kms-cmk-not-scheduled-用于删除	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	s3-已bucket-server-side-encryption启用	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	sagemaker-endpoint-configuration-kms-密钥已配置	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	sagemaker-notebook-instance-kms-密钥已配置	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	信息系统保护 [分配：组织定义的静态信息] 的 [选择（一项或多项）：机密性；完整性]。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-36	组织将 [分配：组织定义的处理和存储] 分配到多个物理地点。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
SC-36	组织将 [分配：组织定义的处理和存储] 分配到多个物理地点。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
SI-2(2)	组织采用自动化机制 [分配：组织定义的频率] 来确定信息系统组件在缺陷修复方面的状态。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
SI-2(2)	组织采用自动化机制 [分配：组织定义的频率] 来确定信息系统组件在缺陷修复方面的状态。	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
SI-2(2)	组织采用自动化机制 [分配：组织定义的频率] 来确定信息系统组件在缺陷修复方面的状态。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
SI-4(1)	组织将各个入侵检测工具连接起来并配置到信息系统范围的入侵检测系统中。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(2)	组织使用自动化工具来支持事件的近实时分析。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
SI-4(4)	信息系统监控入站和出站通信流量 [分配：组织定义的频率] 中是否存在异常或未经授权的活动或情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(4)	信息系统监控入站和出站通信流量 [分配：组织定义的频率] 中是否存在异常或未经授权的活动或情况。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SI-4(4)	信息系统监控入站和出站通信流量 [分配：组织定义的频率] 中是否存在异常或未经授权的活动或情况。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI-4(4)	信息系统监控入站和出站通信流量 [分配：组织定义的频率] 中是否存在异常或未经授权的活动或情况。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(5)	当出现以下感染或潜在感染迹象时，信息系统会提醒 [分配：组织定义的人员或角色]：[分配：组织定义的感染指标]。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-4(5)	当出现以下感染或潜在感染迹象时，信息系统会提醒 [分配：组织定义的人员或角色]：[分配：组织定义的感染指标]。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SI-4(5)	当出现以下感染或潜在感染迹象时，信息系统会提醒 [分配：组织定义的人员或角色]：[分配：组织定义的感染指标]。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI-4(5)	当出现以下感染或潜在感染迹象时，信息系统会提醒 [分配：组织定义的人员或角色]：[分配：组织定义的感染指标]。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(16)	组织将来自整个信息系统中使用的监控工具的信息关联起来。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-4(16)	组织将来自整个信息系统中使用的监控工具的信息关联起来。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	cloud-trail-cloud-watch-启用日志	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(a)(b)(c)	组织：a. 监控要检测的信息系统：1. 根据 [分配：组织定义的监控目标] 的攻击和潜在攻击指标；以及 2. 未经授权的本地、网络和远程连接；b. 通过 [分配：组织定义的技术和方法] 识别未经授权使用信息系统的行为；c. i. 在信息系统内战略性地部署监控设备，以收集组织确定的基本信息；ii 在系统内的临时地点部署监控设备，以跟踪组织感兴趣的特定类型的交易。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
SI-7	组织使用完整性验证工具来检测对 [分配：组织定义的软件、固件和信息] 的未经授权的更改。	cloud-trail-log-file-已启用验证	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
SI-7(1)	信息系统在 [选择（一项或多项）：启动时；在 [分配：组织定义的过渡状态或安全相关事件]；[分配：组织定义的频率]] 对 [分配：组织定义的软件、固件和信息] 执行完整性检查。	ec2-管理instance-managed-by-systems器	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(1)	信息系统在 [选择（一项或多项）：启动时；在 [分配：组织定义的过渡状态或安全相关事件]；[分配：组织定义的频率]] 对 [分配：组织定义的软件、固件和信息] 执行完整性检查。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
SI-7(1)	信息系统在 [选择（一项或多项）：启动时；在 [分配：组织定义的过渡状态或安全相关事件]；[分配：组织定义的频率]] 对 [分配：组织定义的软件、固件和信息] 执行完整性检查。	cloud-trail-log-file-已启用验证	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	elasticache-redis-cluster-automatic-备份检查	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	组织根据适用的联邦法律、行政令、指令、政策、法规、标准和操作要求，处理和保留信息系统内的信息及系统输出的信息。	cw-loggroup-retention-period-检查	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

模板

该模板可在以下网址获得 GitHub：NIST 800-53 操作最佳实践 rev 4。

NIST 800-53 rev 5 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了 NIST 800-53 和托管 C AWS onfig 规则之间的映射示例。每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个 NIST 800-53 控件相关。一个 NIST 800-53 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	账户管理 | 自动化系统账户管理	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
AC-2(1)	账户管理 | 自动化系统账户管理	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
AC-2(1)	账户管理 | 自动化系统账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控

控制 ID	控制描述	AWS Config 规则	指南
			制、回滚和委托权限管理。
AC-2(1)	账户管理 | 自动化系统账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(1)	账户管理 | 自动化系统账户管理	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	账户管理 | 自动化系统账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	账户管理 | 自动化系统账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	账户管理 | 自动化系统账户管理	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	账户管理 | 自动化系统账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2(1)	账户管理 | 自动化系统账户管理	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-2(1)	账户管理 | 自动化系统账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	账户管理 | 自动化系统账户管理	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC-2(1)	账户管理 | 自动化系统账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	账户管理 | 自动化系统账户管理	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC-2(1)	账户管理 | 自动化系统账户管理	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC-2(1)	账户管理 | 自动化系统账户管理	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC-2(1)	账户管理 | 自动化系统账户管理	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC-2(3)	账户管理 | 禁用账户	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(3)	账户管理 | 禁用账户	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(3)	账户管理 | 禁用账户	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-2(4)	账户管理 | 自动审计操作	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	账户管理 | 自动审计操作	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC-2(4)	账户管理 | 自动审计操作	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	账户管理 | 自动审计操作	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AC-2(4)	账户管理 | 自动审计操作	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC-2(4)	账户管理 | 自动审计操作	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	账户管理 | 自动审计操作	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AC-2(4)	账户管理 | 自动审计操作	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2(4)	账户管理 | 自动审计操作	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AC-2(12)	账户管理 | 非典型使用情况的账户监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC-2	账户管理	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-2	账户管理	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-2	账户管理	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-3(7)	强制访问权限 | 基于角色的访问控制	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC-3(7)	强制访问权限 | 基于角色的访问控制	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC-3(7)	强制访问权限 | 基于角色的访问控制	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
AC-3(7)	强制访问权限 | 基于角色的访问控制	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC-3(7)	强制访问权限 | 基于角色的访问控制	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC-3(7)	强制访问权限 | 基于角色的访问控制	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-3(7)	强制访问权限 | 基于角色的访问控制	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-3(7)	强制访问权限 | 基于角色的访问控制	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-3(7)	强制访问权限 | 基于角色的访问控制	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-3(7)	强制访问权限 | 基于角色的访问控制	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-3(7)	强制访问权限 | 基于角色的访问控制	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-3(7)	强制访问权限 | 基于角色的访问控制	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-3(7)	强制访问权限 | 基于角色的访问控制	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-3(7)	强制访问权限 | 基于角色的访问控制	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-3(7)	强制访问权限 | 基于角色的访问控制	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-3(7)	强制访问权限 | 基于角色的访问控制	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-3(7)	强制访问权限 | 基于角色的访问控制	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(7)	强制访问权限 | 基于角色的访问控制	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-3(15)	强制访问权限 | 自由和强制访问控制	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC-3(15)	强制访问权限 | 自由和强制访问控制	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(15)	强制访问权限 | 自由和强制访问控制	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
AC-3(15)	强制访问权限 | 自由和强制访问控制	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-3(15)	强制访问权限 | 自由和强制访问控制	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
AC-3(15)	强制访问权限 | 自由和强制访问控制	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-3(15)	强制访问权限 | 自由和强制访问控制	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
AC-3(15)	强制访问权限 | 自由和强制访问控制	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
AC-3(15)	强制访问权限 | 自由和强制访问控制	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
AC-3(15)	强制访问权限 | 自由和强制访问控制	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
AC-3	强制访问权限	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC-3	强制访问权限	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC-3	强制访问权限	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
AC-3	强制访问权限	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC-3	强制访问权限	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-3	强制访问权限	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-3	强制访问权限	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-3	强制访问权限	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-3	强制访问权限	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-3	强制访问权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-3	强制访问权限	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-3	强制访问权限	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-3	强制访问权限	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-3	强制访问权限	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-3	强制访问权限	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-3	强制访问权限	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-3	强制访问权限	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(21)	强制执行信息流 | 信息流的物理或逻辑分离	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC-4(26)	强制执行信息流 | 审计筛选操作	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(26)	强制执行信息流 | 审计筛选操作	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC-4(26)	强制执行信息流 | 审计筛选操作	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(26)	强制执行信息流 | 审计筛选操作	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AC-4(26)	强制执行信息流 | 审计筛选操作	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AC-4(26)	强制执行信息流 | 审计筛选操作	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(26)	强制执行信息流 | 审计筛选操作	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC-4(26)	强制执行信息流 | 审计筛选操作	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AC-4(26)	强制执行信息流 | 审计筛选操作	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(26)	强制执行信息流 | 审计筛选操作	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AC-4(26)	强制执行信息流 | 审计筛选操作	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-4(26)	强制执行信息流 | 审计筛选操作	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AC-4(26)	强制执行信息流 | 审计筛选操作	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
AC-4	强制执行信息流	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-4	强制执行信息流	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
AC-4	强制执行信息流	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
AC-4	强制执行信息流	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
AC-4	强制执行信息流	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
AC-4	强制执行信息流	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
AC-4	强制执行信息流	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
AC-4	强制执行信息流	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4	强制执行信息流	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4	强制执行信息流	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-4	强制执行信息流	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
AC-4	强制执行信息流	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-4	强制执行信息流	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-4	强制执行信息流	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-4	强制执行信息流	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-4	强制执行信息流	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-4	强制执行信息流	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-4	强制执行信息流	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-4	强制执行信息流	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
AC-4	强制执行信息流	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-4	强制执行信息流	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-4	强制执行信息流	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
AC-5	职责分离	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
AC-5	职责分离	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
AC-5	职责分离	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-5	职责分离	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-5	职责分离	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-5	职责分离	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6(2)	最低权限 | 非安全功能的非特权访问权限	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6(2)	最低权限 | 非安全功能的非特权访问权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(2)	最低权限 | 非安全功能的非特权访问权限	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-6(3)	最低权限 | 特权命令的网络访问权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC-6(3)	最低权限 | 特权命令的网络访问权限	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(3)	最低权限 | 特权命令的网络访问权限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-6(3)	最低权限 | 特权命令的网络访问权限	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(3)	最低权限 | 特权命令的网络访问权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6(3)	最低权限 | 特权命令的网络访问权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6(9)	最低权限 | 记录特权功能的使用情况	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(9)	最低权限 | 记录特权功能的使用情况	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AC-6(9)	最低权限 | 记录特权功能的使用情况	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(9)	最低权限 | 记录特权功能的使用情况	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AC-6(9)	最低权限 | 记录特权功能的使用情况	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AC-6(9)	最低权限 | 记录特权功能的使用情况	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(9)	最低权限 | 记录特权功能的使用情况	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AC-6(9)	最低权限 | 记录特权功能的使用情况	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(9)	最低权限 | 记录特权功能的使用情况	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AC-6(10)	最低权限 | 禁止非特权用户执行特权功能	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6(10)	最低权限 | 禁止非特权用户执行特权功能	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6(10)	最低权限 | 禁止非特权用户执行特权功能	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-6	最低权限	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
AC-6	最低权限	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
AC-6	最低权限	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
AC-6	最低权限	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
AC-6	最低权限	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC-6	最低权限	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-6	最低权限	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-6	最低权限	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-6	最低权限	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
AC-6	最低权限	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
AC-6	最低权限	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
AC-6	最低权限	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-6	最低权限	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-6	最低权限	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-6	最低权限	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-6	最低权限	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-6	最低权限	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-6	最低权限	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AC-17(2)	远程访问 | 使用加密来保护机密性和完整性	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
AC-17(2)	远程访问 | 使用加密来保护机密性和完整性	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(2)	远程访问 | 使用加密来保护机密性和完整性	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
AC-17(2)	远程访问 | 使用加密来保护机密性和完整性	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-17(2)	远程访问 | 使用加密来保护机密性和完整性	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
AC-17(2)	远程访问 | 使用加密来保护机密性和完整性	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
AC-17(2)	远程访问 | 使用加密来保护机密性和完整性	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
AC-21	信息共享	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
AC-21	信息共享	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
AC-21	信息共享	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
AC-21	信息共享	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-21	信息共享	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-21	信息共享	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-21	信息共享	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-21	信息共享	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
AC-21	信息共享	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
AC-21	信息共享	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
AC-21	信息共享	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
AC-21	信息共享	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-21	信息共享	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
AC-21	信息共享	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
AC-21	信息共享	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
AC-21	信息共享	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
AC-21	信息共享	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-21	信息共享	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
AC-21	信息共享	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
AC-21	信息共享	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
AU-2	事件日志记录	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	事件日志记录	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU-2	事件日志记录	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	事件日志记录	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU-2	事件日志记录	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-2	事件日志记录	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	事件日志记录	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-2	事件日志记录	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-2	事件日志记录	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	事件日志记录	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU-2	事件日志记录	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-2	事件日志记录	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-2	事件日志记录	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
AU-3	审计记录的内容	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
AU-3	审计记录的内容	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-3	审计记录的内容	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-3	审计记录的内容	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-3	审计记录的内容	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU-3	审计记录的内容	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-3	审计记录的内容	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-3	审计记录的内容	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)	审计记录的审查、分析和报告 | 自动化流程集成	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-6(1)	审计记录的审查、分析和报告 | 自动化流程集成	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)	审计记录的审查、分析和报告 | 自动化流程集成	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AU-6(1)	审计记录的审查、分析和报告 | 自动化流程集成	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-6(3)	审计记录的审查、分析和报告 | 关联审计记录存储库	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-6(4)	审计记录审查、分析和报告 | 集中审查和分析	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(5)	审计记录审查、分析和报告 | 审计记录的综合分析	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-6(5)	审计记录审查、分析和报告 | 审计记录的综合分析	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
AU-6(5)	审计记录审查、分析和报告 | 审计记录的综合分析	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
AU-6(5)	审计记录审查、分析和报告 | 审计记录的综合分析	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
AU-7(1)	减少审计记录并生成报告 | 自动处理	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU-9(2)	保护审计信息 | 存储在单独的物理系统或组件上	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
AU-9(2)	保护审计信息 | 存储在单独的物理系统或组件上	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
AU-9(2)	保护审计信息 | 存储在单独的物理系统或组件上	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
AU-9(7)	保护审计信息 | 存储在具有不同操作系统的组件上	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-9	保护审计信息	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
AU-9	保护审计信息	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-9	保护审计信息	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
AU-9	保护审计信息	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
AU-9	保护审计信息	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
AU-10	不可否认性	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AU-10	不可否认性	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU-10	不可否认性	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AU-10	不可否认性	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU-10	不可否认性	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-10	不可否认性	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
AU-10	不可否认性	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
AU-10	不可否认性	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-10	不可否认性	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
AU-10	不可否认性	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
AU-10	不可否认性	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-10	不可否认性	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-12	审计记录生成	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计记录生成	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
AU-12	审计记录生成	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计记录生成	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
AU-12	审计记录生成	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
AU-12	审计记录生成	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计记录生成	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
AU-12	审计记录生成	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
AU-12	审计记录生成	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计记录生成	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
AU-12	审计记录生成	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
AU-12	审计记录生成	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
AU-12	审计记录生成	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
AU-14(1)	会话审计 | 系统启动	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CA-7	持续监控	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
CA-7	持续监控	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
CA-7	持续监控	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
CA-7	持续监控	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	s3-event-notifications-enabled	Amazon S3 事件通知可以提醒相关人员注意对您的存储桶对象的任何意外或故意修改。示例警报包括：创建了新对象、对象移除、对象恢复、丢失和复制的对象。
CA-7	持续监控	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CA-7	持续监控	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
CA-7	持续监控	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CA-7	持续监控	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
CA-7	持续监控	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
CA-7	持续监控	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
CA-7	持续监控	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CA-7	持续监控	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
CA-7	持续监控	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
CA-9(1)	内部系统连接 | 合规性检查	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
CA-9(1)	内部系统连接 | 合规性检查	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
CA-9(1)	内部系统连接 | 合规性检查	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
CA-9(1)	内部系统连接 | 合规性检查	rds-instance-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Relational Database Service (Amazon RDS) 数据库实例的攻击面。
CA-9(1)	内部系统连接 | 合规性检查	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CA-9(1)	内部系统连接 | 合规性检查	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
CA-9(1)	内部系统连接 | 合规性检查	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CA-9(1)	内部系统连接 | 合规性检查	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
CA-9(1)	内部系统连接 | 合规性检查	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CA-9(1)	内部系统连接 | 合规性检查	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
CA-9(1)	内部系统连接 | 合规性检查	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CA-9(1)	内部系统连接 | 合规性检查	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
CA-9(1)	内部系统连接 | 合规性检查	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CA-9(1)	内部系统连接 | 合规性检查	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CA-9(1)	内部系统连接 | 合规性检查	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CA-9(1)	内部系统连接 | 合规性检查	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CA-9(1)	内部系统连接 | 合规性检查	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	redshift-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Redshift 集群的攻击面。
CA-9(1)	内部系统连接 | 合规性检查	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CA-9(1)	内部系统连接 | 合规性检查	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CA-9(1)	内部系统连接 | 合规性检查	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
CA-9(1)	内部系统连接 | 合规性检查	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CM-2(2)	基线配置 | 提供自动支持以实现准确性和时效性	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-2(2)	基线配置 | 提供自动支持以实现准确性和时效性	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM-2(2)	基线配置 | 提供自动支持以实现准确性和时效性	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
CM-2(2)	基线配置 | 提供自动支持以实现准确性和时效性	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CM-2(2)	基线配置 | 提供自动支持以实现准确性和时效性	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CM-2(2)	基线配置 | 提供自动支持以实现准确性和时效性	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CM-2	基线配置	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
CM-2	基线配置	rds-instance-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Relational Database Service (Amazon RDS) 数据库实例的攻击面。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-2	基线配置	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
CM-2	基线配置	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
CM-2	基线配置	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
CM-2	基线配置	redshift-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Redshift 集群的攻击面。

控制 ID	控制描述	AWS Config 规则	指南
CM-2	基线配置	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CM-3(6)	配置变更控制 | 加密管理	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
CM-3(6)	配置变更控制 | 加密管理	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
CM-3(6)	配置变更控制 | 加密管理	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CM-3(6)	配置变更控制 | 加密管理	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
CM-3(6)	配置变更控制 | 加密管理	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CM-3(6)	配置变更控制 | 加密管理	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CM-3(6)	配置变更控制 | 加密管理	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
CM-3(6)	配置变更控制 | 加密管理	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CM-3(6)	配置变更控制 | 加密管理	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CM-3(6)	配置变更控制 | 加密管理	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
CM-3(6)	配置变更控制 | 加密管理	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
CM-3(6)	配置变更控制 | 加密管理	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
CM-3(6)	配置变更控制 | 加密管理	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
CM-3(6)	配置变更控制 | 加密管理	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
CM-3(6)	配置变更控制 | 加密管理	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CM-3(6)	配置变更控制 | 加密管理	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CM-3(6)	配置变更控制 | 加密管理	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CM-3(6)	配置变更控制 | 加密管理	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
CM-3(6)	配置变更控制 | 加密管理	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CM-3(6)	配置变更控制 | 加密管理	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
CM-3	配置变更控制	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
CM-3	配置变更控制	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
CM-7	最少功能	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
CM-7	最少功能	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
CM-7	最少功能	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
CM-8(1)	系统组件清单 | 安装和移除期间更新	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM-8(1)	系统组件清单 | 安装和移除期间更新	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
CM-8(2)	系统组件清单 | 自动维护	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
CM-8(3)	系统组件清单 | 自动检测未经授权的组件	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-8(3)	系统组件清单 | 自动检测未经授权的组件	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CM-8(3)	系统组件清单 | 自动检测未经授权的组件	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
CM-8(3)	系统组件清单 | 自动检测未经授权的组件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
CM-8	系统组件清单	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
CM-8	系统组件清单	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
CP-2(2)	应急计划 | 容量规划	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
CP-2(2)	应急计划 | 容量规划	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(1)	备用存储站点 | 与主站点分离	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-6(1)	备用存储站点 | 与主站点分离	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(1)	备用存储站点 | 与主站点分离	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-6(1)	备用存储站点 | 与主站点分离	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(1)	备用存储站点 | 与主站点分离	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-6(1)	备用存储站点 | 与主站点分离	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CP-6(1)	备用存储站点 | 与主站点分离	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(1)	备用存储站点 | 与主站点分离	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CP-6(2)	备用存储站点 | 恢复时间和恢复点目标	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
CP-6	备用存储站点	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-6	备用存储站点	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-6	备用存储站点	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-6	备用存储站点	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CP-6	备用存储站点	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-6	备用存储站点	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CP-6	备用存储站点	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
CP-6	备用存储站点	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	系统备份	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9	系统备份	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	系统备份	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-9	系统备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	系统备份	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。
CP-9	系统备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-9	系统备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	系统备份	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CP-9	系统备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	系统备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
CP-9	系统备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-9	系统备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CP-10	系统恢复和重组	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	系统恢复和重组	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
CP-10	系统恢复和重组	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	系统恢复和重组	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
CP-10	系统恢复和重组	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
CP-10	系统恢复和重组	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	系统恢复和重组	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
CP-10	系统恢复和重组	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
CP-10	系统恢复和重组	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	系统恢复和重组	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
CP-10	系统恢复和重组	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	系统恢复和重组	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
CP-10	系统恢复和重组	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
CP-10	系统恢复和重组	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
CP-10	系统恢复和重组	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
IA-2(1)	标识和身份验证（组织用户）| 特权账户的多重身份验证	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA-2(1)	标识和身份验证（组织用户）| 特权账户的多重身份验证	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA-2(1)	标识和身份验证（组织用户）| 特权账户的多重身份验证	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA-2(1)	标识和身份验证（组织用户）| 特权账户的多重身份验证	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2(2)	标识和身份验证（组织用户）| 非特权账户的多重身份验证	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA-2(2)	标识和身份验证（组织用户）| 非特权账户的多重身份验证	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
IA-2(2)	标识和身份验证（组织用户）| 非特权账户的多重身份验证	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2(2)	标识和身份验证（组织用户）| 非特权账户的多重身份验证	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2(6)	标识和身份验证（组织用户）| 账户访问权限 - 独立设备	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
IA-2(6)	标识和身份验证（组织用户）| 账户访问权限 - 独立设备	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA-2(6)	标识和身份验证（组织用户）| 账户访问权限 - 独立设备	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-2(6)	标识和身份验证（组织用户）| 账户访问权限 - 独立设备	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA-2(8)	标识和身份验证（组织用户）| 账户访问权限 - 防重播	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
IA-2(8)	标识和身份验证（组织用户）| 账户访问权限 - 防重播	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
IA-2(8)	标识和身份验证（组织用户）| 账户访问权限 - 防重播	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
IA-2(8)	标识和身份验证（组织用户）| 账户访问权限 - 防重播	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
IA-5(1)	身份验证器管理 | 基于密码的身份验证	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA-5(1)	身份验证器管理 | 基于密码的身份验证	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
IA-5(1)	身份验证器管理 | 基于密码的身份验证	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA-5(1)	身份验证器管理 | 基于密码的身份验证	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
IA-5(1)	身份验证器管理 | 基于密码的身份验证	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
IA-5(1)	身份验证器管理 | 基于密码的身份验证	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
IA-5(1)	身份验证器管理 | 基于密码的身份验证	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
IA-5(1)	身份验证器管理 | 基于密码的身份验证	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
IA-5(7)	身份验证器管理 | 无嵌入式未加密静态身份验证器	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
IR-4(1)	事件处理 | 自动事件处理流程	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
IR-4(5)	事件处理 | 自动禁用系统	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
RA-3(4)	风险评估 | 预测性网络分析	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SA-3	系统开发生命周期	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
SA-3	系统开发生命周期	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
SA-8(19)	安全和隐私工程原则 | 持续保护	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SA-8(21)	安全和隐私工程原理 | 自我分析	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SA-8(22)	安全和隐私工程原则 | 问责制和可追溯性	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
SA-8(25)	安全和隐私工程原理 | 经济安全	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SA-11(1)	开发人员测试和评估 | 静态代码分析	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SA-11(6)	开发人员测试和评估 | 攻击面审查	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SA-15(2)	开发流程、标准和工具 | 安全和隐私跟踪工具	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SA-15(2)	开发流程、标准和工具 | 安全和隐私跟踪工具	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SA-15(8)	开发流程、标准和工具 | 威胁和漏洞信息的重用	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SA-15(8)	开发流程、标准和工具 | 威胁和漏洞信息的重用	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SC-5(1)	D enial-of-service 保护 | 限制攻击其他系统的能力	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，A mazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
SC-5(2)	D enial-of-service 保护 | 容量、带宽和冗余	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC-5(3)	D enial-of-service 保护 | 检测和监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SC-5	D enial-of-service 防护	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SC-7(3)	边界保护 | 接入点	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	边界保护 | 接入点	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
SC-7(3)	边界保护 | 接入点	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	边界保护 | 接入点	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(3)	边界保护 | 接入点	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(3)	边界保护 | 接入点	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	边界保护 | 接入点	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(3)	边界保护 | 接入点	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(3)	边界保护 | 接入点	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	边界保护 | 接入点	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	边界保护 | 接入点	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(3)	边界保护 | 接入点	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	边界保护 | 接入点	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7(3)	边界保护 | 接入点	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	边界保护 | 接入点	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-7(3)	边界保护 | 接入点	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	边界保护 | 接入点	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(3)	边界保护 | 接入点	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(3)	边界保护 | 接入点	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(3)	边界保护 | 接入点	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SC-7(4)	边界保护 | 外部电信服务	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
SC-7(4)	边界保护 | 外部电信服务	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-7(4)	边界保护 | 外部电信服务	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
SC-7(4)	边界保护 | 外部电信服务	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
SC-7(4)	边界保护 | 外部电信服务	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-7(4)	边界保护 | 外部电信服务	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC-7(4)	边界保护 | 外部电信服务	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-7(4)	边界保护 | 外部电信服务	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC-7(4)	边界保护 | 外部电信服务	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(4)	边界保护 | 外部电信服务	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(4)	边界保护 | 外部电信服务	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-7(4)	边界保护 | 外部电信服务	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-7(4)	边界保护 | 外部电信服务	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
SC-7(4)	边界保护 | 外部电信服务	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(4)	边界保护 | 外部电信服务	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7(4)	边界保护 | 外部电信服务	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7(4)	边界保护 | 外部电信服务	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-7(4)	边界保护 | 外部电信服务	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(4)	边界保护 | 外部电信服务	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(4)	边界保护 | 外部电信服务	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC-7(4)	边界保护 | 外部电信服务	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SC-7(4)	边界保护 | 外部电信服务	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(4)	边界保护 | 外部电信服务	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-7(5)	边界保护 | 默认拒绝 - 允许按例外处理	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(5)	边界保护 | 默认拒绝 - 允许按例外处理	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
SC-7(5)	边界保护 | 默认拒绝 - 允许按例外处理	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(5)	边界保护 | 默认拒绝 - 允许按例外处理	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(9)	边界保护 | 限制威胁性传出通信流量	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
SC-7(9)	边界保护 | 限制威胁性传出通信流量	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(10)	边界保护 | 防止渗透	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
SC-7(10)	边界保护 | 防止渗透	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
SC-7(10)	边界保护 | 防止渗透	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-7(10)	边界保护 | 防止渗透	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(10)	边界保护 | 防止渗透	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC-7(10)	边界保护 | 防止渗透	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
SC-7(10)	边界保护 | 防止渗透	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
SC-7(10)	边界保护 | 防止渗透	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(10)	边界保护 | 防止渗透	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-7(10)	边界保护 | 防止渗透	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(10)	边界保护 | 防止渗透	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
SC-7(10)	边界保护 | 防止渗透	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(10)	边界保护 | 防止渗透	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-7(10)	边界保护 | 防止渗透	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
SC-7(10)	边界保护 | 防止渗透	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(10)	边界保护 | 防止渗透	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-7(10)	边界保护 | 防止渗透	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(10)	边界保护 | 防止渗透	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
SC-7(11)	边界保护 | 限制传入通信流量	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
SC-7(11)	边界保护 | 限制传入通信流量	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
SC-7(11)	边界保护 | 限制传入通信流量	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
SC-7(11)	边界保护 | 限制传入通信流量	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC-7(11)	边界保护 | 限制传入通信流量	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(11)	边界保护 | 限制传入通信流量	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(11)	边界保护 | 限制传入通信流量	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(11)	边界保护 | 限制传入通信流量	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(11)	边界保护 | 限制传入通信流量	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7(11)	边界保护 | 限制传入通信流量	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-7(11)	边界保护 | 限制传入通信流量	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(11)	边界保护 | 限制传入通信流量	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(11)	边界保护 | 限制传入通信流量	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SC-7(11)	边界保护 | 限制传入通信流量	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(11)	边界保护 | 限制传入通信流量	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-7(16)	边界保护 | 防止发现系统组件	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC-7(16)	边界保护 | 防止发现系统组件	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
SC-7(16)	边界保护 | 防止发现系统组件	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC-7(16)	边界保护 | 防止发现系统组件	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(16)	边界保护 | 防止发现系统组件	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(16)	边界保护 | 防止发现系统组件	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(16)	边界保护 | 防止发现系统组件	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(16)	边界保护 | 防止发现系统组件	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(16)	边界保护 | 防止发现系统组件	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7(16)	边界保护 | 防止发现系统组件	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-7(16)	边界保护 | 防止发现系统组件	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(16)	边界保护 | 防止发现系统组件	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(16)	边界保护 | 防止发现系统组件	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SC-7(16)	边界保护 | 防止发现系统组件	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(16)	边界保护 | 防止发现系统组件	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-7(20)	边界保护 | 动态隔离和分割	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(20)	边界保护 | 动态隔离和分割	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
SC-7(20)	边界保护 | 动态隔离和分割	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(20)	边界保护 | 动态隔离和分割	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC-7(20)	边界保护 | 动态隔离和分割	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(20)	边界保护 | 动态隔离和分割	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(20)	边界保护 | 动态隔离和分割	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(20)	边界保护 | 动态隔离和分割	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(20)	边界保护 | 动态隔离和分割	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(20)	边界保护 | 动态隔离和分割	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(20)	边界保护 | 动态隔离和分割	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(20)	边界保护 | 动态隔离和分割	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(20)	边界保护 | 动态隔离和分割	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(20)	边界保护 | 动态隔离和分割	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7(20)	边界保护 | 动态隔离和分割	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(20)	边界保护 | 动态隔离和分割	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-7(20)	边界保护 | 动态隔离和分割	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(20)	边界保护 | 动态隔离和分割	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(20)	边界保护 | 动态隔离和分割	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(20)	边界保护 | 动态隔离和分割	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(20)	边界保护 | 动态隔离和分割	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SC-7(21)	边界保护 | 系统组件隔离	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
SC-7(21)	边界保护 | 系统组件隔离	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
SC-7(21)	边界保护 | 系统组件隔离	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
SC-7(21)	边界保护 | 系统组件隔离	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
SC-7(21)	边界保护 | 系统组件隔离	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(21)	边界保护 | 系统组件隔离	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(21)	边界保护 | 系统组件隔离	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7(21)	边界保护 | 系统组件隔离	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7(21)	边界保护 | 系统组件隔离	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7(21)	边界保护 | 系统组件隔离	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-7(21)	边界保护 | 系统组件隔离	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(21)	边界保护 | 系统组件隔离	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7(21)	边界保护 | 系统组件隔离	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SC-7(21)	边界保护 | 系统组件隔离	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7(21)	边界保护 | 系统组件隔离	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-7	边界保护	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
SC-7	边界保护	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
SC-7	边界保护	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
SC-7	边界保护	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7	边界保护	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7	边界保护	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7	边界保护	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
SC-7	边界保护	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
SC-7	边界保护	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
SC-7	边界保护	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
SC-7	边界保护	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云中资源的访问。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7	边界保护	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
SC-7	边界保护	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
SC-7	边界保护	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
SC-7	边界保护	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
SC-8(1)	传输机密性和完整性 | 加密保护	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(1)	传输机密性和完整性 | 加密保护	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-8(1)	传输机密性和完整性 | 加密保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	传输机密性和完整性 | 加密保护	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(1)	传输机密性和完整性 | 加密保护	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	传输机密性和完整性 | 加密保护	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	传输机密性和完整性 | 加密保护	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(1)	传输机密性和完整性 | 加密保护	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-8(1)	传输机密性和完整性 | 加密保护	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(1)	传输机密性和完整性 | 加密保护	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8(2)	传输机密性和完整性 | 传输前和传输后处理	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	传输机密性和完整性	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	传输机密性和完整性	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC-8	传输机密性和完整性	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	传输机密性和完整性	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
SC-8	传输机密性和完整性	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-8	传输机密性和完整性	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	传输机密性和完整性	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC-8	传输机密性和完整性	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC-8	传输机密性和完整性	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-8	传输机密性和完整性	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-12(2)	加密密钥的建立和管理 | 对称密钥	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
SC-12(2)	加密密钥的建立和管理 | 对称密钥	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC-12(3)	加密密钥的建立和管理 | 非对称密钥	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-12(3)	加密密钥的建立和管理 | 非对称密钥	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-12(3)	加密密钥的建立和管理 | 非对称密钥	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
SC-12(3)	加密密钥的建立和管理 | 非对称密钥	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-12(3)	加密密钥的建立和管理 | 非对称密钥	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
SC-12(3)	加密密钥的建立和管理 | 非对称密钥	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-12(3)	加密密钥的建立和管理 | 非对称密钥	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-12	加密密钥的建立和管理	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
SC-12	加密密钥的建立和管理	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
SC-13	加密保护	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
SC-13	加密保护	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13	加密保护	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13	加密保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
SC-13	加密保护	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
SC-13	加密保护	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13	加密保护	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13	加密保护	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SC-13	加密保护	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13	加密保护	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC-13	加密保护	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC-13	加密保护	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC-13	加密保护	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC-13	加密保护	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-13	加密保护	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
SC-13	加密保护	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13	加密保护	redshift-cluster-c onfiguration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-13	加密保护	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13	加密保护	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-13	加密保护	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-13	加密保护	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
SC-13	加密保护	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-23(3)	会话真实性 | 系统生成的唯一会话标识符	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23(3)	会话真实性 | 系统生成的唯一会话标识符	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23(3)	会话真实性 | 系统生成的唯一会话标识符	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
SC-23(3)	会话真实性 | 系统生成的唯一会话标识符	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23(3)	会话真实性 | 系统生成的唯一会话标识符	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23(3)	会话真实性 | 系统生成的唯一会话标识符	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
SC-23(3)	会话真实性 | 系统生成的唯一会话标识符	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-23(3)	会话真实性 | 系统生成的唯一会话标识符	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23(3)	会话真实性 | 系统生成的唯一会话标识符	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-23(5)	会话真实性 | 允许的证书颁发机构	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-23(5)	会话真实性 | 允许的证书颁发机构	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-23	会话真实性	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-23	会话真实性	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23	会话真实性	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
SC-23	会话真实性	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-23	会话真实性	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23	会话真实性	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SC-23	会话真实性	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
SC-23	会话真实性	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SC-23	会话真实性	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
SC-23	会话真实性	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28(1)	保护静态信息 | 加密保护	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
SC-28(1)	保护静态信息 | 加密保护	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
SC-28(1)	保护静态信息 | 加密保护	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28(1)	保护静态信息 | 加密保护	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28(1)	保护静态信息 | 加密保护	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28(1)	保护静态信息 | 加密保护	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28(1)	保护静态信息 | 加密保护	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28(1)	保护静态信息 | 加密保护	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28(1)	保护静态信息 | 加密保护	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SC-28(1)	保护静态信息 | 加密保护	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
SC-28(1)	保护静态信息 | 加密保护	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28(1)	保护静态信息 | 加密保护	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC-28(1)	保护静态信息 | 加密保护	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
SC-28(1)	保护静态信息 | 加密保护	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
SC-28(1)	保护静态信息 | 加密保护	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28(1)	保护静态信息 | 加密保护	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
SC-28(1)	保护静态信息 | 加密保护	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28(1)	保护静态信息 | 加密保护	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC-28(1)	保护静态信息 | 加密保护	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
SC-28(1)	保护静态信息 | 加密保护	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28(3)	保护静态信息 | 加密密钥	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
SC-28(3)	保护静态信息 | 加密密钥	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
SC-28	保护静态信息	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
SC-28	保护静态信息	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	保护静态信息	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	保护静态信息	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
SC-28	保护静态信息	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	保护静态信息	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	保护静态信息	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SC-28	保护静态信息	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	保护静态信息	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	保护静态信息	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
SC-28	保护静态信息	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
SC-28	保护静态信息	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SC-28	保护静态信息	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
SC-28	保护静态信息	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	保护静态信息	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	保护静态信息	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	保护静态信息	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-28	保护静态信息	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SC-28	保护静态信息	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SC-28	保护静态信息	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SC-36(2)	分布式处理和存储 | 同步	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
SC-36	分布式处理和存储	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
SC-36	分布式处理和存储	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
SC-36	分布式处理和存储	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
SC-36	分布式处理和存储	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
SI-2(2)	缺陷修复 | 自动缺陷修复状态	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
SI-2(2)	缺陷修复 | 自动缺陷修复状态	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
SI-2(2)	缺陷修复 | 自动缺陷修复状态	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-2(3)	缺陷修复 | 修复缺陷的时间和纠正措施的基准	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
SI-2(3)	缺陷修复 | 修复缺陷的时间和纠正措施的基准	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
SI-2(3)	缺陷修复 | 修复缺陷的时间和纠正措施的基准	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
SI-2(4)	缺陷修复 | 自动补丁管理工具	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
SI-2(4)	缺陷修复 | 自动补丁管理工具	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
SI-2(4)	缺陷修复 | 自动补丁管理工具	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
SI-2(5)	缺陷修复 | 自动软件和固件更新	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
SI-2(5)	缺陷修复 | 自动软件和固件更新	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
SI-2(5)	缺陷修复 | 自动软件和固件更新	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-2	缺陷修复	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
SI-2	缺陷修复	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
SI-2	缺陷修复	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
SI-2	缺陷修复	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
SI-2	缺陷修复	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-2	缺陷修复	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
SI-2	缺陷修复	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
SI-2	缺陷修复	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
SI-2	缺陷修复	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-3(8)	恶意代码防护 | 检测未经授权的命令	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
SI-3(8)	恶意代码防护 | 检测未经授权的命令	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD _TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
SI-3(8)	恶意代码防护 | 检测未经授权的命令	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
SI-3(8)	恶意代码防护 | 检测未经授权的命令	s3-event-notifications-enabled	Amazon S3 事件通知可以提醒相关人员注意对您的存储桶对象的任何意外或故意修改。示例警报包括：创建了新对象、对象移除、对象恢复、丢失和复制的对象。
SI-3(8)	恶意代码防护 | 检测未经授权的命令	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-3(8)	恶意代码防护 | 检测未经授权的命令	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI-3(8)	恶意代码防护 | 检测未经授权的命令	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SI-3(8)	恶意代码防护 | 检测未经授权的命令	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-3(8)	恶意代码防护 | 检测未经授权的命令	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
SI-3(8)	恶意代码防护 | 检测未经授权的命令	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-3(8)	恶意代码防护 | 检测未经授权的命令	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
SI-4(1)	系统监控 | 系统范围的入侵检测系统	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(2)	系统监控 | 用于实时分析的自动化工具和机制	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-4(4)	系统监控 | 入站和出站通信流量	s3-event-notifications-enabled	Amazon S3 事件通知可以提醒相关人员注意对您的存储桶对象的任何意外或故意修改。示例警报包括：创建了新对象、对象移除、对象恢复、丢失和复制的对象。
SI-4(4)	系统监控 | 入站和出站通信流量	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(5)	系统监控 | 系统生成的警报	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI-4(5)	系统监控 | 系统生成的警报	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(5)	系统监控 | 系统生成的警报	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-4(12)	系统监控 | 组织生成的自动警报	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(13)	系统监控 | 分析流量和事件模式	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-4(20)	系统监控 | 特权用户	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(20)	系统监控 | 特权用户	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
SI-4(20)	系统监控 | 特权用户	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(20)	系统监控 | 特权用户	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
SI-4(20)	系统监控 | 特权用户	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI-4(20)	系统监控 | 特权用户	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(20)	系统监控 | 特权用户	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
SI-4(20)	系统监控 | 特权用户	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(20)	系统监控 | 特权用户	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
SI-4(22)	系统监控 | 未经授权的网络服务	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
SI-4(25)	系统监控 | 优化网络流量分析	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-4	系统监控	s3-event-notifications-enabled	Amazon S3 事件通知可以提醒相关人员注意对您的存储桶对象的任何意外或故意修改。示例警报包括：创建了新对象、对象移除、对象恢复、丢失和复制的对象。
SI-4	系统监控	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
SI-4	系统监控	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
SI-7(1)	软件、固件和信息完整性 | 完整性检查	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(3)	软件、固件和信息完整性 | 集中管理的完整性工具	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
SI-7(6)	软件、固件和信息完整性 | 加密保护	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
SI-7(6)	软件、固件和信息完整性 | 加密保护	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(6)	软件、固件和信息完整性 | 加密保护	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SI-7(6)	软件、固件和信息完整性 | 加密保护	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SI-7(6)	软件、固件和信息完整性 | 加密保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(6)	软件、固件和信息完整性 | 加密保护	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
SI-7(6)	软件、固件和信息完整性 | 加密保护	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
SI-7(6)	软件、固件和信息完整性 | 加密保护	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SI-7(6)	软件、固件和信息完整性 | 加密保护	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(6)	软件、固件和信息完整性 | 加密保护	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
SI-7(6)	软件、固件和信息完整性 | 加密保护	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SI-7(6)	软件、固件和信息完整性 | 加密保护	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(6)	软件、固件和信息完整性 | 加密保护	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
SI-7(6)	软件、固件和信息完整性 | 加密保护	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
SI-7(6)	软件、固件和信息完整性 | 加密保护	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
SI-7(6)	软件、固件和信息完整性 | 加密保护	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(6)	软件、固件和信息完整性 | 加密保护	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
SI-7(6)	软件、固件和信息完整性 | 加密保护	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
SI-7(6)	软件、固件和信息完整性 | 加密保护	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
SI-7(6)	软件、固件和信息完整性 | 加密保护	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(6)	软件、固件和信息完整性 | 加密保护	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SI-7(6)	软件、固件和信息完整性 | 加密保护	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(6)	软件、固件和信息完整性 | 加密保护	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
SI-7(6)	软件、固件和信息完整性 | 加密保护	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
SI-7(6)	软件、固件和信息完整性 | 加密保护	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(6)	软件、固件和信息完整性 | 加密保护	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
SI-7(6)	软件、固件和信息完整性 | 加密保护	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(7)	软件、固件和信息完整性 | 检测和响应集成	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
SI-7(8)	软件、固件和信息完整性 | 重大事件的审计能力	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息管理和保留	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
SI-12	信息管理和保留	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	信息管理和保留	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息管理和保留	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-12	信息管理和保留	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-12	信息管理和保留	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SI-12	信息管理和保留	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
SI-13(5)	可预测的故障预防 | 失效转移功能	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-13(5)	可预测的故障预防 | 失效转移功能	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
SI-13(5)	可预测的故障预防 | 失效转移功能	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
SI-13(5)	可预测的故障预防 | 失效转移功能	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
SI-13(5)	可预测的故障预防 | 失效转移功能	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
SI-13(5)	可预测的故障预防 | 失效转移功能	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
SI-13(5)	可预测的故障预防 | 失效转移功能	s3-version-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
SI-13(5)	可预测的故障预防 | 失效转移功能	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
SI-13(5)	可预测的故障预防 | 失效转移功能	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
SI-13(5)	可预测的故障预防 | 失效转移功能	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
SI-13(5)	可预测的故障预防 | 失效转移功能	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
SI-13(5)	可预测的故障预防 | 失效转移功能	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
SI-13(5)	可预测的故障预防 | 失效转移功能	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
SI-13(5)	可预测的故障预防 | 失效转移功能	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
SI-13(5)	可预测的故障预防 | 失效转移功能	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
SI-20	污点	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
SI-20	污点	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
SI-20	污点	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

模板

该模板可在以下网址获得 GitHub：NIST 800-53 操作最佳实践 rev 5。

NIST 800 171 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了 NIST 800-171 和托管 C AWS onfig 规则之间的映射示例。每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个 NIST 800-171 控件相关。一个 NIST 800-171 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	opensearch-access-control-enabled	确保在您的亚马逊 OpenSearch 服务域上启用精细访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
3.1.1	仅允许授权用户、代表授权用户行事的进程或设备（包括其他系统）访问系统。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	opensearch-access-control-enabled	确保在您的亚马逊 OpenSearch 服务域上启用精细访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
3.1.2	将系统的访问限制在授权用户获准执行的事务类型和功能范围内。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3.1.3	根据批准的授权控制 CUI 流。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.1.3	根据批准的授权控制 CUI 流。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.3	根据批准的授权控制 CUI 流。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.3	根据批准的授权控制 CUI 流。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.1.3	根据批准的授权控制 CUI 流。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
3.1.3	根据批准的授权控制 CUI 流。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.1.3	根据批准的授权控制 CUI 流。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.3	根据批准的授权控制 CUI 流。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.3	根据批准的授权控制 CUI 流。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.1.3	根据批准的授权控制 CUI 流。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.1.3	根据批准的授权控制 CUI 流。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.1.3	根据批准的授权控制 CUI 流。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3	根据批准的授权控制 CUI 流。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
3.1.3	根据批准的授权控制 CUI 流。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.1.4	分离个人职责，在不串通的情况下降低恶意活动的风险。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.1.5	采用最低权限原则，包括特定的安全功能和特权账户。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.6	访问非安全功能时，请使用非特权账户或角色。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.1.7	防止非特权用户执行特权功能并审计此类功能的执行情况。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.7	防止非特权用户执行特权功能并审计此类功能的执行情况。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
3.1.7	防止非特权用户执行特权功能并审计此类功能的执行情况。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
3.1.7	防止非特权用户执行特权功能并审计此类功能的执行情况。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.1.7	防止非特权用户执行特权功能并审计此类功能的执行情况。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.1.7	防止非特权用户执行特权功能并审计此类功能的执行情况。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1.7	防止非特权用户执行特权功能并审计此类功能的执行情况。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
3.1.12	监视和控制远程访问会话。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.1.12	监视和控制远程访问会话。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
3.1.12	监视和控制远程访问会话。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.1.12	监视和控制远程访问会话。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.1.12	监视和控制远程访问会话。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
3.1.12	监视和控制远程访问会话。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
3.1.12	监视和控制远程访问会话。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
3.1.12	监视和控制远程访问会话。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
3.1.12	监视和控制远程访问会话。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
3.1.12	监视和控制远程访问会话。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.1.12	监视和控制远程访问会话。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.1.12	监视和控制远程访问会话。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
3.1.12	监视和控制远程访问会话。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.1.13	使用加密机制来保护远程访问会话的机密性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.1.13	使用加密机制来保护远程访问会话的机密性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.13	使用加密机制来保护远程访问会话的机密性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.13	使用加密机制来保护远程访问会话的机密性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
3.1.13	使用加密机制来保护远程访问会话的机密性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.1.13	使用加密机制来保护远程访问会话的机密性。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
3.1.13	使用加密机制来保护远程访问会话的机密性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.13	使用加密机制来保护远程访问会话的机密性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.14	通过托管访问控制点进行远程访问。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3.1.14	通过托管访问控制点进行远程访问。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.1.14	通过托管访问控制点进行远程访问。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.14	通过托管访问控制点进行远程访问。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.14	通过托管访问控制点进行远程访问。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.1.14	通过托管访问控制点进行远程访问。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
3.1.14	通过托管访问控制点进行远程访问。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
3.1.14	通过托管访问控制点进行远程访问。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
3.1.14	通过托管访问控制点进行远程访问。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.1.14	通过托管访问控制点进行远程访问。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.14	通过托管访问控制点进行远程访问。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.14	通过托管访问控制点进行远程访问。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.1.14	通过托管访问控制点进行远程访问。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.1.14	通过托管访问控制点进行远程访问。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
3.1.14	通过托管访问控制点进行远程访问。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.14	通过托管访问控制点进行远程访问。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.20	验证和控制/限制与外部系统的连接和外部系统的使用。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
3.3.1	根据需要创建并保留系统审计记录，以便对非法、未经授权或不适当的系统活动进行监控、分析、调查和报告。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.3.2	确保每个系统用户的行为可以唯一追踪到这些用户，以便追究其行为责任。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
3.3.4	在审计流程失败时发出警报。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.3.4	在审计流程失败时发出警报。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.3.5	关联审计审查、分析和报告流程，以便调查和应对不当、可疑或异常活动的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.3.5	关联审计审查、分析和报告流程，以便调查和应对不当、可疑或异常活动的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.3.8	保护审计信息和审计工具免遭未经授权的访问、修改和删除。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
3.3.8	保护审计信息和审计工具免遭未经授权的访问、修改和删除。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
3.3.8	保护审计信息和审计工具免遭未经授权的访问、修改和删除。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
3.3.8	保护审计信息和审计工具免遭未经授权的访问、修改和删除。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.3.8	保护审计信息和审计工具免遭未经授权的访问、修改和删除。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
3.3.8	保护审计信息和审计工具免遭未经授权的访问、修改和删除。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.3.8	保护审计信息和审计工具免遭未经授权的访问、修改和删除。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.3.8	保护审计信息和审计工具免遭未经授权的访问、修改和删除。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
3.3.8	保护审计信息和审计工具免遭未经授权的访问、修改和删除。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
3.4.1	在相应的系统开发生命周期内，建立并维护组织系统的基线配置和库存（包括硬件、软件、固件和文档）。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.4.6	采用最少功能原则，将组织系统配置为仅提供基本功能。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.4.7	限制、禁用和防止使用不必要的功能、端口、协议或服务。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
3.4.7	限制、禁用和防止使用不必要的功能、端口、协议或服务。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.4.7	限制、禁用和防止使用不必要的功能、端口、协议或服务。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
3.4.7	限制、禁用和防止使用不必要的功能、端口、协议或服务。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.4.9	控制和监控用户安装的软件。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
3.4.9	控制和监控用户安装的软件。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织系统的先决条件。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。
3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织系统的先决条件。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
3.5.2	验证（或核实）这些用户、进程或设备的身份，这是允许访问组织系统的先决条件。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
3.5.3	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
3.5.3	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
3.5.3	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
3.5.3	对特权账户的本地和网络访问权限以及非特权账户的网络访问权限使用多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
3.5.5	防止在规定的时间段内重用标识符。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.5.6	在规定的非活动时间后禁用标识符。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.5.7	在创建新密码时，强制执行最低密码复杂度和更改字符的规定。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.5.8	禁止在指定的次数范围内重复使用密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.5.10	仅存储和传输受加密保护的密码。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.5.10	仅存储和传输受加密保护的密码。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.5.10	仅存储和传输受加密保护的密码。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.5.10	仅存储和传输受加密保护的密码。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
3.5.10	仅存储和传输受加密保护的密码。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.5.10	仅存储和传输受加密保护的密码。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.5.10	仅存储和传输受加密保护的密码。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.5.10	仅存储和传输受加密保护的密码。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.5.10	仅存储和传输受加密保护的密码。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.5.10	仅存储和传输受加密保护的密码。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
3.5.10	仅存储和传输受加密保护的密码。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.6.1	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
3.6.1	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.6.1	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。
3.6.1	为组织系统建立操作事件处理能力，包括准备、检测、分析、遏制、恢复和用户响应活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.11.2	定期扫描组织系统和应用程序中的漏洞，并在发现影响系统的新漏洞时进行扫描。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.11.2	定期扫描组织系统和应用程序中的漏洞，并在发现影响系统的新漏洞时进行扫描。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.11.3	根据风险评估修复漏洞。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
3.13.1	在组织系统的外部边界和关键内部边界监控、控制和保护通信（即组织系统传输或接收的信息）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	opensearch-access-control-enabled	确保在您的 Amazon OpenSearch 服务域上启用了精细的访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.2	采用架构设计、软件开发技术和系统工程原理，促进组织系统内的有效信息安全。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
3.13.6	默认情况下拒绝网络通信流量，并在例外情况下允许网络通信流量（即全部拒绝、按例外情况允许）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.6	默认情况下拒绝网络通信流量，并在例外情况下允许网络通信流量（即全部拒绝、按例外情况允许）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
3.13.6	默认情况下拒绝网络通信流量，并在例外情况下允许网络通信流量（即全部拒绝、按例外情况允许）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.13.8	实施加密机制，防止在传输过程中未经授权泄露 CUI，除非另有其他物理保护措施的保护。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.13.10	为组织系统中使用的密码技术建立和管理加密密钥。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
3.13.10	为组织系统中使用的密码技术建立和管理加密密钥。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
3.13.16	保护静态 CUI 的机密性。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
3.13.16	保护静态 CUI 的机密性。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.13.16	保护静态 CUI 的机密性。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.13.16	保护静态 CUI 的机密性。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
3.13.16	保护静态 CUI 的机密性。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.13.16	保护静态 CUI 的机密性。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
3.13.16	保护静态 CUI 的机密性。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
3.13.16	保护静态 CUI 的机密性。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
3.13.16	保护静态 CUI 的机密性。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.13.16	保护静态 CUI 的机密性。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
3.13.16	保护静态 CUI 的机密性。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
3.13.16	保护静态 CUI 的机密性。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
3.13.16	保护静态 CUI 的机密性。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
3.13.16	保护静态 CUI 的机密性。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
3.13.16	保护静态 CUI 的机密性。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.13.16	保护静态 CUI 的机密性。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
3.13.16	保护静态 CUI 的机密性。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.13.16	保护静态 CUI 的机密性。	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
3.14.1	及时识别、报告和纠正信息及系统缺陷。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.14.1	及时识别、报告和纠正信息及系统缺陷。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.14.2	在组织系统的适当位置提供针对恶意代码的保护。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.14.2	在组织系统的适当位置提供针对恶意代码的保护。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.14.3	监控系统安全警报和建议，并采取相应措施。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.14.3	监控系统安全警报和建议，并采取相应措施。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
3.14.3	监控系统安全警报和建议，并采取相应措施。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
3.14.3	监控系统安全警报和建议，并采取相应措施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.14.3	监控系统安全警报和建议，并采取相应措施。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
3.14.4	当有新版本可用时，更新恶意代码保护机制。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
3.14.6	监控组织系统，包括入站和出站通信流量，以检测攻击和潜在攻击的迹象。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.14.7	识别对组织系统的未经授权使用。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
3.14.7	识别对组织系统的未经授权使用。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REG ION_CLOUD _TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
3.14.7	识别对组织系统的未经授权使用。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
3.14.7	识别对组织系统的未经授权使用。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
3.14.7	识别对组织系统的未经授权使用。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
3.14.7	识别对组织系统的未经授权使用。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
3.14.7	识别对组织系统的未经授权使用。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
3.14.7	识别对组织系统的未经授权使用。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
3.14.7	识别对组织系统的未经授权使用。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
3.14.7	识别对组织系统的未经授权使用。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.14.7	识别对组织系统的未经授权使用。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
3.14.7	识别对组织系统的未经授权使用。	redshift-cluster-c onfiguration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.14.7	识别对组织系统的未经授权使用。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
3.14.7	识别对组织系统的未经授权使用。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

模板

该模板可在以下网址获得 GitHub：NIST 800 171 操作最佳实践。

NIST 800 172 操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了 NIST 800-172 和托管 C AWS onfig 规则之间的映射示例。每条 Config 规则都适用于特定的 AWS 资源，并与一个或多个 NIST 800-172 控件相关。一个 NIST 800-172 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	alb-desync-mode-check	为了帮助保护应用程序免受 HTTP Desync 漏洞的影响，请确保在应用程序负载均衡器上启用 HTTP Desync 缓解模式。HTTP Desync 问题可能导致请求走私，并使您的应用程序容易受到请求队列或缓存中毒的影响。异步缓解模式包括“监控”、“防御”和“最严格”。默认模式是防御。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	clb-desync-mode-check	为了帮助保护应用程序免受 HTTP Desync 漏洞的影响，请确保在应用程序负载均衡器上启用 HTTP Desync 缓解模式。HTTP Desync 问题可能导致请求走私，并使您的应用程序容易受到请求队列或缓存中毒的影响。异步缓解模式包括“监控”、“防御”和“最严格”。默认模式是防御。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	ec2-token-hop-limit-check	确保实例元数据服务 (IMDS) HTTP PUT 响应仅限于 Amazon Elastic Compute Cloud (Amazon EC2) 实例。在 IMDSv2 中，默认情况下包含密钥令牌的 PUT 响应无法传送到实例之外，因为元数据响应跃点限制设置为 1（Config 默认值）。如果此值大于 1，则令牌可以离开 EC2 实例。
3.1.3e	使用 [分配：组织定义的安全信息传输解决方案] 来控制互联系统上安全域之间的信息流动。	nacl-no-unrestricted-ssh-rdp	网络访问控制列表 (NACL) 中的远程服务器管理端口（例如端口 22 (SSH) 和端口 3389 (RDP)）不应设为可公开访问，因为这可能会允许对您的 VPC 内的资源进行意外访问。
3.2.1e	[分配：组织定义的频率] 提供认知培训，重点是识别和应对来自社交工程、高级持久威胁行为者、漏洞和可疑行为的威胁；[分配：组织定义的频率] 或在威胁发生重大变化时更新培训。	security-awareness-program-exists（过程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。

控制 ID	控制描述	AWS Config 规则	指南
3.4.2e	使用自动化机制来检测配置错误或未经授权的系统组件；检测到这些组件后，[选择（一项或多项）：移除组件；将组件置于隔离或补救网络中] 以方便打补丁、重新配置或采取其他缓解措施。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
3.4.2e	使用自动化机制来检测配置错误或未经授权的系统组件；检测到这些组件后，[选择（一项或多项）：移除组件；将组件置于隔离或补救网络中] 以方便打补丁、重新配置或采取其他缓解措施。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
3.4.2e	使用自动化机制来检测配置错误或未经授权的系统组件；检测到这些组件后，[选择（一项或多项）：移除组件；将组件置于隔离或补救网络中] 以方便打补丁、重新配置或采取其他缓解措施。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
3.4.2e	使用自动化机制来检测配置错误或未经授权的系统组件；检测到这些组件后，[选择（一项或多项）：移除组件；将组件置于隔离或补救网络中] 以方便打补丁、重新配置或采取其他缓解措施。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
3.4.3e	使用自动发现和管理工具来维护完整 up-to-date、准确且随时可用的系统组件清单。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
3.4.3e	使用自动发现和管理工具来维护完整 up-to-date、准确且随时可用的系统组件清单。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
3.4.3e	使用自动发现和管理工具来维护完整 up-to-date、准确且随时可用的系统组件清单。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
3.4.3e	使用自动发现和管理工具来维护完整 up-to-date、准确且随时可用的系统组件清单。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。
3.4.3e	使用自动发现和管理工具来维护完整 up-to-date、准确且随时可用的系统组件清单。	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	控制描述	AWS Config 规则	指南
3.5.2e	对于不支持多重身份验证或复杂账户管理的系统和系统组件，采用自动机制生成、保护、轮换和管理密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.5.2e	对于不支持多重身份验证或复杂账户管理的系统和系统组件，采用自动机制生成、保护、轮换和管理密码。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
3.5.2e	对于不支持多重身份验证或复杂账户管理的系统和系统组件，采用自动机制生成、保护、轮换和管理密码。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
3.5.2e	对于不支持多重身份验证或复杂账户管理的系统和系统组件，采用自动机制生成、保护、轮换和管理密码。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
3.11.1e	将 [分配：组织定义的威胁情报来源] 作为风险评估的一部分，为组织系统、安全架构、所选安全解决方案、监控、威胁搜寻以及响应和恢复活动的开发提供指导和信息。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.11.2e	开展网络威胁搜寻活动 [选择（一项或多项）：[分配：组织定义的频率]；[分配：组织定义的事件]]，在 [分配：组织定义的系统] 中搜索入侵指标，并检测、跟踪和破坏逃避现有控制的威胁。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.11.5e	根据当前和累积的威胁情报，[分配：组织定义的频率] 评估安全解决方案的有效性，以应对组织系统和组织面临的预期风险。	annual-risk-assessment-performed（过程检查）	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	nacl-no-unrestricted-ssh-rdp	网络访问控制列表 (NACL) 中的远程服务器管理端口（例如端口 22 (SSH) 和端口 3389 (RDP)）不应设为可公开访问，因为这可能会允许对您的 VPC 内的资源进行意外访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
3.13.4e	在组织系统和系统组件中使用 [选择：（一项或多项）：[分配：组织定义的物理隔离技术]；[分配：组织定义的逻辑隔离技术]]。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
3.14.1e	使用信任根机制或加密签名验证 [分配：组织定义的安全关键软件或基本软件] 的完整性。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
3.14.2e	持续监控组织系统和系统组件是否存在异常或可疑行为。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.14.2e	持续监控组织系统和系统组件是否存在异常或可疑行为。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
3.14.2e	持续监控组织系统和系统组件是否存在异常或可疑行为。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
3.14.2e	持续监控组织系统和系统组件是否存在异常或可疑行为。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
3.14.2e	持续监控组织系统和系统组件是否存在异常或可疑行为。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
3.14.2e	持续监控组织系统和系统组件是否存在异常或可疑行为。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.14.2e	持续监控组织系统和系统组件是否存在异常或可疑行为。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.14.6e	使用从 [分配：组织定义的外部组织] 获得的威胁指标信息和有效的缓解措施，来指导入侵检测和威胁搜寻并为其提供信息。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.14.7e	使用 [分配：组织定义的验证方法或技术] 验证 [分配：组织定义的安全关键或基本软件、固件和硬件组件] 的正确性。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
3.14.7e	使用 [分配：组织定义的验证方法或技术] 验证 [分配：组织定义的安全关键或基本软件、固件和硬件组件] 的正确性。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
3.14.7e	使用 [分配：组织定义的验证方法或技术] 验证 [分配：组织定义的安全关键或基本软件、固件和硬件组件] 的正确性。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
3.14.7e	使用 [分配：组织定义的验证方法或技术] 验证 [分配：组织定义的安全关键或基本软件、固件和硬件组件] 的正确性。	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。为了协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。

控制 ID	控制描述	AWS Config 规则	指南
3.14.7e	使用 [分配：组织定义的验证方法或技术] 验证 [分配：组织定义的安全关键或基本软件、固件和硬件组件] 的正确性。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。

模板

该模板可在以下网址获得 GitHub：NIST 800 172 操作最佳实践。

NIST 800 181 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了 NIST 800 181 和 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 NIST 800 181 控件相关。一个 NIST 800 181 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
T0008	分析和规划数据容量需求的预期变化。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的

控制 ID	控制描述	AWS Config 规则	指南
			读/写容量以处理突发流量，而不进行节流。
T0008	分析和规划数据容量需求的预期变化。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0008	分析和规划数据容量需求的预期变化。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
T0008	分析和规划数据容量需求的预期变化。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0008	分析和规划数据容量需求的预期变化。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0008	分析和规划数据容量需求的预期变化。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0008	分析和规划数据容量需求的预期变化。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
T0008	分析和规划数据容量需求的预期变化。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
T0008	分析和规划数据容量需求的预期变化。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0008	分析和规划数据容量需求的预期变化。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
T0008	分析和规划数据容量需求的预期变化。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
T0008	分析和规划数据容量需求的预期变化。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
T0008	分析和规划数据容量需求的预期变化。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
T0008	分析和规划数据容量需求的预期变化。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	opensearch-encrypted-at-rest	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elasticsearch Service (Amazon ES) 域启用了加密。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
T0017	应用以服务为导向的安全架构原则，以满足组织的机密性、完整性和可用性要求。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
T0024	收集和维护满足系统网络安全报告要求所需的数据。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
T0042	与网络防御分析师协调，管理和管理专业网络防御应用程序的规则和签名（例如，入侵检测/保护系统、防病毒和内容黑名单）的更新。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
T0047	关联事件数据以识别特定漏洞，并提出建议以实现快速修复。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
T0051	根据关键系统功能定义适当的系统可用性级别，并确保根据系统要求确定适当的灾难恢复和操作连续性要求，以包括任何适当的故障转移/备用站点要求、备份要求以及系统恢复/还原的重要支持性要求。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
T0065	制定和实施网络备份和恢复程序。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
T0065	制定和实施网络备份和恢复程序。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
T0065	制定和实施网络备份和恢复程序。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0065	制定和实施网络备份和恢复程序。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0065	制定和实施网络备份和恢复程序。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
T0065	制定和实施网络备份和恢复程序。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
T0065	制定和实施网络备份和恢复程序。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
T0065	制定和实施网络备份和恢复程序。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
T0065	制定和实施网络备份和恢复程序。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
T0065	制定和实施网络备份和恢复程序。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
T0065	制定和实施网络备份和恢复程序。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
T0065	制定和实施网络备份和恢复程序。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
T0070	为正在开发的系统制定灾难恢复和操作连续性计划，并确保在系统进入生产环境之前进行测试。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
T0086	确保为集成到系统设计中的商业产品应用安全补丁的工作符合管理机构为预期操作环境规定的时间表。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
T0086	确保为集成到系统设计中的商业产品应用安全补丁的工作符合管理机构为预期操作环境规定的时间表。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
T0086	确保为集成到系统设计中的商业产品应用安全补丁的工作符合管理机构为预期操作环境规定的时间表。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
T0086	确保为集成到系统设计中的商业产品应用安全补丁的工作符合管理机构为预期操作环境规定的时间表。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0110	识别和/或确定安全事件是否表明存在需要采取具体法律行动的违法行为。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
T0110	识别和/或确定安全事件是否表明存在需要采取具体法律行动的违法行为。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
T0110	识别和/或确定安全事件是否表明存在需要采取具体法律行动的违法行为。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
T0128	在可行的情况下，集成更新或修补系统软件的自动功能，并根据系统运行环境的当前和预计的修补时间表要求，制定手动更新和修补系统软件的流程和程序。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
T0128	在可行的情况下，集成更新或修补系统软件的自动功能，并根据系统运行环境的当前和预计的修补时间表要求，制定手动更新和修补系统软件的流程和程序。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
T0128	在可行的情况下，集成更新或修补系统软件的自动功能，并根据系统运行环境的当前和预计的修补时间表要求，制定手动更新和修补系统软件的流程和程序。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
T0128	在可行的情况下，集成更新或修补系统软件的自动功能，并根据系统运行环境的当前和预计的修补时间表要求，制定手动更新和修补系统软件的流程和程序。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
T0144	管理账户、网络权限以及对系统和设备的访问权限。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	opensearch-in-vpc-only	确保亚马逊 E AWS lasticsearch 服务 (Amazon ES) 域位于亚马逊虚拟私有云 (亚马逊 VPC) 中，从而管理对云的访问。Amazon VPC 中的 Amazon ES 域可实现 Amazon ES 与 Amazon VPC 中其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
T0144	管理账户、网络权限以及对系统和设备的访问权限。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
T0144	管理账户、网络权限以及对系统和设备的访问权限。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
T0151	监控和评估企业网络安全保障措施的有效性，以确保其提供预期的保护级别。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
T0151	监控和评估企业网络安全保障措施的有效性，以确保其提供预期的保护级别。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
T0151	监控和评估企业网络安全保障措施的有效性，以确保其提供预期的保护级别。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
T0152	监控和维护数据库以确保最佳性能。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0152	监控和维护数据库以确保最佳性能。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
T0152	监控和维护数据库以确保最佳性能。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
T0152	监控和维护数据库以确保最佳性能。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0152	监控和维护数据库以确保最佳性能。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
T0152	监控和维护数据库以确保最佳性能。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0152	监控和维护数据库以确保最佳性能。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0152	监控和维护数据库以确保最佳性能。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
T0152	监控和维护数据库以确保最佳性能。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0152	监控和维护数据库以确保最佳性能。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
T0152	监控和维护数据库以确保最佳性能。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0152	监控和维护数据库以确保最佳性能。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0153	监控网络容量和性能。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
T0153	监控网络容量和性能。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
T0153	监控网络容量和性能。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
T0153	监控网络容量和性能。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
T0154	监控和报告知识管理资产和资源的使用情况。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
T0154	监控和报告知识管理资产和资源的使用情况。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
T0154	监控和报告知识管理资产和资源的使用情况。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
T0154	监控和报告知识管理资产和资源的使用情况。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
T0154	监控和报告知识管理资产和资源的使用情况。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
T0154	监控和报告知识管理资产和资源的使用情况。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
T0154	监控和报告知识管理资产和资源的使用情况。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
T0154	监控和报告知识管理资产和资源的使用情况。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
T0154	监控和报告知识管理资产和资源的使用情况。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
T0154	监控和报告知识管理资产和资源的使用情况。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
T0154	监控和报告知识管理资产和资源的使用情况。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0154	监控和报告知识管理资产和资源的使用情况。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
T0154	监控和报告知识管理资产和资源的使用情况。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
T0156	监督配置管理并提出建议。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
T0156	监督配置管理并提出建议。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
T0156	监督配置管理并提出建议。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
T0156	监督配置管理并提出建议。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
T0156	监督配置管理并提出建议。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
T0156	监督配置管理并提出建议。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
T0156	监督配置管理并提出建议。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
T0156	监督配置管理并提出建议。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
T0156	监督配置管理并提出建议。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
T0160	修补网络漏洞，确保信息免受外界侵害。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
T0160	修补网络漏洞，确保信息免受外界侵害。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
T0160	修补网络漏洞，确保信息免受外界侵害。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
T0162	对数据库执行备份和恢复以确保数据完整性。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0162	对数据库执行备份和恢复以确保数据完整性。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0162	对数据库执行备份和恢复以确保数据完整性。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0162	对数据库执行备份和恢复以确保数据完整性。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
T0162	对数据库执行备份和恢复以确保数据完整性。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
T0162	对数据库执行备份和恢复以确保数据完整性。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。
T0162	对数据库执行备份和恢复以确保数据完整性。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0162	对数据库执行备份和恢复以确保数据完整性。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
T0162	对数据库执行备份和恢复以确保数据完整性。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
T0162	对数据库执行备份和恢复以确保数据完整性。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
T0162	对数据库执行备份和恢复以确保数据完整性。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
T0162	对数据库执行备份和恢复以确保数据完整性。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
T0162	对数据库执行备份和恢复以确保数据完整性。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
T0162	对数据库执行备份和恢复以确保数据完整性。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
T0162	对数据库执行备份和恢复以确保数据完整性。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
T0166	使用从企业内部各种来源收集的信息进行事件关联，以获得态势感知并确定所观察到的攻击的有效性。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
T0168	与已建立的数据库进行哈希比较。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	opensearch-in-vpc-only	确保亚马逊 E AWS lasticsearch 服务 (Amazon ES) 域位于亚马逊虚拟私有云 (亚马逊 VPC) 中，从而管理对云的访问。Amazon VPC 中的 Amazon ES 域可实现 Amazon ES 与 Amazon VPC 中其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
T0195	根据任务要求提供受管理的相关信息流（通过基于 Web 的门户网站或其他方式）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
T0215	识别可能存在的安全违规行为，并根据需要采取适当措施报告事件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
T0244	验证应用程序软件/网络/系统安全态势是否按规定实施，记录偏差，并建议所需措施以纠正这些偏差。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
T0244	验证应用程序软件/网络/系统安全态势是否按规定实施，记录偏差，并建议所需措施以纠正这些偏差。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
T0244	验证应用程序软件/网络/系统安全态势是否按规定实施，记录偏差，并建议所需措施以纠正这些偏差。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
T0258	及时检测、识别可能的攻击/入侵、异常活动和滥用活动并发出警报，并将这些事件和活动与良性活动区分开来。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
T0259	使用网络防御工具持续监控和分析系统活动，以识别恶意活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如， defense-in-multiple 地点、分层防御、安全稳健性）。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如， defense-in-multiple 地点、分层防御、安全稳健性）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls （配置默认值：True）、blockPublicPolicy （配置默认值：True）和参数 blockPublicAcls （配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
T0262	采用经批准 defense-in-depth 的原则和实践（例如， defense-in-multiple 地点、分层防御、安全稳健性）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如， defense-in-multiple 地点、分层防御、安全稳健性）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	opensearch-in-vpc-only	确保亚马逊 E AWS lasticsearch 服务 (Amazon ES) 域位于亚马逊虚拟私有云 (亚马逊 VPC) 中，从而管理对云的访问。Amazon VPC 中的 Amazon ES 域可实现 Amazon ES 与 Amazon VPC 中其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0262	采用经批准 defense-in-depth 的原则和实践（例如，defense-in-multiple 地点、分层防御、安全稳健性）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如， defense-in-multiple 地点、分层防御、安全稳健性）。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
T0262	采用经批准 defense-in-depth 的原则和实践（例如， defense-in-multiple 地点、分层防御、安全稳健性）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
T0262	采用经批准 defense-in-depth 的原则和实践（例如， defense-in-multiple 地点、分层防御、安全稳健性）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
T0284	设计和开发与网络安全相关的新工具/技术。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
T0284	设计和开发与网络安全相关的新工具/技术。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
T0284	设计和开发与网络安全相关的新工具/技术。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
T0284	设计和开发与网络安全相关的新工具/技术。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
T0284	设计和开发与网络安全相关的新工具/技术。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
T0284	设计和开发与网络安全相关的新工具/技术。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
T0284	设计和开发与网络安全相关的新工具/技术。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
T0284	设计和开发与网络安全相关的新工具/技术。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
T0284	设计和开发与网络安全相关的新工具/技术。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
T0284	设计和开发与网络安全相关的新工具/技术。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
T0284	设计和开发与网络安全相关的新工具/技术。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
T0284	设计和开发与网络安全相关的新工具/技术。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
T0284	设计和开发与网络安全相关的新工具/技术。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0284	设计和开发与网络安全相关的新工具/技术。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
T0284	设计和开发与网络安全相关的新工具/技术。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
T0284	设计和开发与网络安全相关的新工具/技术。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0284	设计和开发与网络安全相关的新工具/技术。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0284	设计和开发与网络安全相关的新工具/技术。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
T0284	设计和开发与网络安全相关的新工具/技术。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
T0284	设计和开发与网络安全相关的新工具/技术。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
T0284	设计和开发与网络安全相关的新工具/技术。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	opensearch-in-vpc-only	确保亚马逊 E AWS lasticsearch 服务 (Amazon ES) 域位于亚马逊虚拟私有云 (亚马逊 VPC) 中，从而管理对云的访问。Amazon VPC 中的 Amazon ES 域可实现 Amazon ES 与 Amazon VPC 中其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。
T0284	设计和开发与网络安全相关的新工具/技术。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0284	设计和开发与网络安全相关的新工具/技术。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0284	设计和开发与网络安全相关的新工具/技术。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
T0284	设计和开发与网络安全相关的新工具/技术。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
T0284	设计和开发与网络安全相关的新工具/技术。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0284	设计和开发与网络安全相关的新工具/技术。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0284	设计和开发与网络安全相关的新工具/技术。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
T0284	设计和开发与网络安全相关的新工具/技术。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
T0284	设计和开发与网络安全相关的新工具/技术。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
T0306	支持事件管理、服务级别管理、变更管理、发布管理、连续性管理以及数据库和数据管理系统的可用性管理。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
T0306	支持事件管理、服务级别管理、变更管理、发布管理、连续性管理以及数据库和数据管理系统的可用性管理。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
T0306	支持事件管理、服务级别管理、变更管理、发布管理、连续性管理以及数据库和数据管理系统的可用性管理。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
T0314	根据适用的网络安全要求制定系统安全背景、初步的系统安全操作概念 (CONOPS)，并定义基准系统安全要求。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
T0314	根据适用的网络安全要求制定系统安全背景、初步的系统安全操作概念 (CONOPS)，并定义基准系统安全要求。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
T0314	根据适用的网络安全要求制定系统安全背景、初步的系统安全操作概念 (CONOPS)，并定义基准系统安全要求。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
T0314	根据适用的网络安全要求制定系统安全背景、初步的系统安全操作概念 (CONOPS)，并定义基准系统安全要求。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
T0314	根据适用的网络安全要求制定系统安全背景、初步的系统安全操作概念 (CONOPS)，并定义基准系统安全要求。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
T0314	根据适用的网络安全要求制定系统安全背景、初步的系统安全操作概念 (CONOPS)，并定义基准系统安全要求。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
T0333	执行网络防御趋势分析和报告。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
T0333	执行网络防御趋势分析和报告。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
T0347	评估源数据和后续发现的有效性。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
T0358	为特权访问用户设计和开发系统管理功能。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
T0358	为特权访问用户设计和开发系统管理功能。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0358	为特权访问用户设计和开发系统管理功能。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
T0358	为特权访问用户设计和开发系统管理功能。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
T0358	为特权访问用户设计和开发系统管理功能。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0358	为特权访问用户设计和开发系统管理功能。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0358	为特权访问用户设计和开发系统管理功能。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0358	为特权访问用户设计和开发系统管理功能。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
T0376	根据组织要求建立、实施和评估网络劳动力管理计划并为其配备资源。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0416	通过利用现有的公钥基础架构 (PKI) 库并在适当时加入证书管理和加密功能，为应用程序提供公钥。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
T0421	管理明确的组织知识（例如硬拷贝文档、数字文件）的索引/编目、存储和访问。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	opensearch-in-vpc-only	确保亚马逊 E AWS lasticsearch 服务 (Amazon ES) 域位于亚马逊虚拟私有云 (亚马逊 VPC) 中，从而管理对云的访问。Amazon VPC 中的 Amazon ES 域可实现 Amazon ES 与 Amazon VPC 中其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
T0475	根据最低权限原则评估适当的访问控制和 need-to-know.	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
T0489	按照既定程序实施系统安全措施，以确保机密性、完整性、可用性、身份验证和不可否认性。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
T0491	根据组织标准为系统用户安装和配置硬件、软件和外围设备。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
T0491	根据组织标准为系统用户安装和配置硬件、软件和外围设备。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
T0491	根据组织标准为系统用户安装和配置硬件、软件和外围设备。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
T0503	监控外部数据源（例如网络防御供应商站点、计算机应急响应小组、Security Focus），以了解网络防御威胁的最新情况，并确定哪些安全问题可能会对企业产生影响。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
T0509	执行信息安全风险评估。	annual-risk-assessment-performed（过程检查）	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	elasticsearch-node-to-node-encryption-check	确保已启用亚马逊 Elasticsearch Service 的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	opensearch-encrypted-at-rest	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elasticsearch Service (Amazon ES) 域启用了加密。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	opensearch-node-to-node-encryption-check	确保已启用亚马逊 Elasticsearch Service 的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	elasticsearch-encrypted-at-rest	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elasticsearch Service (Amazon ES) 域启用了加密。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
T0553	应用网络安全功能（例如加密、访问控制和身份管理）以减少漏洞利用机会。	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
T0557	集成与网络空间相关的关键管理功能。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后立即进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
T0557	集成与网络空间相关的关键管理功能。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
T0576	评估所有来源的情报并推荐目标以支持网络操作目标。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
T0609	对无线计算机和数字网络进行接入启用。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击
T0609	对无线计算机和数字网络进行接入启用。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
T0609	对无线计算机和数字网络进行接入启用。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
T0609	对无线计算机和数字网络进行接入启用。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
T0609	对无线计算机和数字网络进行接入启用。	elasticsearch-in-vpc-only	确保亚马逊 E AWS lasticsearch 服务 (Amazon ES) 域位于亚马逊虚拟私有云 (亚马逊 VPC) 中，从而管理对云的访问。Amazon VPC 中的 Amazon ES 域可实现 Amazon ES 与 Amazon VPC 中其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
T0609	对无线计算机和数字网络进行接入启用。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
T0609	对无线计算机和数字网络进行接入启用。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
T0609	对无线计算机和数字网络进行接入启用。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0609	对无线计算机和数字网络进行接入启用。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
T0609	对无线计算机和数字网络进行接入启用。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
T0609	对无线计算机和数字网络进行接入启用。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
T0609	对无线计算机和数字网络进行接入启用。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
T0609	对无线计算机和数字网络进行接入启用。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
T0609	对无线计算机和数字网络进行接入启用。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
T0609	对无线计算机和数字网络进行接入启用。	opensearch-in-vpc-only	确保亚马逊 E AWS lasticsearch 服务 (Amazon ES) 域位于亚马逊虚拟私有云 (亚马逊 VPC) 中，从而管理对云的访问。Amazon VPC 中的 Amazon ES 域可实现 Amazon ES 与 Amazon VPC 中其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
T0609	对无线计算机和数字网络进行接入启用。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
T0609	对无线计算机和数字网络进行接入启用。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
T0616	对网络中的系统进行网络侦察和漏洞分析。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
T0686	识别威胁漏洞。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
T0686	识别威胁漏洞。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	elasticsearch-logs-to-cloudwatch	确保 Amazon Elasticsearch 服务域启用错误日志，并将其流式传输到亚马逊 CloudWatch 日志以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired（配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired（配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
T0706	通过传统和替代技术（例如，社交网络分析、呼叫链接、流量分析）收集有关网络的信息。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
T0777	分析网络或系统管理员及其活动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
T0805	报告源自情报的重大网络事件和入侵。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
T0877	与适用的组织单位合作，监督消费者信息访问权	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
T0877	与适用的组织单位合作，监督消费者信息访问权	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
T0877	与适用的组织单位合作，监督消费者信息访问权	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
T0877	与适用的组织单位合作，监督消费者信息访问权	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0877	与适用的组织单位合作，监督消费者信息访问权	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
T0877	与适用的组织单位合作，监督消费者信息访问权	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
T0877	与适用的组织单位合作，监督消费者信息访问权	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
T0877	与适用的组织单位合作，监督消费者信息访问权	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0877	与适用的组织单位合作，监督消费者信息访问权	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0877	与适用的组织单位合作，监督消费者信息访问权	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
T0877	与适用的组织单位合作，监督消费者信息访问权	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
T0935	执行信息安全风险评估。	annual-risk-assessment-performed（过程检查）	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。
T0960	监控系统及其运行环境的变化。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。

控制 ID	控制描述	AWS Config 规则	指南
T0960	监控系统及其运行环境的变化。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
T0960	监控系统及其运行环境的变化。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
T0960	监控系统及其运行环境的变化。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。
T0960	监控系统及其运行环境的变化。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
T0960	监控系统及其运行环境的变化。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
T0960	监控系统及其运行环境的变化。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
T0960	监控系统及其运行环境的变化。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
T0992	确定持续监控结果将如何用于持续授权。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
T0992	确定持续监控结果将如何用于持续授权。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
T0992	确定持续监控结果将如何用于持续授权。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Managemen t (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatt erns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
T0992	确定持续监控结果将如何用于持续授权。	iam-group-has-users-check	AWS Identity and Access Managemen t (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0992	确定持续监控结果将如何用于持续授权。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0992	确定持续监控结果将如何用于持续授权。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
T0992	确定持续监控结果将如何用于持续授权。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
T0992	确定持续监控结果将如何用于持续授权。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
T0992	确定持续监控结果将如何用于持续授权。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
T0992	确定持续监控结果将如何用于持续授权。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
T0992	确定持续监控结果将如何用于持续授权。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
T0993	建立持续监控工具和技术访问控制流程及程序。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
T0993	建立持续监控工具和技术访问控制流程及程序。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
T0993	建立持续监控工具和技术访问控制流程及程序。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
T0993	建立持续监控工具和技术访问控制流程及程序。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

模板

该模板可在以下网址获得 GitHub：NIST 800 181 操作最佳实践。

NIST 1800 25 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了 NIST 1800-25 和托管 AWS Config 规则之间的映射示例。每个控件都 AWS Config 适用于特定的 AWS 资源，并与一个或多个 NIST 1800-25 控件相关。一个 NIST 1800-25 控件可以与多个规则相关联。 AWS Config 有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
ID.AM-2	清点组织内的软件平台和应用程序	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
ID.AM-2	清点组织内的软件平台和应用程序	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Syste

控制 ID	控制描述	AWS Config 规则	指南
			ms Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
ID.AM-2	清点组织内的软件平台和应用程序	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
ID.AM-2	清点组织内的软件平台和应用程序	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。

控制 ID	控制描述	AWS Config 规则	指南
ID.AM-2	清点组织内的软件平台和应用程序	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
ID.RA-1	识别并记录资产漏洞	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
ID.RA-1	识别并记录资产漏洞	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
ID.RA-1	识别并记录资产漏洞	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
ID.RA-1	识别并记录资产漏洞	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCreden tialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
PR.AC-3	远程访问受管理。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.AC-3	远程访问受管理。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
PR.AC-3	远程访问受管理。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.AC-3	远程访问受管理。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-3	远程访问受管理。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-3	远程访问受管理。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-3	远程访问受管理。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
PR.AC-3	远程访问受管理。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-3	远程访问受管理。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-3	远程访问受管理。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.AC-3	远程访问受管理。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-3	远程访问受管理。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-3	远程访问受管理。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
PR.AC-3	远程访问受管理。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
PR.DS-1	D ata-at-rest 受到保护	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
PR.DS-1	D ata-at-rest 受到保护	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
PR.DS-1	D ata-at-rest 受到保护	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
PR.DS-1	D ata-at-rest 受到保护	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
PR.DS-1	D ata-at-rest 受到保护	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
PR.DS-1	D ata-at-rest 受到保护	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-2	D ata-in-transit 受到保护	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-2	D ata-in-transit 受到保护	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
PR.DS-2	D ata-in-transit 受到保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-2	D ata-in-transit 受到保护	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-2	D ata-in-transit 受到保护	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-2	D ata-in-transit 受到保护	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-2	D ata-in-transit 受到保护	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
PR.DS-2	D ata-in-transit 受到保护	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-2	D ata-in-transit 受到保护	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-6	完整性检查机制用于验证软件、固件和信息的完整性	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
PR.DS-6	完整性检查机制用于验证软件、固件和信息的完整性	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-3	配置变更控制流程已到位	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
PR.IP-3	配置变更控制流程已到位	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
PR.IP-4	对信息进行备份，并维护和测试备份	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.IP-4	对信息进行备份，并维护和测试备份	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.IP-4	对信息进行备份，并维护和测试备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
PR.IP-4	对信息进行备份，并维护和测试备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
PR.IP-4	对信息进行备份，并维护和测试备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
PR.IP-4	对信息进行备份，并维护和测试备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
PR.IP-9	实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	response-plan-exists-maintained（流程检查）	确保制定和维护事件响应计划，并将其分发给负责人。更新并正式记录响应计划，有助于确保响应人员了解自己的角色、责任以及在事件发生时应遵循的流程。
PR.IP-10	对响应和恢复计划进行测试。	response-plan-tested（流程检查）	确保对事件响应和恢复计划进行测试。这有助于了解您的计划在事件期间是否有效，以及是否需要弥补任何不足或进行更新。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-12	制定并实施漏洞管理计划。	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。这可能包括漏洞管理工具、环境扫描节奏、角色和职责。
PR.IP-12	制定并实施漏洞管理计划	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-12	制定并实施漏洞管理计划	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
PR.IP-12	制定并实施漏洞管理计划	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
PR.MA-2	以防止未经授权访问的方式批准、记录和执行组织资产的远程维护	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
PR.MA-2	以防止未经授权访问的方式批准、记录和执行组织资产的远程维护	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
PR.PT-1	通信和控制网络受到保护	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
PR.PT-4	通信和控制网络受到保护	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.PT-4	通信和控制网络受到保护	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.PT-4	通信和控制网络受到保护	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
PR.PT-4	通信和控制网络受到保护	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-4	通信和控制网络受到保护	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-4	通信和控制网络受到保护	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-4	通信和控制网络受到保护	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
PR.PT-4	通信和控制网络受到保护	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.PT-4	通信和控制网络受到保护	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.PT-4	通信和控制网络受到保护	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.PT-4	通信和控制网络受到保护	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.PT-4	通信和控制网络受到保护	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.PT-4	通信和控制网络受到保护	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
PR.PT-4	通信和控制网络受到保护	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
DE.CM-8	执行漏洞扫描。	vuln-scans-performed（流程检查）	确保根据您的合规要求执行漏洞扫描。扫描节奏、使用的工具和结果的使用应由您的组织定义。

控制 ID	控制描述	AWS Config 规则	指南
RS.MI-3	新发现的漏洞会被缓解或记录为可接受的风险。	vuln-mitigated-accepted（流程检查）	确保新发现的漏洞得到补救或记录为可接受的风险。诸如 Sec AWS urity Hub、Amazon Guard Duty、Amazon Inspector 和 AWS Config 之类的服务可以帮助识别环境中的漏洞。应根据贵组织的合规要求对漏洞进行补救或将其作为风险接受。
RS.MI-3	新发现的漏洞会被缓解或记录为可接受的风险	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

模板

该模板可在以下网址获得 GitHub：NIST 1800 操作最佳实践 25。

NIST CSF 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下内容提供了 NIST 网络安全框架 (CSF) 和托管 C AWS onfig 规则之间的映射示例。每 AWS Config 条规则都适用于特定的 AWS 资源，并与一个或多个 NIST CSF 控制相关。一个 NIST CSF 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REG ION_CLOUD _TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此

控制 ID	控制描述	AWS Config 规则	指南
			外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
DE.AE-1	为用户和系统建立并管理网络运行和预期数据流的基准	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-2	分析检测到的事件以了解攻击目标和方法	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
DE.AE-2	分析检测到的事件以了解攻击目标和方法	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
DE.AE-3	从多个来源和传感器收集事件数据并进行关联	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-4	确定事件的影响	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
DE.AE-4	确定事件的影响	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
DE.AE-4	确定事件的影响	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-4	确定事件的影响	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
DE.AE-4	确定事件的影响	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-4	确定事件的影响	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-4	确定事件的影响	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
DE.AE-4	确定事件的影响	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
DE.CM-1	监控网络以检测潜在的网络安全事件	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
DE.CM-1	监控网络以检测潜在的网络安全事件	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-1	监控网络以检测潜在的网络安全事件	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
DE.CM-1	监控网络以检测潜在的网络安全事件	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
DE.CM-1	监控网络以检测潜在的网络安全事件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-1	监控网络以检测潜在的网络安全事件	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-1	监控网络以检测潜在的网络安全事件	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
DE.CM-1	监控网络以检测潜在的网络安全事件	s3-event-notifications-enabled	Amazon S3 事件通知可以提醒相关人员注意对您的存储桶对象的任何意外或故意修改。示例警报包括：创建了新对象、对象移除、对象恢复、丢失和复制的对象。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-1	监控网络以检测潜在的网络安全事件	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
DE.CM-1	监控网络以检测潜在的网络安全事件	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-3	监控人员活动以检测潜在的网络安全事件	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
DE.CM-3	监控人员活动以检测潜在的网络安全事件	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
DE.CM-3	监控人员活动以检测潜在的网络安全事件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-3	监控人员活动以检测潜在的网络安全事件	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-3	监控人员活动以检测潜在的网络安全事件	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-3	监控人员活动以检测潜在的网络安全事件	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
DE.CM-4	检测到恶意代码	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认：30）、 daysHighSev （配置默认值：7）和 （配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-4	检测到恶意代码	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
DE.CM-5	检测到未经授权的移动代码	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
DE.CM-5	检测到未经授权的移动代码	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-5	检测到未经授权的移动代码	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
DE.CM-5	检测到未经授权的移动代码	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-5	检测到未经授权的移动代码	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
DE.CM-5	检测到未经授权的移动代码	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-6	监控外部服务提供商的活动，以检测潜在的网络安全事件	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
DE.CM-6	监控外部服务提供商的活动，以检测潜在的网络安全事件	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
DE.CM-6	监控外部服务提供商的活动，以检测潜在的网络安全事件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-6	监控外部服务提供商的活动，以检测潜在的网络安全事件	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-6	监控外部服务提供商的活动，以检测潜在的网络安全事件	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-6	监控外部服务提供商的活动，以检测潜在的网络安全事件	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
DE.CM-7	监控未经授权的人员、连接、设备和软件	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
DE.CM-7	监控未经授权的人员、连接、设备和软件	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-7	监控未经授权的人员、连接、设备和软件	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
DE.CM-7	监控未经授权的人员、连接、设备和软件	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
DE.CM-7	监控未经授权的人员、连接、设备和软件	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-7	监控未经授权的人员、连接、设备和软件	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-7	监控未经授权的人员、连接、设备和软件	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
DE.CM-7	监控未经授权的人员、连接、设备和软件	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
DE.CM-7	监控未经授权的人员、连接、设备和软件	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
DE.DP-4	传达事件检测信息	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
DE.DP-4	传达事件检测信息	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
DE.DP-4	传达事件检测信息	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
DE.DP-4	传达事件检测信息	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
DE.DP-4	传达事件检测信息	s3-event-notifications-enabled	Amazon S3 事件通知可以提醒相关人员注意对您的存储桶对象的任何意外或故意修改。示例警报包括：创建了新对象、对象移除、对象恢复、丢失和复制的对象。

控制 ID	控制描述	AWS Config 规则	指南
DE.DP-4	传达事件检测信息	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
DE.DP-4	传达事件检测信息	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
DE.DP-5	检测过程不断改进	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
ID.AM-2	清点组织内的软件平台和应用程序	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
ID.AM-2	清点组织内的软件平台和应用程序	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
ID.AM-2	清点组织内的软件平台和应用程序	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
ID.AM-2	清点组织内的软件平台和应用程序	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。

控制 ID	控制描述	AWS Config 规则	指南
ID.AM-2	清点组织内的软件平台和应用程序	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
ID.AM-3	制定组织沟通和数据流图	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
ID.AM-3	制定组织沟通和数据流图	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
ID.AM-3	制定组织沟通和数据流图	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
ID.AM-3	制定组织沟通和数据流图	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
ID.AM-3	制定组织沟通和数据流图	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
ID.AM-3	制定组织沟通和数据流图	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
ID.AM-3	制定组织沟通和数据流图	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
ID.BE-5	为所有运营状态制定了支持提供关键服务的复原力要求（例如，在胁迫/攻击下、恢复期间、正常运营）	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
ID.RA-1	识别并记录资产漏洞	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
ID.RA-1	识别并记录资产漏洞	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
ID.RA-1	识别并记录资产漏洞	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
ID.RA-1	识别并记录资产漏洞	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
ID.RA-2	网络威胁情报来自信息共享论坛和来源	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
ID.RA-3	识别和记录内部和外部威胁	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
ID.RA-3	识别和记录内部和外部威胁	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
ID.RA-5	使用威胁、漏洞、可能性和影响来确定风险	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
ID.RA-5	使用威胁、漏洞、可能性和影响来确定风险	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
ID.RA-5	使用威胁、漏洞、可能性和影响来确定风险	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
ID.RA-5	使用威胁、漏洞、可能性和影响来确定风险	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
ID.SC-4	定期使用审计、测试结果或其他形式的评估对供应商和第三方合作伙伴进行评估，以确认他们履行了合同义务。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
ID.SC-4	定期使用审计、测试结果或其他形式的评估对供应商和第三方合作伙伴进行评估，以确认他们履行了合同义务。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
ID.SC-4	定期使用审计、测试结果或其他形式的评估对供应商和第三方合作伙伴进行评估，以确认他们履行了合同义务。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
ID.SC-4	定期使用审计、测试结果或其他形式的评估对供应商和第三方合作伙伴进行评估，以确认他们履行了合同义务。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-1	针对授权设备、用户和流程签发、管理、验证、吊销并审计身份和凭证	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
PR.AC-3	远程访问受管理。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
PR.AC-3	远程访问受管理。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
PR.AC-3	远程访问受管理。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-3	远程访问受管理。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-3	远程访问受管理。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-3	远程访问受管理。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
PR.AC-3	远程访问受管理。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-3	远程访问受管理。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-3	远程访问受管理。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.AC-3	远程访问受管理。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-3	远程访问受管理。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-3	远程访问受管理。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
PR.AC-3	远程访问受管理。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-3	远程访问受管理。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-4	管理访问权限和授权，采用最低权限和职责分离原则	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
PR.AC-5	网络完整性受到保护（例如，网络隔离、网络分段）	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-6	身份得到证明，与凭证绑定，并在互动中得到确认	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-6	身份得到证明，与凭证绑定，并在互动中得到确认	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-7	对用户、设备和其他资产进行身份验证（例如，单因素、多因素），与交易风险（例如，个人的安全和隐私风险以及其他组织风险）相称	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-7	对用户、设备和其他资产进行身份验证（例如，单因素、多因素），与交易风险（例如，个人的安全和隐私风险以及其他组织风险）相称	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
PR.AC-7	对用户、设备和其他资产进行身份验证（例如，单因素、多因素），与交易风险（例如，个人的安全和隐私风险以及其他组织风险）相称	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
PR.AC-7	对用户、设备和其他资产进行身份验证（例如，单因素、多因素），与交易风险（例如，个人的安全和隐私风险以及其他组织风险）相称	root-account-hardware-mfa-enabled	确保为根用户启用硬件 MFA，从而管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-7	对用户、设备和其他资产进行身份验证（例如，单因素、多因素），与交易风险（例如，个人的安全和隐私风险以及其他组织风险）相称	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
PR.AT-1	告知所有用户并对其进行培训	security-awareness-program-exists （过程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
PR.DS-1	D ata-at-rest 受到保护	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail跟踪启用了加密。
PR.DS-1	D ata-at-rest 受到保护	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
PR.DS-1	D ata-at-rest 受到保护	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
PR.DS-1	D ata-at-rest 受到保护	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
PR.DS-1	D ata-at-rest 受到保护	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	redshift-cluster-c onfiguration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
PR.DS-1	D ata-at-rest 受到保护	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-1	D ata-at-rest 受到保护	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-2	D ata-in-transit 受到保护	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-2	D ata-in-transit 受到保护	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-2	D ata-in-transit 受到保护	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-2	D ata-in-transit 受到保护	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-2	D ata-in-transit 受到保护	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-2	D ata-in-transit 受到保护	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
PR.DS-2	D ata-in-transit 受到保护	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
PR.DS-2	D ata-in-transit 受到保护	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-2	D ata-in-transit 受到保护	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-3	资产在拆除、转移和处置过程中得到正式管理	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-3	资产在拆除、转移和处置过程中得到正式管理	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
PR.DS-3	资产在拆除、转移和处置过程中得到正式管理	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-4	保持足够的容量以确保可用性	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.DS-4	保持足够的容量以确保可用性	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-4	保持足够的容量以确保可用性	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.DS-4	保持足够的容量以确保可用性	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-4	保持足够的容量以确保可用性	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
PR.DS-4	保持足够的容量以确保可用性	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-4	保持足够的容量以确保可用性	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
PR.DS-4	保持足够的容量以确保可用性	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-4	保持足够的容量以确保可用性	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
PR.DS-4	保持足够的容量以确保可用性	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
PR.DS-4	保持足够的容量以确保可用性	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-4	保持足够的容量以确保可用性	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
PR.DS-4	保持足够的容量以确保可用性	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-4	保持足够的容量以确保可用性	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
PR.DS-4	保持足够的容量以确保可用性	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-4	保持足够的容量以确保可用性	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
PR.DS-4	保持足够的容量以确保可用性	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
PR.DS-5	实施了防止数据泄露的保护措施	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
PR.DS-5	实施了防止数据泄露的保护措施	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
PR.DS-5	实施了防止数据泄露的保护措施	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
PR.DS-5	实施了防止数据泄露的保护措施	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
PR.DS-5	实施了防止数据泄露的保护措施	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.DS-5	实施了防止数据泄露的保护措施	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.DS-5	实施了防止数据泄露的保护措施	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
PR.DS-5	实施了防止数据泄露的保护措施	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.DS-5	实施了防止数据泄露的保护措施	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.DS-5	实施了防止数据泄露的保护措施	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
PR.DS-5	实施了防止数据泄露的保护措施	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-5	实施了防止数据泄露的保护措施	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.DS-5	实施了防止数据泄露的保护措施	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.DS-5	实施了防止数据泄露的保护措施	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-6	完整性检查机制用于验证软件、固件和信息的完整性	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
PR.DS-6	完整性检查机制用于验证软件、固件和信息的完整性	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-7	开发和测试环境与生产环境是分开的	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
PR.DS-7	开发和测试环境与生产环境是分开的	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-7	开发和测试环境与生产环境是分开的	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
PR.DS-7	开发和测试环境与生产环境是分开的	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
PR.DS-7	开发和测试环境与生产环境是分开的	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-7	开发和测试环境与生产环境是分开的	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-1	创建和维护信息技术/工业控制系统的基准配置，其中包含安全原则（例如功能最少的概念）	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
PR.IP-2	实施了用于管理系统的系统开发生命周期	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-2	实施了用于管理系统的系统开发生命周期	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub
PR.IP-2	实施了用于管理系统的系统开发生命周期	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
PR.IP-3	配置变更控制流程已到位	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-3	配置变更控制流程已到位	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
PR.IP-4	对信息进行备份，并维护和测试备份	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.IP-4	对信息进行备份，并维护和测试备份	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.IP-4	对信息进行备份，并维护和测试备份	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
PR.IP-4	对信息进行备份，并维护和测试备份	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
PR.IP-4	对信息进行备份，并维护和测试备份	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
PR.IP-4	对信息进行备份，并维护和测试备份	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-4	对信息进行备份，并维护和测试备份	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
PR.IP-7	保护流程得到改进	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
PR.IP-8	保护技术的有效性是共享的	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-8	保护技术的有效性是共享的	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.IP-8	保护技术的有效性是共享的	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.IP-8	保护技术的有效性是共享的	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.IP-8	保护技术的有效性是共享的	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-8	保护技术的有效性是共享的	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.IP-8	保护技术的有效性是共享的	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.IP-8	保护技术的有效性是共享的	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-8	保护技术的有效性是共享的	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
PR.IP-8	保护技术的有效性是共享的	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.IP-8	保护技术的有效性是共享的	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-8	保护技术的有效性是共享的	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.IP-8	保护技术的有效性是共享的	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-12	制定并实施漏洞管理计划	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
PR.IP-12	制定并实施漏洞管理计划	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
PR.IP-12	制定并实施漏洞管理计划	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
PR.MA-2	以防止未经授权访问的方式批准、记录和执行组织资产的远程维护	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
PR.MA-2	以防止未经授权访问的方式批准、记录和执行组织资产的远程维护	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
PR.PT-1	通信和控制网络受到保护	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细信息包括访问 Amazon S3 存储桶的 AWS 账户信息、IP 地址和事件时间。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
PR.PT-1	根据政策确定、记录、实施和审查审计/日志记录	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
PR.PT-4	通信和控制网络受到保护	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.PT-4	通信和控制网络受到保护	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.PT-4	通信和控制网络受到保护	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
PR.PT-4	通信和控制网络受到保护	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-4	通信和控制网络受到保护	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-4	通信和控制网络受到保护	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-4	通信和控制网络受到保护	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
PR.PT-4	通信和控制网络受到保护	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.PT-4	通信和控制网络受到保护	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.PT-4	通信和控制网络受到保护	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.PT-4	通信和控制网络受到保护	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.PT-4	通信和控制网络受到保护	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.PT-4	通信和控制网络受到保护	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-4	通信和控制网络受到保护	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
PR.PT-4	通信和控制网络受到保护	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-5	实施机制（例如故障安全、负载平衡、热交换），以满足正常和不利情况下的弹性要求	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
PR.PT-5	实施机制（例如故障保护、负载平衡、热交换）以满足正常和不利情况下的弹性要求	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-5	实施机制（例如故障保护、负载平衡、热交换）以满足正常和不利情况下的弹性要求	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
PR.PT-5	实施机制（例如故障保护、负载平衡、热交换）以满足正常和不利情况下的弹性要求	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
RC.RP-1	恢复计划在网络安全事件发生期间或之后执行	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
RS.AN-2	事件的影响已为人所知	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
RS.MI-3	新发现的漏洞会被缓解或记录为可接受的风险	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
RS.RP-1	响应计划在事件发生期间或之后执行	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RS.RP-1	响应计划在事件发生期间或之后执行	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
RS.RP-1	响应计划在事件发生期间或之后执行	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
RS.RP-1	响应计划在事件发生期间或之后执行	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
RS.RP-1	响应计划在事件发生期间或之后执行	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
RS.RP-1	响应计划在事件发生期间或之后执行	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
RS.RP-1	响应计划在事件发生期间或之后执行	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RS.RP-1	响应计划在事件发生期间或之后执行	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
RS.RP-1	响应计划在事件发生期间或之后执行	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RS.RP-1	响应计划在事件发生期间或之后执行	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RS.RP-1	响应计划在事件发生期间或之后执行	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
RS.RP-1	响应计划在事件发生期间或之后执行	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
RS.RP-1	响应计划在事件发生期间或之后执行	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
RS.RP-1	响应计划在事件发生期间或之后执行	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
RS.RP-1	响应计划在事件发生期间或之后执行	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
RS.RP-1	响应计划在事件发生期间或之后执行	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
RS.RP-1	响应计划在事件发生期间或之后执行	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
RS.RP-1	响应计划在事件发生期间或之后执行	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
RS.RP-1	响应计划在事件发生期间或之后执行	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
RS.RP-1	响应计划在事件发生期间或之后执行	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

模板

该模板可在以下网址获得 GitHub：NIST CSF 操作最佳实践。

NIST 隐私框架 v1.0 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

下面提供了 NIST 隐私框架和 AWS 托管 Config 规则之间的映射示例。每 AWS Config 条规则适用于特定 AWS 资源，并与一个或多个 NIST 隐私框架控件相关。NIST 隐私框架控件可以与多个 AWS Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P7	建立并实施了传输处理权限和相关数据值与数据元素的机制。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CT.DM-P7	建立并实施了传输处理权限和相关数据值与数据元素的机制。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
CT.DM-P7	建立并实施了传输处理权限和相关数据值与数据元素的机制。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚

控制 ID	控制描述	AWS Config 规则	指南
			马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CT.DM-P7	建立并实施了传输处理权限和相关数据值与数据元素的机制。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CT.DM-P7	建立并实施了传输处理权限和相关数据值与数据元素的机制。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P7	建立并实施了传输处理权限和相关数据值与数据元素的机制。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
CT.DM-P7	建立并实施了传输处理权限和相关数据值与数据元素的机制。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CT.DM-P7	建立并实施了传输处理权限和相关数据值与数据元素的机制。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P7	建立并实施了传输处理权限和相关数据值与数据元素的机制。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	audit-log-policy-exists（流程检查）	制定并维护审计日志管理策略，以定义贵组织的日志记录要求。这包括但不限于审查和保留审计日志。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage（配置默认值：80）参数。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
CT.DM-P8	审计/日志记录是根据策略确定、记录、实施和审查的，并纳入数据最小化原则。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
ID.DE-P2	使用隐私风险评估流程对数据处理生态系统各方（例如服务提供商、客户、合作伙伴、产品制造商、应用程序开发商）进行识别、优先排序和评估。	annual-risk-assessment-performed（流程检查）	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P1	针对授权个人、流程和设备签发、管理、验证、吊销并审计身份和凭证。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.AC-P3	远程访问受管理。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-P3	远程访问受管理。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-P3	远程访问受管理。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-P3	远程访问受管理。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-P3	远程访问受管理。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
PR.AC-P3	远程访问受管理。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
PR.AC-P3	远程访问受管理。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-P3	远程访问受管理。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-P3	远程访问受管理。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.AC-P3	远程访问受管理。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-P3	远程访问受管理。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-P3	远程访问受管理。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.AC-P3	远程访问受管理。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
PR.AC-P3	远程访问受管理。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
PR.AC-P3	远程访问受管理。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P3	远程访问受管理。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P4	管理访问权限和授权，采用最低权限和职责分离原则。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P5	网络完整性受到保护（例如，网络隔离、网络分段）。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P6	个人和设备经过验证并绑定凭证，并根据交易风险（例如，个人的安全和隐私风险以及其他组织风险）进行身份验证。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P6	个人和设备经过验证并绑定凭证，并根据交易风险（例如，个人的安全和隐私风险以及其他组织风险）进行身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
PR.AC-P6	个人和设备经过验证并绑定凭证，并根据交易风险（例如，个人的安全和隐私风险以及其他组织风险）进行身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
PR.AC-P6	个人和设备经过验证并绑定凭证，并根据交易风险（例如，个人的安全和隐私风险以及其他组织风险）进行身份验证。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
PR.AC-P6	个人和设备经过验证并绑定凭证，并根据交易风险（例如，个人的安全和隐私风险以及其他组织风险）进行身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
PR.DS-P1	D ata-at-rest 受到保护。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-P1	D ata-at-rest 受到保护。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P1	D ata-at-rest 受到保护。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
PR.DS-P1	D ata-at-rest 受到保护。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-P1	D ata-at-rest 受到保护。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
PR.DS-P1	D ata-at-rest 受到保护。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P1	D ata-at-rest 受到保护。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
PR.DS-P1	D ata-at-rest 受到保护。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-P1	D ata-at-rest 受到保护。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P1	D ata-at-rest 受到保护。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-P1	D ata-at-rest 受到保护。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P1	D ata-at-rest 受到保护。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
PR.DS-P1	D ata-at-rest 受到保护。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P1	D ata-at-rest 受到保护。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
PR.DS-P1	D ata-at-rest 受到保护。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-P1	D ata-at-rest 受到保护。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P1	D ata-at-rest 受到保护。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
PR.DS-P1	D ata-at-rest 受到保护。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P1	D ata-at-rest 受到保护。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
PR.DS-P2	D ata-in-transit 受到保护。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-P2	D ata-in-transit 受到保护。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P2	D ata-in-transit 受到保护。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
PR.DS-P2	D ata-in-transit 受到保护。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
PR.DS-P2	D ata-in-transit 受到保护。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
PR.DS-P4	保持足够的容量以确保可用性。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
PR.DS-P4	保持足够的容量以确保可用性。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
PR.DS-P4	保持足够的容量以确保可用性。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
PR.DS-P4	保持足够的容量以确保可用性。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.DS-P4	保持足够的容量以确保可用性。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.DS-P4	保持足够的容量以确保可用性。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.DS-P4	保持足够的容量以确保可用性。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.DS-P4	保持足够的容量以确保可用性。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
PR.DS-P4	保持足够的容量以确保可用性。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
PR.DS-P4	保持足够的容量以确保可用性。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
PR.DS-P4	保持足够的容量以确保可用性。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
PR.DS-P4	保持足够的容量以确保可用性。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P4	保持足够的容量以确保可用性。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.DS-P4	保持足够的容量以确保可用性。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.DS-P5	实施了防止数据泄露的保护措施。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P5	实施了防止数据泄露的保护措施。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
PR.DS-P5	实施了防止数据泄露的保护措施。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
PR.DS-P5	实施了防止数据泄露的保护措施。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P5	实施了防止数据泄露的保护措施。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.DS-P5	实施了防止数据泄露的保护措施。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.DS-P5	实施了防止数据泄露的保护措施。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P5	实施了防止数据泄露的保护措施。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.DS-P5	实施了防止数据泄露的保护措施。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P5	实施了防止数据泄露的保护措施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
PR.DS-P5	实施了防止数据泄露的保护措施。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
PR.DS-P5	实施了防止数据泄露的保护措施。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P5	实施了防止数据泄露的保护措施。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.DS-P5	实施了防止数据泄露的保护措施。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P5	实施了防止数据泄露的保护措施。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.DS-P5	实施了防止数据泄露的保护措施。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P5	实施了防止数据泄露的保护措施。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
PR.DS-P5	实施了防止数据泄露的保护措施。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.DS-P5	实施了防止数据泄露的保护措施。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P5	实施了防止数据泄露的保护措施。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.DS-P5	实施了防止数据泄露的保护措施。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.DS-P5	实施了防止数据泄露的保护措施。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.DS-P5	实施了防止数据泄露的保护措施。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
PR.DS-P6	完整性检查机制用于验证软件、固件和信息的完整性。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
PR.MA-P2	以防止未经授权访问的方式批准、记录和执行组织资产的远程维护。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
PR.MA-P2	以防止未经授权访问的方式批准、记录和执行组织资产的远程维护。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
PR.PO-P1	创建和维护信息技术的基准配置，其中包含安全原则（例如，功能最少的概念）。	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P1	创建和维护信息技术的基准配置，其中包含安全原则（例如，功能最少的概念）。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
PR.PO-P1	创建和维护信息技术的基准配置，其中包含安全原则（例如，功能最少的概念）。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P1	创建和维护信息技术的基准配置，其中包含安全原则（例如，功能最少的概念）。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
PR.PO-P1	创建和维护信息技术的基准配置，其中包含安全原则（例如，功能最少的概念）。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
PR.PO-P1	创建和维护信息技术的基准配置，其中包含安全原则（例如，功能最少的概念）。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P1	创建和维护信息技术的基准配置，其中包含安全原则（例如，功能最少的概念）。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
PR.PO-P1	创建和维护信息技术的基准配置，其中包含安全原则（例如，功能最少的概念）。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
AT-1：PR.PO-P10	制定并实施漏洞管理计划。	vuln-management-plan-exists（流程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P2	已建立并实施配置变更控制流程。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
PR.PO-P2	已建立并实施配置变更控制流程。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
PR.PO-P3	对信息进行备份，并维护和测试备份。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P3	对信息进行备份，并维护和测试备份。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PO-P3	对信息进行备份，并维护和测试备份。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P3	对信息进行备份，并维护和测试备份。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PO-P3	对信息进行备份，并维护和测试备份。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P3	对信息进行备份，并维护和测试备份。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PO-P3	对信息进行备份，并维护和测试备份。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P3	对信息进行备份，并维护和测试备份。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PO-P3	对信息进行备份，并维护和测试备份。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P3	对信息进行备份，并维护和测试备份。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
PR.PO-P3	对信息进行备份，并维护和测试备份。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P3	对信息进行备份，并维护和测试备份。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
PR.PO-P3	对信息进行备份，并维护和测试备份。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P3	对信息进行备份，并维护和测试备份。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
PR.PO-P3	对信息进行备份，并维护和测试备份。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P3	对信息进行备份，并维护和测试备份。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
PR.PO-P3	对信息进行备份，并维护和测试备份。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P3	对信息进行备份，并维护和测试备份。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PO-P3	对信息进行备份，并维护和测试备份。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PO-P7	制定、实施和管理响应计划（事件响应和业务连续性）和恢复计划（事件恢复和灾难恢复）。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PO-P8	对响应和恢复计划进行测试。	response-plan-tested（流程检查）	确保对事件响应和恢复计划进行测试。这有助于了解您的计划在事件期间是否有效，以及是否需要弥补任何不足或进行更新。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
PR.PT-P2	通过将系统配置为仅提供基本功能，从而纳入最少功能原则。	redshift-enhanced-vpc-routing-enabled	增强型 VPC 路由会强制群集和数据存储库之间的所有 COPY 和 UNLOAD 流量都通过 Amazon VPC。然后，您可以使用安全组和网络访问控制列表等 VPC 功能，来保护网络流量。还可以使用 VPC 流日志来监控网络流量。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
PR.PT-P3	通信和控制网络受到保护。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-P3	通信和控制网络受到保护。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-P3	通信和控制网络受到保护。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-P3	通信和控制网络受到保护。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
PR.PT-P3	通信和控制网络受到保护。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
PR.PT-P3	通信和控制网络受到保护。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
PR.PT-P3	通信和控制网络受到保护。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
PR.PT-P3	通信和控制网络受到保护。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
PR.PT-P3	通信和控制网络受到保护。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
PR.PT-P3	通信和控制网络受到保护。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
PR.PT-P3	通信和控制网络受到保护。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
PR.PT-P3	通信和控制网络受到保护。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
PR.PT-P3	通信和控制网络受到保护。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
PR.PT-P3	通信和控制网络受到保护。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P3	通信和控制网络受到保护。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
PR.PT-P4	实施机制（例如故障保护、负载平衡、热交换），以满足正常和不利情况下的弹性要求。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

模板

该模板可在以下网址获得 GitHub：NIST 隐私框架操作最佳实践 v1.0。

NYDFS 23 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全

确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了纽约州金融服务部 (NYDFS) 对金融服务公司的网络安全要求 (23 NYCRR 500) 与托管 AWS Config 规则之间的映射示例。每 AWS Config 条规则都适用于特定的 AWS 资源，并与一个或多个美国 NYDFS 控制措施有关。一个美国 NYDFS 23 NYCRR 500 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用

控制 ID	控制描述	AWS Config 规则	指南
			静态加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
500.02(a)	(a) 网络安全计划。每个被涵盖实体均应维护网络安全计划，旨在保护被涵盖实体信息系统的机密性、完整性和可用性。	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Managemen t 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
500.02(b)(2)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(2) 使用防御性基础设施并实施政策和程序，保护所涵盖实体的信息系统以及存储在这些信息系统上的非公开信息免受未经授权的访问、使用或其他恶意行为的侵害。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
500.02(b)(3)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(3) 检测网络安全事件。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
500.02(b)(5)	(b) 网络安全计划应基于所涵盖实体的风险评估，旨在履行以下核心网络安全职能：(5) 从网络安全事件中恢复并恢复正常运营和服务。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
500.05	每个所涵盖实体的网络安全计划均应包括根据所涵盖实体的风险评估制定的监控和测试，旨在评估所涵盖实体网络安全计划的有效性。监控和测试应包括持续监控或定期渗透测试和漏洞评估。如果没有有效的持续监控或其他系统来持续检测信息系统中可能会产生或指示存在漏洞的变化，则所涵盖实体应：(a) 根据风险评估确定的相关已识别风险，每年对所涵盖实体的信息系统进行年度渗透测试；(b) 每半年进行一次漏洞评估，包括对信息系统进行任何系统性扫描或审查，以根据风险评估合理确定所涵盖实体信息系统中公开已知的网络安全漏洞。	vuln-management-plan-exists（过程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。

控制 ID	控制描述	AWS Config 规则	指南
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

控制 ID	控制描述	AWS Config 规则	指南
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	控制描述	AWS Config 规则	指南
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
500.06(b)	(b) 每个所涵盖实体均应将本部分第 500.06(a)(1) 款所要求的记录保存不少于五年，并应将本部分第 500.06(a)(2) 款所要求的记录保存不少于三年。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
500.06(a)	(a) 每个所涵盖实体均应在适用范围内根据其风险评估安全地维护系统：(1) 旨在重建足以支持所涵盖实体的正常运营和义务的重大金融交易；(2) 包括旨在检测和应对网络安全事件的审计跟踪记录，这些事件很有可能对所涵盖实体正常运营的任何重要部分造成重大损害。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	ecs-task-definition-user-for-host-mode-check	如果任务定义具有提升的权限，那是因为客户专门选择了这些配置。当任务定义启用了主机联网，但客户未选择使用提升权限时，此控制会检查权限是否意外提升。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
500.07	作为其网络安全计划的一部分，根据所涵盖实体的风险评估，每个所涵盖实体均应限制用户对提供非公开信息访问权限的信息系统的访问权限，并应定期审查此类访问权限。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
500.8(a)	(a) 每个所涵盖实体的网络安全计划均应包括书面程序、指导方针和标准，旨在确保对所涵盖实体使用的内部开发的应用程序使用安全的开发实践；还应包括用于评估、测评或测试所涵盖实体在所涵盖实体技术环境背景下使用的外部开发应用程序的安全性的程序。	codebuild-project-envvar-awscred-check	确保 Codebuild 项目环境中不存在身份验证凭据 AWS_ACCESS_KEY_ID 和 AWS_SECRET_ACCESS_KEY。AWS 不要以明文形式存储这些变量。以明文形式存储这些变量会导致意外的数据泄露和未经授权的访问。
500.8(a)	(a) 每个所涵盖实体的网络安全计划均应包括书面程序、指导方针和标准，旨在确保对所涵盖实体使用的内部开发的应用程序使用安全的开发实践；还应包括用于评估、测评或测试所涵盖实体在所涵盖实体技术环境背景下使用的外部开发应用程序的安全性的程序。	codebuild-project-source-repo-url-check	确保 GitHub 或 Bitbucket 源存储库网址不包含个人访问令牌，即 AWS Codebuild 项目环境中的登录凭证。使用 OAuth 代替个人访问令牌或登录凭证来授予访问或 Bitbucket 存储库的授权。 GitHub

控制 ID	控制描述	AWS Config 规则	指南
500.09	(a) 每个所涵盖实体均应定期对所涵盖实体的信息系统进行风险评估，以便为本部分所要求的网络安全计划的设计提供信息。应在合理必要时更新此类风险评估，以应对所涵盖实体信息系统、非公开信息或业务运营的变化。所涵盖实体的风险评估应允许修改控制措施，以应对技术发展和不断演变的威胁，并应考虑所涵盖实体业务运营中与网络安全、收集或存储的非公开信息、使用的信息系统以及保护非公开信息和信息系统的控制措施的可用性和有效性相关的特殊风险。	annual-risk-assessment-performed（过程检查）>	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。

控制 ID	控制描述	AWS Config 规则	指南
500.12	(a) 多重身份验证。根据其风险评估，每个所涵盖实体均应使用有效的控制措施，其中可能包括多重身份验证或基于风险的身份验证，以防止未经授权访问非公开信息或信息系统。(b) 除非所涵盖实体的 CISO 以书面形式批准使用合理等同或更安全的访问控制，否则任何从外部网络访问所涵盖实体内部网络的个人均应使用多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
500.12	(a) 多重身份验证。根据其风险评估，每个所涵盖实体均应使用有效的控制措施，其中可能包括多重身份验证或基于风险的身份验证，以防止未经授权访问非公开信息或信息系统。(b) 除非所涵盖实体的 CISO 以书面形式批准使用合理等同或更安全的访问控制，否则任何从外部网络访问所涵盖实体内部网络的个人均应使用多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
500.12	(a) 多重身份验证。根据其风险评估，每个所涵盖实体均应使用有效的控制措施，其中可能包括多重身份验证或基于风险的身份验证，以防止未经授权访问非公开信息或信息系统。(b) 除非所涵盖实体的 CISO 以书面形式批准使用合理等同或更安全的访问控制，否则任何从外部网络访问所涵盖实体内部网络的个人均应使用多重身份验证。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
500.12	(a) 多重身份验证。根据其风险评估，每个所涵盖实体均应使用有效的控制措施，其中可能包括多重身份验证或基于风险的身份验证，以防止未经授权访问非公开信息或信息系统。(b) 除非所涵盖实体的 CISO 以书面形式批准使用合理等同或更安全的访问控制，否则任何从外部网络访问所涵盖实体内部网络的个人均应使用多重身份验证。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
500.12	(a) 多重身份验证。根据其风险评估，每个所涵盖实体均应使用有效的控制措施，其中可能包括多重身份验证或基于风险的身份验证，以防止未经授权访问非公开信息或信息系统。(b) 除非所涵盖实体的 CISO 以书面形式批准使用合理等同或更安全的访问控制，否则任何从外部网络访问所涵盖实体内部网络的个人均应使用多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	cloudwatch-alarm-action-check	当某个指标在指定数量的评估周期内突破阈值时，Amazon 会发出 CloudWatch 警报。告警根据指标或表达式在多个时间段内相对于某阈值的值执行一项或多项操作。此规则需要 alarmActionRequired （配置默认值：True）、 insufficientDataAction必填项（配置默认值：True）、 okActionRequired （配置默认值：False）的值。实际值应反映您的环境的警报操作。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。

控制 ID	控制描述	AWS Config 规则	指南
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

控制 ID	控制描述	AWS Config 规则	指南
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	控制描述	AWS Config 规则	指南
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
500.14(a)	(a) 实施基于风险的政策、程序和控制措施，旨在监控授权用户的活动，并检测此类授权用户未经授权访问或使用或篡改非公开信息的行为。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
500.14(b)	作为其网络安全计划的一部分，每个所涵盖实体均应：(b) 定期为所有人员提供网络安全意识培训，这些培训经过更新，可反映所涵盖实体在其风险评估中发现的风险。	security-awareness-program-exists（过程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
500.15(a)	(a) 作为其网络安全计划的一部分，根据其风险评估，每个所涵盖实体均应实施包括加密在内的控制措施，以保护所涵盖实体持有或传输的非公开信息，无论这些信息是通过外部网络传输还是静态信息。	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
500.16	(a) 作为其网络安全计划的一部分，每个所涵盖实体均应制定书面事件响应计划，旨在迅速应对任何对所涵盖实体的信息系统的机密性、完整性或可用性或所涵盖实体业务或运营的任何方面的持续功能产生重大影响的网络安全事件，并从中恢复。	response-plan-exists-maintained（过程检查）	确保制定和维护事件响应计划，并将其分发给负责人。

模板

该模板可在以下网址获得 GitHub：NYDFS 运营最佳实践 23。

NZISM 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下是新西兰政府通信安全局 (GCSB)《信息安全手册》(NZISM) 2022-09 年版本 3.6 和 Managed Config 规则之间的映射示例。 AWS 每条 Config 规则都适用于特定 AWS 资源，并与一个或多个 NZISM 控件相关。一个 NZISM 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

该示例合规包模板包含与 NZISM 框架内控制措施的映射，NZISM 框架是保护性安全要求 (PSR) 框架不可分割的一部分，规定了新西兰政府对人员、信息和人身安全管理的期望。

NZISM 根据知识共享署名 4.0 新西兰许可证获得许可，网址为 https://creativecommons.org/licenses/by/4.0/。版权信息可在 NZISM 新西兰信息安全手册 | 法律、隐私和版权中找到。

控制 ID	AWS Config 规则	指南
1149	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
1149	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
1149	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。
1149	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有

控制 ID	AWS Config 规则	指南
		明确的读写权限，否则无法修改其文件系统。
1149	ec2-hardening-and-state-management（流程检查）	经过强化的 EC2 服务器映像生成过程和状态管理器关联配置为删除不需要的组件和服务，并安装反恶意软件和日志代理。
1661	cloudfront-default-root-object-configured	此控件检查 Amazon CloudFront 分配是否配置为返回默认根对象的特定对象。如果 CloudFront 发行版未配置默认根对象，则控件将失败。用户有时可能会请求分配的根 URL，而不是分配中的对象。发生这种情况时，指定默认根对象可以帮助您避免公开 Web 分配的内容。此规则必须应用于 us-east-1 区域。
1667	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
1667	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
1841	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
1841	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
1841	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
1841	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	AWS Config 规则	指南
1847	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1847	cloudfront-viewer-policy-https	此控件可检查 Amazon CloudFront 分配是否要求查看者直接使用 HTTPS 或是否使用重定向。如果将缓存行为 defaultCacheBehavior 或缓 ViewerProtocolPolicy 存行为设置为全部允许，则控件将失败。HTTPS (TLS) 可用于帮助防止潜在的攻击者使用 person-in-the-middle 或类似的攻击来窃听或操纵网络流量。只允许通过 HTTPS (TLS) 进行加密连接。此规则必须应用于 us-east-1 区域。
1847	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
1847	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1847	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
1858	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
1893	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCreden tialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
1893	federate-with-central-idp （流程检查）	需要访问 AWS 资源的员工身份通过与 SSO 联合的中央 IdP 进行身份验证。 AWS 在 3 次登录尝试失败后，集中 IdP 会锁定系统用户。
1946	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
1946	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
1998	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
1998	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
1998	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
2013 年	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	AWS Config 规则	指南
2013 年	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
2013 年	cloudfront-accesslogs-enabled	此控件检查 CloudFront 发行版上是否启用了服务器访问日志记录。如果未为分配启用访问日志记录，则控制失败。CloudFront 访问日志提供有关 CloudFront 收到的每个用户请求的详细信息。每个日志都包含诸如收到请求的日期和时间、发出请求的查看器的 IP 地址、请求的来源以及查看器请求的端口号等信息。这些日志对于安全和访问审计、取证调查等应用很有用。此规则必须应用于 us-east-1 区域。
2013 年	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	AWS Config 规则	指南
2013 年	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
2013 年	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
2022	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	AWS Config 规则	指南
2022	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
2028	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
2082	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。预生产环境可获得豁免。
2082	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
2082	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2082	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	AWS Config 规则	指南
2082	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
2082	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
2082	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
2082	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2082	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relationa l Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2082	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
2082	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2091	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2091	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2091	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2598	elb-custom-security-policy-ssl-check	为帮助保护传输中的数据，请确保您的经典 ElasticLoadBalancer SSL 侦听器使用自定义安全策略。这些策略可以提供各种高强度的加密算法，以帮助确保系统之间的加密网络通信。此规则要求您为 SSL 侦听器设置自定义安全策略。默认的安全策略是：Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256。
2600	elb-custom-security-policy-ssl-check	为帮助保护传输中的数据，请确保您的经典 ElasticLoadBalancer SSL 侦听器使用自定义安全策略。这些策略可以提供各种高强度的加密算法，以帮助确保系统之间的加密网络通信。此规则要求您为 SSL 侦听器设置自定义安全策略。默认的安全策略是：Protocol-TLSv1.2,ECDHE-ECDSA-AES128-GCM-SHA256。
2726	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
3021	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	AWS Config 规则	指南
3021	kms-cmk-for-each-data-classification（进程检查）	已为每种不同的数据分类定义了至少一个 KMS 客户主密钥 (CMK)，并使用这些 CMK 来加密存储在该分类下的所有数据。
3205	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
3449	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
3449	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。

控制 ID	AWS Config 规则	指南
3449	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
3451	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
3451	ec2-critical-security-patch-auto-approval（过程检查）	已在补丁管理器中配置了 Windows 和/或 Linux 的补丁基准，包括在发布后 2 天内自动批准关键安全补丁。
3452	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
3452	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
3452	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。
3453	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	AWS Config 规则	指南
3453	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
3562	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
3562	cloudfront-associated-with-waf	此控件检查 CloudFront 发行版是否与 AWS WAF 或 AWS WAFv2 Web ACL 相关联。如果分配未与 Web ACL 关联，则控制失败。 AWS WAF 是一种 Web 应用程序防火墙，可帮助保护 Web 应用程序和 API 免受攻击。通过它，您可以配置一组规则（称为 Web 访问控制列表，即 Web ACL），基于可自定义的 Web 安全规则以及您定义的条件，允许、阻止或统计 Web 请求。确保您的 CloudFront 发行版与 AWS WAF Web ACL 关联，以帮助保护其免受恶意攻击。此规则必须应用于 us-east-1 区域。
3562	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3562	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	AWS Config 规则	指南
3562	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
3562	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3562	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
3562	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
3562	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
3562	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
3562	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
3562	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3562	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3562	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
3562	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
3562	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
3562	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
3623	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
3623	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
3623	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3623	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
3815	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
3875	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3875	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
4333	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	AWS Config 规则	指南
4441	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
4441	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
4441	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
4441	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
4441	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
4441	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
4441	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
4445	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
4445	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
4829	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
4829	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	AWS Config 规则	指南
4829	rds-cluster-multi-az-enabled	Amazon Relational Database Service (Amazon RDS) 集群应启用多可用区复制，以帮助确保所存储数据的可用性。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
4829	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。
4838	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	AWS Config 规则	指南
4838	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
4838	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
4838	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
4838	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
4839	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
4839	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
4839	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
4839	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
4839	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4839	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
4839	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
4839	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4839	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
4839	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
4839	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
4839	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
4839	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
4839	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
4839	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
4839	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
4839	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
4849	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
4849	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
4849	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	AWS Config 规则	指南
4849	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
4849	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
4849	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	AWS Config 规则	指南
4849	rds-cluster-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
4849	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
4849	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
4849	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	AWS Config 规则	指南
4849	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
6843	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
6843	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户

控制 ID	AWS Config 规则	指南
6852	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
6852	federate-with-central-idp（流程检查）	需要访问 AWS 资源的员工身份通过与 SSO 联合的中央 IdP 进行身份验证。 AWS 在 3 次登录尝试失败后，集中 IdP 会锁定系统用户。
6860	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
6860	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。

控制 ID	AWS Config 规则	指南
6861	cloudtrail-security-trail-enabled	此规则通过检查是否启用了多个设置 AWS CloudTrail，有助于确保使用 AWS 推荐的安全最佳实践。其中包括使用日志加密、日志验证和 AWS CloudTrail 在多个区域启用。
6953	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
6953	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。AWS 账户
7436	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
7436	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
7436	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
7436	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
7437	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	AWS Config 规则	指南
7437	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
7437	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
7437	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	AWS Config 规则	指南
7466	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
7466	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
7466	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。
7466	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
7466	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
7466	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。
7466	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
7466	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
7466	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
7466	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	AWS Config 规则	指南
7466	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
7466	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
7466	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
7466	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
7466	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
7466	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
7466	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
7496	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	AWS Config 规则	指南
7496	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
7496	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrai l 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	AWS Config 规则	指南
7496	cloudfront-accesslogs-enabled	此控件检查 CloudFront 发行版上是否启用了服务器访问日志记录。如果未为分配启用访问日志记录，则控制失败。CloudFront 访问日志提供有关 CloudFront 收到的每个用户请求的详细信息。每个日志都包含诸如收到请求的日期和时间、发出请求的查看器的 IP 地址、请求的来源以及查看器请求的端口号等信息。这些日志对于安全和访问审计、取证调查等应用很有用。此规则必须应用于 us-east-1 区域。
7496	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
7496	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	AWS Config 规则	指南
7496	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
7496	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

模板

该模板可在以下网址获得 GitHub：NZISM 最佳运营实践。

PCI DSS 3.2.1 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了支付卡行业数据安全标准 (PCI DSS) 3.2.1 和托管 C AWS onfig 规则之间的映射示例。每 AWS Config 条规则适用于特定 AWS 资源，并与一个或多个 PCI DSS 控制相关。一个 PCI DSS 控制可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	alb-desync-mode-check	为了帮助保护应用程序免受 HTTP Desync 漏洞的影响，请确保在应用程序负载均衡器上启用 HTTP Desync 缓解模式。HTTP Desync 问题可能导致请求走私，并使您的应用程序容易受到请求队列或缓存中毒的影响。异步缓解模式包括“监控”、“防御”和“最严格”。默认模式是防御。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22

控制 ID	控制描述	AWS Config 规则	指南
			有助于限制远程访问。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
1.2.1	将入站和出站流量限制为持卡人数据环境所需的流量，并明确拒绝所有其他流量。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	alb-desync-mode-check	为了帮助保护应用程序免受 HTTP Desync 漏洞的影响，请确保在应用程序负载均衡器上启用 HTTP Desync 缓解模式。HTTP Desync 问题可能导致请求走私，并使您的应用程序容易受到请求队列或缓存中毒的影响。异步缓解模式包括“监控”、“防御”和“最严格”。默认模式是防御。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3	禁止互联网与持卡人数据环境中的任何系统组件之间的直接公共访问。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	alb-desync-mode-check	为了帮助保护应用程序免受 HTTP Desync 漏洞的影响，请确保在应用程序负载均衡器上启用 HTTP Desync 缓解模式。HTTP Desync 问题可能导致请求走私，并使您的应用程序容易受到请求队列或缓存中毒的影响。异步缓解模式包括“监控”、“防御”和“最严格”。默认模式是防御。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3.1	实施一个 DMZ，以将入站流量限制为仅提供授权的可公开访问服务、协议和端口的系统组件。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	alb-desync-mode-check	为了帮助保护应用程序免受 HTTP Desync 漏洞的影响，请确保在应用程序负载均衡器上启用 HTTP Desync 缓解模式。HTTP Desync 问题可能导致请求走私，并使您的应用程序容易受到请求队列或缓存中毒的影响。异步缓解模式包括“监控”、“防御”和“最严格”。默认模式是防御。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3.2	将入站互联网流量限制为 DMZ 中的 IP 地址。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	alb-desync-mode-check	为了帮助保护应用程序免受 HTTP Desync 漏洞的影响，请确保在应用程序负载均衡器上启用 HTTP Desync 缓解模式。HTTP Desync 问题可能导致请求走私，并使您的应用程序容易受到请求队列或缓存中毒的影响。异步缓解模式包括“监控”、“防御”和“最严格”。默认模式是防御。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3.4	不允许从持卡人数据环境到互联网的未经授权的出站流量。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	netfw-policy-rule-group-associated	AWS Network Firewall 策略定义了您的防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来过滤数据包和流量，并定义默认流量处理方式。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	netfw-stateless-rule-group-not-empty	AWS Network Firewall 规则组包含的规则定义您的防火墙如何处理您的 VPC 中的流量。防火墙策略中空的无状态规则组不会处理流量。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
1.3.6	将存储持卡人数据的系统组件（例如数据库）放置在与 DMZ 和其他不受信任的网络隔离的内部网络区域中。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
2.1	在网络上安装系统之前，始终更改供应商提供的默认设置，并删除或禁用不需要的默认账户。这适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统帐户、 point-of-sale (POS) 终端、支付应用程序、简单网络管理协议 (SNMP) 社区字符串等使用的密码）。	rds-cluster-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Relational Database Service (Amazon RDS) 数据库集群的攻击面。

控制 ID	控制描述	AWS Config 规则	指南
2.1	在网络上安装系统之前，始终更改供应商提供的默认设置，并删除或禁用不需要的默认账户。这适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统帐户、 point-of-sale (POS) 终端、支付应用程序、简单网络管理协议 (SNMP) 社区字符串等使用的密码）。	rds-instance-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Relational Database Service (Amazon RDS) 数据库实例的攻击面。
2.1	在网络上安装系统之前，始终更改供应商提供的默认设置，并删除或禁用不需要的默认账户。这适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统帐户、 point-of-sale (POS) 终端、支付应用程序、简单网络管理协议 (SNMP) 社区字符串等使用的密码）。	redshift-default-admin-check	由于默认用户名是众所周知的，因此更改默认用户名有助于缩小 Amazon Redshift 集群的攻击面。

控制 ID	控制描述	AWS Config 规则	指南
2.1	在网络上安装系统之前，始终更改供应商提供的默认设置，并删除或禁用不需要的默认账户。这适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统帐户、 point-of-sale (POS) 终端、支付应用程序、简单网络管理协议 (SNMP) 社区字符串等使用的密码）。	redshift-default-db-name-check	默认名称是众所周知的，应在配置时进行更改。更改 Amazon Redshift 集群的默认数据库名称有助于减少 Redshift 集群的攻击面。
2.1	在网络上安装系统之前，始终更改供应商提供的默认设置，并删除或禁用不需要的默认账户。这适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统帐户、 point-of-sale (POS) 终端、支付应用程序、简单网络管理协议 (SNMP) 社区字符串等使用的密码）。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
2.1	在网络上安装系统之前，始终更改供应商提供的默认设置，并删除或禁用不需要的默认账户。这适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统帐户、 point-of-sale (POS) 终端、支付应用程序、简单网络管理协议 (SNMP) 社区字符串等使用的密码）。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	ec2-instance-multiple-eni-check	此规则检查您的 Amazon Elastic Cloud (Amazon EC2) 实例是否有多个 ENI。拥有多个 ENI 可能会导致双宿主实例，即具有多个子网的实例。这可能会增加网络安全的复杂性，并引入意想不到的网络路径和访问。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。业界认可的系统强化标准的来源可能包括但不限于：“互联网安全中心 (CIS)” “国际标准化组织 (ISO)” “A SysAdmin 审计网络安全 (SANS) 研究所” “美国国家标准技术研究所 (NIST)”。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在用户名和密码之上增加了一层额外的防护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。业界认可的系统强化标准的来源可能包括但不限于：“互联网安全中心 (CIS)” “国际标准化组织 (ISO)” “A SysAdmin 审计网络安全 (SANS) 研究所” “美国国家标准技术研究所 (NIST)”。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
2.2	为所有系统组件制订配置标准。确保这些标准解决了所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。行业认可的系统强化标准的来源可能包括但不限于：• 互联网安全中心 (CIS) • 国际标准化组织 (ISO) • SysAdmin 审计网络安全 (SANS) 研究所 • 美国国家标准技术研究所 (NIST)。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
2.2.2	仅启用系统运行所必需的服务、协议、守护程序等。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
2.2.3	为任何被认为不安全的必需服务、协议或守护程序实施其他安全功能。	alb-desync-mode-check	为了帮助保护应用程序免受 HTTP Desync 漏洞的影响，请确保在应用程序负载均衡器上启用 HTTP Desync 缓解模式。HTTP Desync 问题可能导致请求走私，并使您的应用程序容易受到请求队列或缓存中毒的影响。异步缓解模式包括“监控”、“防御”和“最严格”。默认模式是防御。

控制 ID	控制描述	AWS Config 规则	指南
2.3	使用强大的加密技术对所有非控制台管理访问进行加密。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.3	使用强大的加密技术对所有非控制台管理访问进行加密。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
2.3	使用强大的加密技术对所有非控制台管理访问进行加密。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.3	使用强大的加密技术对所有非控制台管理访问进行加密。	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon OpenSearch 服务域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
2.3	使用强大的加密技术对所有非控制台管理访问进行加密。	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
2.4	保留 PCI DSS 范围内的系统组件的清单。	ec2-security-group-attached-to-eni-periodic	此规则可确保将安全组附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或 ENI。此规则有助于监控清单中未使用的安全组并管理您的环境。
2.4	保留 PCI DSS 范围内的系统组件的清单。	eip-attached	此规则可确保分配给 Amazon Virtual Private Cloud (Amazon VPC) 的弹性 IP 附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例或正在使用的弹性网络接口。此规则有助于监控您环境中未使用的 EIP。

控制 ID	控制描述	AWS Config 规则	指南
2.4	保留 PCI DSS 范围内的系统组件的清单。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
2.4	保留 PCI DSS 范围内的系统组件的清单。	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。

控制 ID	控制描述	AWS Config 规则	指南
3.1	对所有持卡人数据 (CHD) 的存储实施数据留存和处置政策、程序和流程，至少包括以下内容，从而将持卡人数据的存储量保持在最低水平：• 将数据存储量和保留时间限制在法律、监管和/或业务要求所需的范围内 • 对持卡人数据的特定保留要求 • 不再需要数据时安全删除数据的流程 • 识别和安全删除存储的超过规定保留期的持卡人数据的季度流程。	s3-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
3.1	对所有持卡人数据 (CHD) 的存储实施数据留存和处置政策、程序和流程，至少包括以下内容，从而将持卡人数据的存储量保持在最低水平：• 将数据存储量和保留时间限制在法律、监管和/或业务要求所需的范围内 • 对持卡人数据的特定保留要求 • 不再需要数据时安全删除数据的流程 • 识别和安全删除存储的超过规定保留期的持卡人数据的季度流程。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue （配置默认：1）、 requiredRetentionDays （配置默认值：35）和 requiredFrequencyUnit （配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
3.1	对所有持卡人数据 (CHD) 的存储实施数据留存和处置政策、程序和流程，至少包括以下内容，从而将持卡人数据的存储量保持在最低水平：• 将数据存储量和保留时间限制在法律、监管和/或业务要求所需的范围内 • 对持卡人数据的特定保留要求 • 不再需要数据时安全删除数据的流程 • 识别和安全删除存储的超过规定保留期的持卡人数据的季度流程。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays （配置默认值：35）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
3.1	对所有持卡人数据 (CHD) 的存储实施数据留存和处置政策、程序和流程，至少包括以下内容，从而将持卡人数据的存储量保持在最低水平：• 将数据存储量和保留时间限制在法律、监管和/或业务要求所需的范围内 • 对持卡人数据的特定保留要求 • 不再需要数据时安全删除数据的流程 • 识别和安全删除存储的超过规定保留期的持卡人数据的季度流程。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.4	使用以下任何一种方法，使 PAN 无论存储在任何地方（包括便携式数字媒体、备份媒体和日志中）都无法读取：• 基于强加密技术的单向散列（散列必须是整个 PAN 的散列）• 截断（不能使用散列来替换被截断的 PAN 部分）• 索引令牌和小键盘（小键盘必须安全存储）• 强加密技术以及相关的密钥管理过程和程序。注意：如果恶意个人可以同时访问截断和散列版本的 PAN，那么重建原始 PAN 数据的难度相对较小。如果实体环境中存在同一 PAN 的散列版本和截断版本，则必须设置其他控制措施，以确保散列版本和截断版本无法关联以重建原始 PAN。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.5.2	将加密密钥的访问权限限制在必要的最少保管人范围内。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略

控制 ID	控制描述	AWS Config 规则	指南
3.5.2	将加密密钥的访问权限限制在必要的最少保管人范围内。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.5.3	始终以以下一种（或多种）形式存储用于加密/解密持卡人数据的机密和私钥：• 使用密钥加密密钥加密，该密钥的强度至少与数据加密密钥相同，并且与数据加密密钥分开存储 • 在安全的加密设备中（例如硬件（主机）安全模块（HSM）或 PTS 批准的 point-of-interaction 设备）• 至少两个全长密钥组件或密钥共享，符合行业公认的方法注意：不要求将公钥存储在其中一个中这些表格。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.5.3	始终以以下一种（或多种）形式存储用于加密/解密持卡人数据的机密和私钥：• 使用密钥加密密钥加密，该密钥的强度至少与数据加密密钥相同，并且与数据加密密钥分开存储 • 在安全的加密设备中（例如硬件（主机）安全模块（HSM）或 PTS 批准的 point-of-interaction 设备）• 至少两个全长密钥组件或密钥共享，符合行业公认的方法注意：不要求将公钥存储在其中一个中这些表格。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.5.3	始终以以下一种（或多种）形式存储用于加密/解密持卡人数据的机密和私钥：• 使用密钥加密密钥加密，该密钥的强度至少与数据加密密钥相同，并且与数据加密密钥分开存储 • 在安全的加密设备中（例如硬件（主机）安全模块（HSM）或 PTS 批准的 point-of-interaction 设备）• 至少两个全长密钥组件或密钥共享，符合行业公认的方法注意：不要求将公钥存储在其中一个中这些表格。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
3.6.4	根据相关应用程序供应商或密钥所有者的定义，并基于行业最佳实践和指南（例如，NIST 专题出版物 800-57），在密钥有效期结束后（例如，在规定的时间过后和/或在特定密钥产生了一定量的密码文本后），更改密钥的加密密钥。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。

控制 ID	控制描述	AWS Config 规则	指南
3.6.5	当密钥的完整性被削弱（例如，知道明文密钥组件的员工离职）或怀疑密钥被泄露时，可以根据需要停用或更换（例如存档、销毁和/或撤销）密钥。注意：如果需要保留已停用或替换的加密密钥，则必须对这些密钥进行安全存档（例如，使用密钥加密密钥）。存档的加密密钥只能用于解密/验证目的。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
3.6.7	防止未经授权替换加密密钥。	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon OpenSearch 服务域的连接启用 HTTPS。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。Node-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
4.1	在通过开放式公共网络传输期间，使用强大的加密和安全协议来保护敏感的持卡人数据，包括：• 仅接受可信的密钥和证书。• 使用的协议仅支持安全版本或配置。• 加密强度适合所使用的加密方法。开放式公共网络的示例包括但不限于：• 互联网 • 无线技术，包括 802.11 和蓝牙 • 蜂窝技术，例如全球移动通信系统 (GSM)、码分多址 (CDMA) • 通用分组无线电服务 (GPRS) • 卫星通信	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
6.2	通过安装供应商提供的适用安全补丁，确保保护所有系统组件和软件以免受到已知漏洞的攻击。请在发布后的一个月内安装重要安全补丁。注意：关键安全补丁应根据要求 6.1 中定义的风险等级流程进行识别。	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。

控制 ID	控制描述	AWS Config 规则	指南
6.2	通过安装供应商提供的适用安全补丁，确保保护所有系统组件和软件以免受到已知漏洞的攻击。请在发布后的一个月内安装重要安全补丁。注意：关键安全补丁应根据要求 6.1 中定义的风险等级流程进行识别。	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
6.2	通过安装供应商提供的适用安全补丁，确保保护所有系统组件和软件以免受到已知漏洞的攻击。请在发布后的一个月内安装重要安全补丁。注意：关键安全补丁应根据要求 6.1 中定义的风险等级流程进行识别。	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
6.2	通过安装供应商提供的适用安全补丁，确保保护所有系统组件和软件以免受到已知漏洞的攻击。请在发布后的一个月内安装重要安全补丁。注意：关键安全补丁应根据要求 6.1 中定义的风险等级流程进行识别。	ecs-fargate-latest-platform-version	系统会自动为您的 AWS Fargate 任务部署安全更新和补丁。如果发现影响 AWS Fargate 平台版本的安全问题，请 AWS 修补平台版本。要协助对运行 AWS Fargate 的亚马逊弹性容器服务 (ECS) 任务进行补丁管理，请将您的服务独立任务更新为使用最新平台版本。
6.2	通过安装供应商提供的适用安全补丁，确保保护所有系统组件和软件以免受到已知漏洞的攻击。请在发布后的一个月内安装重要安全补丁。注意：关键安全补丁应根据要求 6.1 中定义的风险等级流程进行识别。	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
6.2	通过安装供应商提供的适用安全补丁，确保保护所有系统组件和软件以免受到已知漏洞的攻击。请在发布后的一个月内安装重要安全补丁。注意：关键安全补丁应根据要求 6.1 中定义的风险等级流程进行识别。	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
6.3.2	在向生产环境或客户发布之前，先审查自定义代码，以识别任何潜在的编码漏洞（使用手动或自动流程），至少应包括以下内容：• 代码更改由原始代码作者以外的个人以及了解代码审查技术和安全编码实践的个人进行审查。• 代码审查确保代码是根据安全编码指南开发的 • 在发布之前进行适当的更正。• 代码审查结果在发布前由管理层审查和批准。（接下一页）	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。

控制 ID	控制描述	AWS Config 规则	指南
6.6	对于面向公众的 Web 应用程序，持续解决新的威胁和漏洞，并通过以下任一方法确保这些应用程序免遭已知攻击：• 通过手动或自动应用程序漏洞安全评估工具或方法审查面向公众的 Web 应用程序，至少每年审查一次并在进行任何更改后审查。注意：此评估与针对要求 11.2 执行的漏洞扫描不同。• 在面向公众的 Web 应用程序前安装自动检测和防止基于 Web 的攻击的技术解决方案（例如 Web 应用程序防火墙），以持续检查所有流量。	alb-desync-mode-check	为了帮助保护应用程序免受 HTTP Desync 漏洞的影响，请确保在应用程序负载均衡器上启用 HTTP Desync 缓解模式。HTTP Desync 问题可能导致请求走私，并使您的应用程序容易受到请求队列或缓存中毒的影响。异步缓解模式包括“监控”、“防御”和“最严格”。默认模式是防御。

控制 ID	控制描述	AWS Config 规则	指南
6.6	对于面向公众的 Web 应用程序，持续解决新的威胁和漏洞，并通过以下任一方法确保这些应用程序免遭已知攻击：• 通过手动或自动应用程序漏洞安全评估工具或方法审查面向公众的 Web 应用程序，至少每年审查一次并在进行任何更改后审查。注意：此评估与针对要求 11.2 执行的漏洞扫描不同。• 在面向公众的 Web 应用程序前安装自动检测和防止基于 Web 的攻击的技术解决方案（例如 Web 应用程序防火墙），以持续检查所有流量。	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
6.6	对于面向公众的 Web 应用程序，持续解决新的威胁和漏洞，并通过以下任一方法确保这些应用程序免遭已知攻击：• 通过手动或自动应用程序漏洞安全评估工具或方法审查面向公众的 Web 应用程序，至少每年审查一次并在进行任何更改后审查。注意：此评估与针对要求 11.2 执行的漏洞扫描不同。• 在面向公众的 Web 应用程序前安装自动检测和防止基于 Web 的攻击的技术解决方案（例如 Web 应用程序防火墙），以持续检查所有流量。	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	控制描述	AWS Config 规则	指南
6.6	对于面向公众的 Web 应用程序，持续解决新的威胁和漏洞，并通过以下任一方法确保这些应用程序免遭已知攻击：• 通过手动或自动应用程序漏洞安全评估工具或方法审查面向公众的 Web 应用程序，至少每年审查一次并在进行任何更改后审查。注意：此评估与针对要求 11.2 执行的漏洞扫描不同。• 在面向公众的 Web 应用程序前安装自动检测和防止基于 Web 的攻击的技术解决方案（例如 Web 应用程序防火墙），以持续检查所有流量。	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。

控制 ID	控制描述	AWS Config 规则	指南
6.6	对于面向公众的 Web 应用程序，持续解决新的威胁和漏洞，并通过以下任一方法确保这些应用程序免遭已知攻击：• 通过手动或自动应用程序漏洞安全评估工具或方法审查面向公众的 Web 应用程序，至少每年审查一次并在进行任何更改后审查。注意：此评估与针对要求 11.2 执行的漏洞扫描不同。• 在面向公众的 Web 应用程序前安装自动检测和防止基于 Web 的攻击的技术解决方案（例如 Web 应用程序防火墙），以持续检查所有流量。	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。

控制 ID	控制描述	AWS Config 规则	指南
6.6	对于面向公众的 Web 应用程序，持续解决新的威胁和漏洞，并通过以下任一方法确保这些应用程序免遭已知攻击：• 通过手动或自动应用程序漏洞安全评估工具或方法审查面向公众的 Web 应用程序，至少每年审查一次并在进行任何更改后审查。注意：此评估与针对要求 11.2 执行的漏洞扫描不同。• 在面向公众的 Web 应用程序前安装自动检测和防止基于 Web 的攻击的技术解决方案（例如 Web 应用程序防火墙），以持续检查所有流量。	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。

控制 ID	控制描述	AWS Config 规则	指南
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。

控制 ID	控制描述	AWS Config 规则	指南
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

控制 ID	控制描述	AWS Config 规则	指南
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
7.1.1	定义每个角色的访问需求，包括：• 每个角色为履行其工作职能而需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）。	opensearch-access-control-enabled	确保在您的亚马逊 OpenSearch 服务域上启用精细访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch

控制 ID	控制描述	AWS Config 规则	指南
7.1.2	将对特权用户 ID 的访问权限限制为履行工作职责所需的最低权限。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
7.1.2	将对特权用户 ID 的访问权限限制为履行工作职责所需的最低权限。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
7.1.2	将对特权用户 ID 的访问权限限制为履行工作职责所需的最低权限。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
7.1.2	将对特权用户 ID 的访问权限限制为履行工作职责所需的最低权限。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
7.1.2	将对特权用户 ID 的访问权限限制为履行工作职责所需的最低权限。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.1.2	将对特权用户 ID 的访问权限限制为履行工作职责所需的最低权限。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.1.2	将对特权用户 ID 的访问权限限制为履行工作职责所需的最低权限。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
7.1.2	将对特权用户 ID 的访问权限限制为履行工作职责所需的最低权限。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.1.2	将对特权用户 ID 的访问权限限制为履行工作职责所需的最低权限。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	ecs-containers-nonprivileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。

控制 ID	控制描述	AWS Config 规则	指南
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

控制 ID	控制描述	AWS Config 规则	指南
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含“效果”：“允许”和“操作”：“*”而不是“资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
7.2.1	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。该访问控制系统必须包括以下内容：所有系统组件的涵盖范围	opensearch-access-control-enabled	确保在您的亚马逊 OpenSearch 服务域上启用精细访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	ecs-containers-non privileged	为了帮助实施最低权限原则，Amazon Elastic Container Service (Amazon ECS) 任务定义不应启用提升权限。在该参数为 true 时，将为该容器提供提升的主机容器实例权限（类似于根用户）。

控制 ID	控制描述	AWS Config 规则	指南
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	ecs-containers-readonly-access	启用对 Amazon Elastic Container Service (ECS) 容器的只读访问有助于遵守最低权限原则。此选项可以减少攻击载体，因为除非容器实例具有明确的读写权限，否则无法修改其文件系统。
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

控制 ID	控制描述	AWS Config 规则	指南
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。

控制 ID	控制描述	AWS Config 规则	指南
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt 实际值应反映贵组织的策略。
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含“效果”：“允许”和“操作”：“*”而不是“资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
7.2.2	为系统组件建立一个访问控制系统，以根据需要了解的内容限制访问并将其设置为“全部拒绝”，除非明确允许。此访问控制系统必须包括以下内容：根据职位分类和职能为个人分配权限。	opensearch-access-control-enabled	确保在您的亚马逊 OpenSearch 服务域上启用精细访问控制。精细的访问控制提供了增强的授权机制，以实现对 Amazon Service 域的最低权限访问。OpenSearch 它允许基于角色的域访问控制，以及索引、文档和字段级安全，支持 OpenSearch 服务仪表板多租户，以及对 Service 和 Kibana 的 HTTP 基本身份验证。OpenSearch
7.2.3	默认“全部拒绝”设置。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Managemen t。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。

控制 ID	控制描述	AWS Config 规则	指南
8.1.1	在允许所有用户访问系统组件或持卡人数据之前，为他们分配一个唯一的 ID。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
8.1.4	删除/禁用 90 天内不活跃的用户账户。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	codebuild-project-environment-privileged-check	要帮助实施最低权限原则，请确保您的 Amazon CodeBuild 项目环境未启用特权模式。应禁用此设置，以防止意外访问 Docker API 及容器的底层硬件。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	ecs-no-environment-secrets	作为安全最佳实践，请将敏感信息作为环境变量传递给容器。通过在 Amazon ECS 任务定义的容器定义中引用 Syst AWS ems Manager 参数存储或 S AWS ecrets Manager 中存储的值，您可以将数据安全地注入到您的亚马逊弹性容器服务 (ECS) 容器中。然后，您可以将敏感信息作为环境变量公开，或在容器的日志配置中公开。

控制 ID	控制描述	AWS Config 规则	指南
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	控制描述	AWS Config 规则	指南
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。

控制 ID	控制描述	AWS Config 规则	指南
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	sagemaker-endpoint-configuration-kms-key-configured	为了帮助保护静态数据，请确保您的 SageMaker 终端节点启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
8.2.1	通过使用强大的加密技术，使所有身份验证凭证（例如密码/短语）在所有系统组件上传输和存储期间不可读。	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
8.2.3	密码/口令必须满足以下条件：• 要求长度至少为七个字符。• 同时包含数字和字母字符。或者，密码/口令的复杂性和强度必须至少等同于上面指定的参数。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为 IAM 密码策略设置 RequireUppercaseCharacters（PCI DSS 默认值：false）、 RequireLowercaseCharacters（PCI DSS 默认值：真）、 RequireSymbols（PCI DSS 默认值：假）、RequireNumbers（PCI DSS 默认值：true）、 MinimumPasswordLength（PCI DSS 默认值：7）、（PCI DSS 默认值：4）和 PasswordReusePrevention MaxPasswordAge（PCI DSS 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.2.4	至少每 90 天更改一次用户密码/密码。	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.2.4	至少每 90 天更改一次用户密码/密码。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为 IAM 密码策略设置 RequireUppercaseCharacters（PCI DSS 默认值：false）、 RequireLowercaseCharacters（PCI DSS 默认值：真）、 RequireSymbols（PCI DSS 默认值：假）、RequireNumbers（PCI DSS 默认值：true）、 MinimumPasswordLength（PCI DSS 默认值：7）、（PCI DSS 默认值：4）和 PasswordReusePrevention MaxPasswordAge（PCI DSS 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.2.4	至少每 90 天更改一次用户密码/密码。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
8.2.5	不允许个人提交与他或她最近使用的四个密码/口令中的任何一个相同的新密码/口令。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为 IAM 密码策略设置 RequireUppercaseCharacters（PCI DSS 默认值：false）、 RequireLowercaseCharacters（PCI DSS 默认值：真）、 RequireSymbols（PCI DSS 默认值：假）、RequireNumbers（PCI DSS 默认值：true）、 MinimumPasswordLength（PCI DSS 默认值：7）、（PCI DSS 默认值：4）和 PasswordReusePrevention MaxPasswordAge（PCI DSS 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.3.1	将所有非控制台访问的多重身份验证加入具有管理访问权限的人员的 CDE 中。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。
8.3.1	将所有非控制台访问的多重身份验证加入具有管理访问权限的人员的 CDE 中。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在用户名和密码之上增加了一层额外的防护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	控制描述	AWS Config 规则	指南
8.3.1	将所有非控制台访问的多重身份验证加入具有管理访问权限的人员的 CDE 中。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
8.3.1	将所有非控制台访问的多重身份验证加入具有管理访问权限的人员的 CDE 中。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
8.3.2	对来自实体网络外部的所有远程网络访问（包括用户和管理员，包括用于支持或维护的第三方访问）采用多重身份验证。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在用户名和密码之上增加了一层额外的防护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
8.3.2	对来自实体网络外部的所有远程网络访问（包括用户和管理员，包括用于支持或维护的第三方访问）采用多重身份验证。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在用户名和密码之上增加了一层额外的防护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
8.3.2	对来自实体网络外部的所有远程网络访问（包括用户和管理员，包括用于支持或维护的第三方访问）采用多重身份验证。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
8.3.2	对来自实体网络外部的所有远程网络访问（包括用户和管理员，包括用于支持或维护的第三方访问）采用多重身份验证。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为用户名和密码增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
10.1	实施审核跟踪，以将对系统组件的所有访问与每个单独的用户关联。	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
10.2.1	为所有系统组件实施自动审核跟踪以重建以下事件：所有单独的用户对持卡人数据的访问	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.2.2	为所有系统组件实施自动审核跟踪以重建以下事件：具有根或管理权限的任何个人执行的所有操作	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
10.2.2	为所有系统组件实施自动审核跟踪以重建以下事件：具有根或管理权限的任何个人执行的所有操作	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
10.2.2	为所有系统组件实施自动审核跟踪以重建以下事件：具有根或管理权限的任何个人执行的所有操作	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
10.2.2	为所有系统组件实施自动审核跟踪以重建以下事件：具有根或管理权限的任何个人执行的所有操作	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
10.2.2	为所有系统组件实施自动审核跟踪以重建以下事件：具有根或管理权限的任何个人执行的所有操作	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	控制描述	AWS Config 规则	指南
10.2.2	为所有系统组件实施自动审核跟踪以重建以下事件：具有根或管理权限的任何个人执行的所有操作	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
10.2.2	为所有系统组件实施自动审核跟踪以重建以下事件：具有根或管理权限的任何个人执行的所有操作	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
10.2.2	为所有系统组件实施自动审核跟踪以重建以下事件：具有根或管理权限的任何个人执行的所有操作	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.2.3	为所有系统组件实施自动审核跟踪以重建以下事件：对所有审核跟踪的访问	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
10.2.4	为所有系统组件实施自动审核跟踪以重建以下事件：无效的逻辑访问尝试	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.2.5	为所有系统组件实施自动审计跟踪记录以重建以下事件：使用和更改标识和身份验证机制（包括但不限于创建新账户和提升权限）以及所有更改、添加或删除具有根或管理权限的账户的操作	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
10.2.5	为所有系统组件实施自动审计跟踪记录以重建以下事件：使用和更改标识和身份验证机制（包括但不限于创建新账户和提升权限）以及所有更改、添加或删除具有根或管理权限的账户的操作	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
10.2.5	为所有系统组件实施自动审计跟踪记录以重建以下事件：使用和更改标识和身份验证机制（包括但不限于创建新账户和提升权限）以及所有更改、添加或删除具有根或管理权限的账户的操作	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
10.2.5	为所有系统组件实施自动审计跟踪记录以重建以下事件：使用和更改标识和身份验证机制（包括但不限于创建新账户和提升权限）以及所有更改、添加或删除具有根或管理权限的账户的操作	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
10.2.5	为所有系统组件实施自动审计跟踪记录以重建以下事件：使用和更改标识和身份验证机制（包括但不限于创建新账户和提升权限）以及所有更改、添加或删除具有根或管理权限的账户的操作	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。

控制 ID	控制描述	AWS Config 规则	指南
10.2.5	为所有系统组件实施自动审计跟踪记录以重建以下事件：使用和更改标识和身份验证机制（包括但不限于创建新账户和提升权限）以及所有更改、添加或删除具有根或管理权限的账户的操作	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
10.2.5	为所有系统组件实施自动审计跟踪记录以重建以下事件：使用和更改标识和身份验证机制（包括但不限于创建新账户和提升权限）以及所有更改、添加或删除具有根或管理权限的账户的操作	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
10.2.5	为所有系统组件实施自动审计跟踪记录以重建以下事件：使用和更改标识和身份验证机制（包括但不限于创建新账户和提升权限）以及所有更改、添加或删除具有根或管理权限的账户的操作	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
10.2.6	为所有系统组件实施自动审计跟踪记录以重建以下事件：初始化、停止或暂停审计日志	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
10.2.6	为所有系统组件实施自动审计跟踪记录以重建以下事件：初始化、停止或暂停审计日志	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
10.2.6	为所有系统组件实施自动审计跟踪记录以重建以下事件：初始化、停止或暂停审计日志	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
10.2.7	为所有系统组件实施自动审计跟踪记录以重建以下事件：创建和删除系统级对象	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
10.2.7	为所有系统组件实施自动审计跟踪记录以重建以下事件：创建和删除系统级对象	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外，AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
10.2.7	为所有系统组件实施自动审计跟踪记录以重建以下事件：创建和删除系统级对象	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
10.2.7	为所有系统组件实施自动审计跟踪记录以重建以下事件：创建和删除系统级对象	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
10.2.7	为所有系统组件实施自动审计跟踪记录以重建以下事件：创建和删除系统级对象	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
10.2.7	为所有系统组件实施自动审计跟踪记录以重建以下事件：创建和删除系统级对象	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
10.2.7	为所有系统组件实施自动审计跟踪记录以重建以下事件：创建和删除系统级对象	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。

控制 ID	控制描述	AWS Config 规则	指南
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。

控制 ID	控制描述	AWS Config 规则	指南
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
10.3.1	对于每个事件，为所有系统组件至少记录以下审计跟踪记录条目：用户标识	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
10.5	保护审计跟踪记录，使其无法更改。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
10.5	保护审计跟踪记录，使其无法更改。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.5	保护审计跟踪记录，使其无法更改。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.5.2	保护审计跟踪记录文件免遭未经授权的修改。	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
10.5.2	保护审计跟踪记录文件免遭未经授权的修改。	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
10.5.2	保护审计跟踪记录文件免遭未经授权的修改。	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
10.5.3	立即将审计跟踪记录文件备份到难以修改的集中式日志服务器或介质。	s3-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
10.5.3	立即将审计跟踪记录文件备份到难以修改的集中式日志服务器或介质。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
10.5.3	立即将审计跟踪记录文件备份到难以修改的集中式日志服务器或介质。	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。

控制 ID	控制描述	AWS Config 规则	指南
10.5.3	立即将审计跟踪记录文件备份到难以修改的集中式日志服务器或介质。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
10.5.5	对日志使用文件完整性监控或更改检测软件，以确保在未生成警报的情况下无法更改现有的日志数据（但添加的新数据应该不会导致警报）	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	控制描述	AWS Config 规则	指南
10.5.5	对日志使用文件完整性监控或更改检测软件，以确保在未生成警报的情况下无法更改现有的日志数据（但添加的新数据应该不会导致警报）	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。
10.7	将审计跟踪记录保留至少一年，其中至少有三个月可以立即进行分析（例如，在线、存档或可从备份中恢复）。	s3-lifecycle-policy-check	确保配置了 Amazon S3 生命周期策略，以帮助定义您希望 Amazon S3 在对象生命周期内采取的操作（例如，将对象过渡到其他存储类、将其存档或在指定时间后删除）。

控制 ID	控制描述	AWS Config 规则	指南
10.7	将审计跟踪记录保留至少一年，其中至少有三个月可以立即进行分析（例如，在线、存档或可从备份中恢复）。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
11.2.3	进行内部和外部扫描，并在发生重大变化后根据需要重新扫描。必须由合格的人员进行扫描。	ecr-private-image-scanning-enabled	Amazon Elastic Container Repository (ECR) 映像扫描可帮助识别容器映像中的软件漏洞。在 ECR 存储库中启用映像扫描功能可为所存储映像的完整性和安全性增加一层验证。

控制 ID	控制描述	AWS Config 规则	指南
11.4	使用入侵检测和/或入侵防御技术来检测和/或防止网络入侵。监控持卡人数据环境周边以及持卡人数据环境关键点的所有流量，并提醒人员注意可疑的漏洞。及时更新所有入侵检测和防护引擎、基准和签名。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
11.4	使用入侵检测和/或入侵防御技术来检测和/或防止网络入侵。监控持卡人数据环境周边以及持卡人数据环境关键点的所有流量，并提醒人员注意可疑的漏洞。及时更新所有入侵检测和防护引擎、基准和签名。	netfw-policy-rule-group-associated	AWS Network Firewall 策略定义了您的防火墙如何监控和处理 Amazon VPC 中的流量。您可以配置无状态和有状态规则组来过滤数据包和流量，并定义默认流量处理方式。

控制 ID	控制描述	AWS Config 规则	指南
11.5	部署更改检测机制（例如文件完整性监控工具），提醒人员注意关键系统文件、配置文件或内容文件未经授权的修改（包括更改、添加和删除）；并将软件配置为至少每周进行一次关键文件比较。	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrail 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。
11.5	部署更改检测机制（例如文件完整性监控工具），提醒人员注意关键系统文件、配置文件或内容文件未经授权的修改（包括更改、添加和删除）；并将软件配置为至少每周进行一次关键文件比较。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

模板

该模板可在以下网址获得 GitHub：PCI DSS 操作最佳实践 3.2.1。

可公开访问资源操作最佳实践

此合规包有助于识别可公开访问的资源。

有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：可公开访问资源的运营最佳实践。

印度储备银行 UCB 网络安全框架操作最佳实践

一致性包提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了印度储备银行 (RBI) 城市合作银行 (UCB) 网络安全框架 (UCB) 与托管 C AWS onfig 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个印度储备银行网络安全框架有关 UCB 的控制措施。一个印度储备银行的 UCB 网络安全框架控制可能与多个 Config 规则有关。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	AWS Config 规则	指南
Annex_I(1.1)	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	AWS Config 规则	指南
Annex_I(1.1)	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。
Annex_I(1.1)	ecr-private-tag-immutability-enabled	启用 Elastic Container Repository (ECR) 标签不可变性，以防止 ECR 映像上的映像标签被覆盖。以前，标签可能会被覆盖，需要手动方法来唯一识别映像。
Annex_I(1.3)	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration （ AWS 基础安全最佳实践值：90 ）。实际值应反映贵组织的策略。
Annex_I(1.3)	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Annex_I(1.3)	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	api-gw-cache-enabled-and-encrypted	为了帮助保护静态数据，请确保为 API Gateway 阶段的缓存启用加密。由于可能会为 API 方法捕获敏感数据，因此应启用静态加密以帮助保护这些数据。
Annex_I(1.3)	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
Annex_I(1.3)	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
Annex_I(1.3)	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Annex_I(1.3)	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。
Annex_I(1.3)	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
Annex_I(1.3)	backup-recovery-point-encrypted	确保您的 AWS Backup 恢复点已启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Annex_I(1.3)	codebuild-project-artifact-encryption	为帮助保护静态敏感数据，请确保为 AWS CodeBuild 工件启用加密。
Annex_I(1.3)	codebuild-project-s3-logs-encrypted	为帮助保护静态敏感数据，请确保对存储在 Amazon S3 中的 AWS CodeBuild 日志启用加密。
Annex_I(1.3)	opensearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保对您的 Amazon S OpenSearch ervice 域启用加密。
Annex_I(1.3)	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	opensearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Annex_I(1.3)	dynamodb-table-encrypted-kms	确保为 Amazon DynamoDB 表启用加密。由于这些表中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。默认情况下，DynamoDB 表使用自有的客户主密钥 (AWS CMK) 进行加密。
Annex_I(1.3)	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Annex_I(1.3)	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。
Annex_I(1.3)	elasticsearch-encrypted-at-rest	由于敏感数据可能存在，并且为了帮助保护静态数据，请确保您的亚马逊 OpenSearch 服务（OpenSearch 服务）域已启用加密。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	elasticsearch-node-to-node-encryption-check	确保启用了 Amazon OpenSearch 服务的 node-to-node 加密。N ode-to-node 加密为亚马逊虚拟私有云（亚马逊 VPC）内的所有通信启用 TLS 1.2 加密。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Annex_I(1.3)	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
Annex_I(1.3)	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Annex_I(1.3)	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
Annex_I(1.3)	rds-snapshot-encrypted	确保为 Amazon Relational Database Service (Amazon RDS) 快照启用加密。由于可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Annex_I(1.3)	rds-storage-encrypted	为了帮助保护静态数据，请确保您的 Amazon Relational Database Service (Amazon RDS) 实例启用了加密。由于 Amazon RDS 实例中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
Annex_I(1.3)	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
Annex_I(1.3)	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。
Annex_I(1.3)	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	sagemaker-endpoint-configuration-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 终端节点已启用 AWS 密钥管理服务 (AWS KMS) 加密。由于敏感数据可以静态存在于 SageMaker 端点中，因此启用静态加密以帮助保护这些数据。
Annex_I(1.3)	sagemaker-notebook-instance-kms-key-configured	为帮助保护静态数据，请确保您的 SageMaker 笔记本电脑启用了 AWS 密钥管理服务 (AWS KMS) 的加密。由于敏感数据可以静态存在于 SageMaker 笔记本中，因此启用静态加密以帮助保护这些数据。
Annex_I(1.3)	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Annex_I(1.3)	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
Annex_I(1.3)	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
Annex_I(1.3)	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
Annex_I(1.3)	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。
Annex_I(1.3)	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
Annex_I(1.3)	no-unrestricted-route-to-igw	确保 Amazon EC2 路由表中没有指向互联网网关的无限制路由。移除或限制 Amazon VPC 内工作负载的互联网访问可以减少环境中的意外访问。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	redshift-cluster-kms-enabled	为了帮助保护静态数据，请确保您的 Amazon Redshift 集群启用了密 AWS 钥管理服务 (AWS KMS) 的加密。由于 Redshift 集群中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
Annex_I(1.3)	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
Annex_I(1.3)	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
Annex_I(1.3)	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
Annex_I(1.3)	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
Annex_I(1.3)	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Annex_I(1.3)	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
Annex_I(1.3)	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
Annex_I(1.3)	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
Annex_I(1.3)	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
Annex_I(1.3)	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	AWS Config 规则	指南
Annex_I(1.3)	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
Annex_I(5.1)	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。
Annex_I(5.1)	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
Annex_I(5.1)	waf-regional-rule-not-empty	确保您的 AWS WAF 有一条不为空的规则。不含条件的规则可能会导致意外行为。
Annex_I(5.1)	waf-regional-rulegroup-not-empty	确保您的 AWS WAF 的规则组不为空。空规则组可能会导致意外行为。

控制 ID	AWS Config 规则	指南
Annex_I(5.1)	waf-regional-webacl-not-empty	附加到 AWS WAF 的 Web ACL 可以包含一组用于检查和控制 Web 请求的规则和规则组。如果 Web ACL 为空，Web 流量将直接通过，而不会被 WAF 检测或处理。
Annex_I(5.1)	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
Annex_I(5.1)	api-gw-associated-with-waf	AWS WAF 允许您配置一组规则（称为 Web 访问控制列表 (Web ACL)），这些规则根据您定义的可自定义 Web 安全规则和条件允许、阻止或计数 Web 请求。确保您的 Amazon API Gateway 阶段与某个 WAF Web ACL 关联，以保护其免受恶意攻击

控制 ID	AWS Config 规则	指南
Annex_I(5.1)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
Annex_I(5.1)	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。
Annex_I(6)	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	AWS Config 规则	指南
Annex_I(6)	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
Annex_I(6)	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev （配置默认值：30）、 daysHighSev （配置默认值：7）和（配置默认：1）。
Annex_I(6)	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
Annex_I(6)	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	AWS Config 规则	指南
Annex_I(6)	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许您选择设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automatedSnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。
Annex_I(6)	vuln-management-plan-exists（过程检查）	确保制定并实施漏洞管理计划，以便有一个正式定义的流程来处理环境中的漏洞。
Annex_I(7.1)	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
Annex_I(7.1)	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
Annex_I(7.1)	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
Annex_I(7.1)	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
Annex_I(7.1)	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	AWS Config 规则	指南
Annex_I(7.2)	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。
Annex_I(7.3)	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。

控制 ID	AWS Config 规则	指南
Annex_I(7.4)	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。
Annex_I(7.4)	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
Annex_I(7.4)	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
Annex_I(7.4)	cloudtrail-s3-dataevents-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。
Annex_I(7.4)	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。

控制 ID	AWS Config 规则	指南
Annex_I(7.4)	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
Annex_I(7.4)	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
Annex_I(7.4)	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	AWS Config 规则	指南
Annex_I(7.4)	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
Annex_I(7.4)	opensearch-audit-logging-enabled	确保在您的 Amazon OpenSearch 服务域上启用了审核日志。审核日志允许您跟踪 OpenSearch 网域上的用户活动，包括身份验证成功和失败、对域名的请求 OpenSearch、索引更改以及传入的搜索查询。
Annex_I(7.4)	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。
Annex_I(7.4)	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。

控制 ID	AWS Config 规则	指南
Annex_I(7.4)	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时，CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
Annex_I(7.4)	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	AWS Config 规则	指南
Annex_I(7.4)	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
Annex_I(7.4)	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
Annex_I(7.4)	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。

控制 ID	AWS Config 规则	指南
Annex_I(7.4)	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDbEncrypted（配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。
Annex_I(10.2)	security-awareness-program-exists（过程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
Annex_I(12)	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
Annex_I(12)	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
Annex_I(12)	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。
Annex_I(12)	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Annex_I(12)	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	AWS Config 规则	指南
Annex_I(12)	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Annex_I(12)	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
Annex_I(12)	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。

控制 ID	AWS Config 规则	指南
Annex_I(12)	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。
Annex_I(12)	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
Annex_I(12)	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	AWS Config 规则	指南
Annex_I(12)	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

模板

该模板可在以下网址获得 GitHub：印度储备银行UCB网络安全框架运营最佳实践。

RBI MD-ITF 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

以下提供了印度储备银行 (RBI) 主方向——信息技术框架和 AWS 托管 Config 规则之间的映射示例。每条 Config 规则都适用于特定 AWS 资源，并与一个或多个印度储备银行主方向——信息技术框架控件相关。RBI Master Direction 信息技术框架控件可以与多个 Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	控制描述	AWS Config 规则	指南
3.1(a)	信息资产的识别和分类。	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软

控制 ID	控制描述	AWS Config 规则	指南
			件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
3.1(a)	信息资产的识别和分类。	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
3.1(a)	信息资产的识别和分类。	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。

控制 ID	控制描述	AWS Config 规则	指南
3.1(a)	信息资产的识别和分类。	ecr-private-tag-immutability-enabled	启用 Elastic Container Repository (ECR) 标签不可变性，以防止 ECR 映像上的映像标签被覆盖。以前，标签可能会被覆盖，需要手动方法来唯一识别映像。
3.1(c)	基于角色的访问控制	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1(c)	基于角色的访问控制	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
3.1(c)	基于角色的访问控制	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。

控制 ID	控制描述	AWS Config 规则	指南
3.1(c)	基于角色的访问控制	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
3.1(c)	基于角色的访问控制	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。
3.1(c)	基于角色的访问控制	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
3.1(c)	基于角色的访问控制	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
3.1(c)	基于角色的访问控制	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1(c)	基于角色的访问控制	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.1(c)	基于角色的访问控制	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1(c)	基于角色的访问控制	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
3.1(c)	基于角色的访问控制	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
3.1(c)	基于角色的访问控制	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
3.1(c)	基于角色的访问控制	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
3.1(c)	基于角色的访问控制	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
3.1(c)	基于角色的访问控制	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
3.1(c)	基于角色的访问控制	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
3.1(c)	基于角色的访问控制	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
3.1(c)	基于角色的访问控制	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
3.1(c)	基于角色的访问控制	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
3.1(c)	基于角色的访问控制	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
3.1(g)	事件管理	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。

控制 ID	控制描述	AWS Config 规则	指南
3.1(g)	事件管理	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
3.1(g)	事件管理	alb-waf-enabled	确保在弹性负载均衡器 (ELB) 上启用 AWS WAF，以帮助保护 Web 应用程序。WAF 有助于保护您的 Web 应用程序或 API 免遭常见 Web 漏洞的侵害。这些 Web 漏洞可能会影响可用性、损害安全性或消耗环境中过多的资源。

控制 ID	控制描述	AWS Config 规则	指南
3.1(g)	事件管理	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
3.1(g)	事件管理	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
3.1(h)	跟踪	api-gw-execution-logging-enabled	API Gateway 日志显示访问 API 的用户以及他们访问 API 的方式的详细视图。这种洞察可实现用户活动的可见性。

控制 ID	控制描述	AWS Config 规则	指南
3.1(h)	跟踪	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
3.1(h)	跟踪	codebuild-project-logging-enabled	确保启用 AWS CodeBuild 项目日志记录，以便将您的构建输出日志发送到亚马逊 CloudWatch 或亚马逊简单存储服务 (Amazon S3) Simple Storage Service。构建输出日志提供有关您的构建项目的详细信息。
3.1(h)	跟踪	opensearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatc h Logs 以进行保留和响应。 OpenSearch 服务错误日志可以帮助进行安全和访问审计，还可以帮助诊断可用性问题。

控制 ID	控制描述	AWS Config 规则	指南
3.1(h)	跟踪	redshift-audit-logging-enabled	要捕获有关您的 Amazon Redshift 集群上的连接和用户活动的信息，请确保已启用审计日志记录。
3.1(h)	跟踪	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户 调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “AWS CloudTrail 记录内容” 中查看。
3.1(h)	跟踪	cloudtrail-s3-data events-enabled	收集 Simple Storage Service (Amazon S3) 数据事件有助于检测任何异常活动。详细 AWS 账户 信息包括访问 Amazon S3 存储桶的信息、IP 地址和事件时间。

控制 ID	控制描述	AWS Config 规则	指南
3.1(h)	跟踪	cw-loggroup-retention-period-check	确保为日志组保留事件日志数据的最短时间，以帮助进行故障排除和取证调查。缺乏过去的事件日志数据会让重建和识别潜在的恶意事件变得困难。
3.1(h)	跟踪	elasticsearch-logs-to-cloudwatch	确保 Amazon S OpenSearch ervice 域已启用错误日志，并将其流式传输到 Amazon CloudWatch Logs 以进行保留和响应。域错误日志可以帮助进行安全和访问审核，还可以帮助诊断可用性问题。
3.1(h)	跟踪	elb-logging-enabled	Elastic Load Balancing 活动是环境中的一个通信中心点。确保已启用 ELB 日志记录。收集的数据将提供有关发送到 ELB 的请求的详细信息。每个日志都包含信息 (例如，收到请求的时间、客户端的 IP 地址、延迟、请求路径和服务器响应)。

控制 ID	控制描述	AWS Config 规则	指南
3.1(h)	跟踪	multi-region-cloudtrail-enabled	AWS CloudTrail 记录 AWS 管理控制台操作和 API 调用。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。 CloudTrail 如果启用了 MULTI_REGION_CLOUD_TRAIL_ENABLED，则会将来自所有 AWS 区域的日志文件传输到您的 S3 存储桶。此外， AWS 启动新区域时， CloudTrail 将在新区域中创建相同的跟踪。因此，您无需采取任何措施，即可收到包含新区域的 API 活动的日志文件。
3.1(h)	跟踪	rds-logging-enabled	为了帮助在环境中进行日志记录和监控，请确保已启用 Amazon Relational Database Service (Amazon RDS) 日志记录。利用 Amazon RDS 日志记录，您可以捕获诸如连接、断开连接、查询或查询的表之类的事件。

控制 ID	控制描述	AWS Config 规则	指南
3.1(h)	跟踪	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
3.1(h)	跟踪	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。

控制 ID	控制描述	AWS Config 规则	指南
3.1(h)	跟踪	wafv2-logging-enabled	要帮助在您的环境中进行日志记录和监控，请在区域和全球 Web ACL 上启用 AWS WAF (V2) 日志记录。 AWS WAF 日志记录提供有关您的 Web ACL 所分析的流量的详细信息。这些日志记录了 AWS WAF 从您的 AWS 资源收到请求的时间、有关请求的信息以及每个请求匹配的规则的操作。
3.1(h)	跟踪	redshift-cluster-configuration-check	要保护静态数据，请确保您的 Amazon Redshift 集群启用了加密。您还必须确保在 Amazon Redshift 集群上部署所需的配置。应启用审计日志记录，以提供有关数据库中连接和用户活动的信息。此规则要求为 clusterDb Encrypted （配置默认：TRUE）和启用 LoggingEnabled（配置默认值：TRUE）设置一个值。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.1(i)	公有密钥基础设施	acm-certificate-expiration-check	通过确保 X509 证书由 ACM 颁发，确保网络完整性得到保护。 AWS 这些证书必须有效且未过期。此规则需要一个值 daysToExpiration（AWS 基础安全最佳实践值：90）。实际值应反映贵组织的策略。
3.1(i)	公有密钥基础设施	alb-http-drop-invalid-header-enabled	确保您的 Elastic Load Balancers (ELB) 已配置为丢弃 http 标头。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1(i)	公有密钥基础设施	alb-http-to-https-redirection-check	为帮助保护传输中的数据，请确保应用负载均衡器自动将未加密的 HTTP 请求重定向到 HTTPS。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1(i)	公有密钥基础设施	api-gw-ssl-enabled	确保 Amazon API Gateway REST API 阶段配置了 SSL 证书，以允许后端系统验证请求来自 API Gateway。
3.1(i)	公有密钥基础设施	opensearch-https-required	由于敏感数据可能存在，并且为了帮助保护传输中的数据，请确保为与您的 Amazon S OpenSearch ervice 域的连接启用 HTTPS。
3.1(i)	公有密钥基础设施	elbv2-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。

控制 ID	控制描述	AWS Config 规则	指南
3.1(i)	公有密钥基础设施	elb-acm-certificate-required	由于可能存在敏感数据，并且为了帮助保护传输中的数据，应确保 Elastic Load Balancing 启用了加密。使用 AWS Certifice Manager 通过 AWS 服务和内部资源管理、配置和部署公共和私有 SSL/TLS 证书。
3.1(i)	公有密钥基础设施	elb-tls-https-listeners-only	确保您的弹性负载均衡器 (ELB) 配置了 SSL 或 HTTPS 侦听器。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.1(i)	公有密钥基础设施	redshift-require-tls-ssl	确保您的 Amazon Redshift 集群需要 TLS/SSL 加密才能连接到 SQL 客户端。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。

控制 ID	控制描述	AWS Config 规则	指南
3.1(i)	公有密钥基础设施	s3-bucket-ssl-requests-only	为了帮助保护传输中的数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶需要请求使用安全套接字层 (SSL)。由于可能存在敏感数据，因此应启用传输中加密以帮助保护这些数据。
3.3	漏洞管理	elastic-beanstalk-managed-updates-enabled	为 Amazon Elastic Beanstalk 环境启用受管平台更新可确保安装环境的最新可用平台修复、更新和功能。及时安装补丁是保护系统的最佳实践。
3.3	漏洞管理	rds-automatic-minor-version-upgrade-enabled	启用 Amazon Relational Database Service (RDS) 实例的自动次要版本升级，以确保安装关系数据库管理系统 (RDBMS) 的最新次要版本更新，其中可能包括安全补丁和错误修复。

控制 ID	控制描述	AWS Config 规则	指南
3.3	漏洞管理	redshift-cluster-maintenancesettings-check	此规则可确保 Amazon Redshift 集群具有适合贵组织的首选设置。具体而言，就是确保它们有首选的数据库维护窗口和自动快照保留期。此规则要求您设置 allowVersionUpgrade. 默认值为 true。它还允许你选择性地设置 preferredMaintenanceWindow（默认值为 sat：16:00-sat：16:30）和周 automated SnapshotRetention期（默认值为 1）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
3.3	漏洞管理	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
3.3	漏洞管理	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。

控制 ID	控制描述	AWS Config 规则	指南
3.3	漏洞管理	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。
3.3	漏洞管理	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。

控制 ID	控制描述	AWS Config 规则	指南
3.5	网络危机管理计划	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
3.5	网络危机管理计划	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
3.5	网络危机管理计划	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
3.5	网络危机管理计划	ec2-managedinstance-association-compliance-status-check	使用 AWS Systems Manager Associations 来帮助清点组织内的软件平台和应用程序。 AWS Systems Manager 会为您的托管实例分配配置状态，并允许您设置操作系统补丁级别、软件安装、应用程序配置以及有关您的环境的其他详细信息的基准。

控制 ID	控制描述	AWS Config 规则	指南
3.5	网络危机管理计划	ec2-managedinstance-patch-compliance-status-check	启用此规则以帮助识别和记录 Amazon Elastic Compute Cloud (Amazon EC2) 漏洞。该规则根据贵组织的政策和程序的要求检查 S AWS ystems Manager 中的 Amazon EC2 实例补丁是否合规。
3.9	IT 风险评估	annual-risk-assessment-performed（过程检查）	对您的组织进行年度风险评估。风险评估有助于确定已识别的风险和/或漏洞对组织造成影响的可能性和影响。
3.12	训练	security-awareness-program-exists（过程检查）	为您的组织制定并维护安全认知计划。安全认知计划教育员工如何保护其组织免受各种安全漏洞或事件的侵害。
4.4(g)	欺诈分析 - 可疑交易分析、贪污、盗窃或涉嫌洗钱、挪用资产、操纵财务记录等。向 RBI 举报欺诈行为的监管要求应由系统驱动。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
4.4(h)	IT 安全系统的容量和性能分析。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。
4.4(h)	IT 安全系统的容量和性能分析。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	clb-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
4.4(h)	IT 安全系统的容量和性能分析。	elbv2-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
4.4(h)	IT 安全系统的容量和性能分析。	lambda-vpc-multi-az-check	如果您的 AWS Lambda 函数配置为连接到您账户中的虚拟私有云 (VPC)，请在至少两个不同的可用区中部署 AWS Lambda 函数，以确保在单个区域发生服务中断的情况下，您的函数可用于处理事件。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。
4.4(h)	IT 安全系统的容量和性能分析。	rds-multi-az-support	Amazon Relationa l Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	s3-bucket-default-lock-enabled	确保默认情况下 Amazon Simple Storage Service (Amazon S3) 存储桶已启用锁定。由于 S3 存储桶中可能存在敏感的静态数据，因此应强制执行静态对象锁定以帮助保护这些数据。
4.4(h)	IT 安全系统的容量和性能分析。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
4.4(h)	IT 安全系统的容量和性能分析。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。
4.4(h)	IT 安全系统的容量和性能分析。	lambda-dlq-check	启用此规则有助于在功能发生故障时通过 Amazon Simple Queue Service (Amazon SQS) 或 Amazon Simple Notification Service (Amazon SNS) 通知相关人员。
4.4(h)	IT 安全系统的容量和性能分析。	beanstalk-enhanced-health-reporting-enabled	AWS Elastic Beanstalk 增强的运行状况报告功能可以更快地响应底层基础设施运行状况的变化。这些变更可能会导致应用程序的可用性不足。Elastic Beanstalk 增强的运行状况报告提供了状态描述符，用于衡量已发现问题的严重性并确定可能的原因以进行调查。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
4.4(h)	IT 安全系统的容量和性能分析。	ebs-optimized-instance	Amazon Elastic Block Store (Amazon EBS) 中的优化实例为 Amazon EBS I/O 操作提供了额外的专用容量。这种优化通过最大限度减少 Amazon EBS I/O 操作与来自您实例的其他流量之间的争用，为您的 EBS 卷提供最佳性能。

控制 ID	控制描述	AWS Config 规则	指南
4.4(h)	IT 安全系统的容量和性能分析。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
4.4(i)	事件报告、事件影响以及为防止将来再发生此类事件而采取的措施。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	控制描述	AWS Config 规则	指南
4.4(i)	事件报告、事件影响以及为防止将来再发生此类事件而采取的措施。	guardduty-non-archived-findings	Amazon 按严重程度对调查结果进行分类：低、中、高，从而 GuardDuty 帮助您了解事件的影响。您可以使用这些分类来确定补救策略和优先级。此规则允许您根据组织政策的 daysLowSev 要求选择性地为非存档的查找结果设置 daysMediumSev（配置默认值：30）、 daysHighSev（配置默认值：7）和（配置默认：1）。
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。

控制 ID	控制描述	AWS Config 规则	指南
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	aurora-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon Aurora 资源。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。

控制 ID	控制描述	AWS Config 规则	指南
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	cmk-backing-key-rotation-enabled	启用密钥轮换，以确保密钥在加密周期结束后进行轮换。
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。

控制 ID	控制描述	AWS Config 规则	指南
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	ec2-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性计算云 (Amazon EC2) 资源包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	fsx-resources-protected-by-backup-plan	为了帮助完成数据备份流程，请确保 AWS 备份计划中包含您的 Amazon FSx 文件系统。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
6.3	NBFC 应考虑是否需要为其关键业务系统和数据中心建立必要的备份站点。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	dynamodb-autoscaling-enabled	Amazon DynamoDB 自动扩展 AWS 使用 Application Auto Scaling 服务来调整自动响应实际流量模式的预配置吞吐容量。这将允许表或全局二级索引增大其预置的读/写容量以处理突发流量，而不进行节流。
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	elb-cross-zone-load-balancing-enabled	为您的 Elastic Load Balancers (ELB) 启用跨区域负载均衡，以帮助保持足够的容量和可用性。跨区域负载均衡可降低在每个启用的可用区维持相同数量实例的需求。它还将提高应用程序处理一个或多个实例丢失情况的能力。

控制 ID	控制描述	AWS Config 规则	指南
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	elb-deletion-protection-enabled	此规则可确保 Elastic Load Balancing 已启用删除保护。使用此功能可防止负载均衡器被意外或恶意删除，因为这可能导致应用程序丧失可用性。
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	clb-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	elbv2-multiple-az	弹性负载均衡 (ELB) 在一个可用区中的多个目标（如 EC2 实例、容器和 IP 地址）之间自动分配传入的流量。为保障高可用性，请确保您的 ELB 已注册来自多个可用区的实例。

控制 ID	控制描述	AWS Config 规则	指南
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	lambda-vpc-multi-az-check	如果您的 AWS Lambda 函数配置为连接到您账户中的虚拟私有云 (VPC)，请在至少两个不同的可用区中部署 AWS Lambda 函数，以确保在单个区域发生服务中断的情况下，您的函数可用于处理事件。
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	rds-instance-deletion-protection-enabled	确保 Amazon Relational Database Service (Amazon RDS) 实例已启用删除保护。使用删除保护可防止您的 Amazon RDS 实例被意外或恶意删除，这可能会导致您的应用程序丧失可用性。

控制 ID	控制描述	AWS Config 规则	指南
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	rds-multi-az-support	Amazon Relational Database Service (Amazon RDS) 中的多可用区支持为数据库实例提供了增强的可用性和耐久性。当您预置多可用区数据库实例时，Amazon RDS 会自动创建一个主数据库实例，并将数据同步复制到不同可用区中的备用实例。每个可用性区域都在各自独立的物理基础设施上运行，具有高度可靠性。如果基础设施出现故障，Amazon RDS 会自动失效转移到备用服务器，这样您就可以在失效转移完成后立即恢复数据库操作。

控制 ID	控制描述	AWS Config 规则	指南
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	vpc-vpn-2-tunnels-up	可实施冗余站点到站点 VPN 隧道来实现弹性需求。它使用两条隧道来帮助确保连接性，以防其中一个站点到站点 VPN 连接不可用。为防止在客户网关不可用的情况下断开连接，您可以使用第二个客户网关为您的 Amazon Virtual Private Cloud (Amazon VPC) 和虚拟私有网关建立第二个站点到站点 VPN 连接。
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	autoscaling-group-elb-healthcheck-required	Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling 组的 Elastic Load Balancer (ELB) 运行状况检查支持维持足够的容量和可用性。负载均衡器会定期发送 ping、尝试进行连接或者发送请求来测试自动扩缩组中的 Amazon EC2 实例。如果实例没有返回报告，则流量会发送到新的 Amazon EC2 实例。

控制 ID	控制描述	AWS Config 规则	指南
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	dynamodb-throughput-limit-check	启用此规则可确保检查您的 Amazon DynamoDB 表上的预置吞吐容量。这是每个表可以支持的读/写活动量。DynamoDB 使用这些信息来预留足够的系统资源，以满足吞吐量需求。当吞吐量接近客户账户的最大限制时，此规则会生成警报。此规则允许您选择设置 AccountRCU（ThresholdPercentage 配置默认值：80）和 AccountWCUThresholdPercentage （配置默认值：80）参数。实际值应反映贵组织的策略。
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。

控制 ID	控制描述	AWS Config 规则	指南
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	lambda-concurrency-check	此规则可确保建立 Lambda 函数的并发上限和下限。这有助于确定函数在任何特定时间提供服务的请求数量的基准。

控制 ID	控制描述	AWS Config 规则	指南
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	rds-enhanced-monitoring-enabled	启用 Amazon Relational Database Service (Amazon RDS)，以帮助监控 Amazon RDS 可用性。这让您可以详细了解您的 Amazon RDS 数据库实例的运行状况。当 Amazon RDS 存储使用多个底层物理设备时，“增强监控”会收集每台设备的数据。此外，当 Amazon RDS 数据库实例在多可用区部署中运行时，会收集辅助主机上每个设备的数据和辅助主机指标。

控制 ID	控制描述	AWS Config 规则	指南
8.1	随着 NBFC 运营规模和复杂性的增加，应逐步扩展 IT 系统。	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	dms-replication-not-public	通过确保 DMS 复制实例无法公开访问来管理对 AWS 云的访问权限。DMS 复制实例可能包含敏感信息，因此需要对此类账户进行访问控制。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	ebs-snapshot-public-restorable-check	通过确保 EBS 快照不可公开还原来管理对 AWS 云的访问权限。EBS 卷快照可能包含敏感信息，因此需要对此类账户进行访问控制。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实例来管理对云的访问。AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	elasticsearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务（OpenSearch 服务）域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。Amazon VPC 中的 OpenSearch 服务域可实现 OpenSearch 服务与 Amazon VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	emr-master-no-public-ip	通过确保无法公开访问 Amazon EMR 集群主节点来管理对 AWS 云的访问。Amazon EMR 集群主节点可能包含敏感信息，因此需要对此类账户进行访问控制。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。

控制 ID	控制描述	AWS Config 规则	指南
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	rds-instance-public-access-check	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	rds-snapshots-public-prohibited	通过确保亚马逊关系数据库服务 (Amazon RDS) 实例不公开，管理对 AWS 云中资源的访问权限。Amazon RDS 数据库实例可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	redshift-cluster-public-access-check	通过确保 Amazon Redshift 集群不公开，管理对 AWS 云端资源的访问权限。Amazon Redshift 集群可能包含敏感信息，因此需要对此类账户实施相应原则和访问控制。

控制 ID	控制描述	AWS Config 规则	指南
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	sagemaker-notebook-no-direct-internet-access	通过确保 Amazon SageMaker 笔记本电脑不允许直接访问互联网，管理对 AWS 云端资源的访问。通过防止直接访问互联网，您可以防止未经授权的用户访问敏感数据。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。

控制 ID	控制描述	AWS Config 规则	指南
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	access-keys-rotated	通过确保 IAM 访问密钥按照组织策略的规定轮换，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	emr-kerberos-enabled	通过为 Amazon EMR 集群启用 Kerberos，可以按照最低权限和职责分离的原则管理和纳入访问权限和授权。在 Kerberos 中，需要进行身份验证的服务和用户称为委托人。委托人存在于 Kerberos 领域中。在该领域中，Kerberos 服务器被称为密钥分配中心 (KDC)。它为委托人提供一种进行身份验证的方法。KDC 通过颁发用于身份验证的票证进行身份验证。KDC 维护一个包含其领域中的委托人、它们的密码及其它有关每个委托人的管理信息的数据库。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	autoscaling-launch-config-public-ip-disabled	如果您使用公有 IP 地址配置网络接口，则可以从互联网访问这些网络接口的相关资源。EC2 资源不应可公开访问，因为这可能会允许意外地访问您的应用程序或服务器。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	ecs-task-definition-nonroot-user	为了帮助实施最低权限原则，请确保指定非根用户来访问您的 Amazon Elastic Container Service (Amazon ECS) 任务定义。

控制 ID	控制描述	AWS Config 规则	指南
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	efs-access-point-enforce-root-directory	为 Amazon Elastic File System (Amazon EFS) 接入点强制使用根目录可确保接入点的用户只能访问指定子目录的文件，从而帮助限制数据访问。
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	efs-access-point-enforce-user-identity	为了帮助实施最低权限原则，请确保为您的 Amazon Elastic File System (Amazon EFS) 启用用户强制执行。启用后，Amazon EFS 会将 NFS 客户端的用户和组 ID 替换为接入点上为所有文件系统操作配置的身份，并只向此强制用户身份授予访问权限。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Managemen t。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。

控制 ID	控制描述	AWS Config 规则	指南
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	subnet-auto-assign-public-ip-disabled	通过确保亚马逊虚拟私有 AWS 云 (VPC) Virtual Private Cloud 子网不会自动分配公有 IP 地址来管理对云的访问。Amazon Elastic Compute Cloud (EC2) 实例在启用此属性的子网中启动时，其主网络接口会分配一个公有 IP 地址。
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户 方法来帮助整合功能最少的原则。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。
8.l	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	opensearch-in-vpc-only	通过确保亚马逊 OpenSearch 服务域位于亚马逊虚拟私有 AWS 云（亚马逊 VPC）内来管理对云的访问。亚马逊 VPC 内的亚马逊 OpenSearch 服务域可实现亚马逊 OpenSearch 服务与亚马逊 VPC 内的其他服务之间的安全通信，无需互联网网关、NAT 设备或 VPN 连接。
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	控制描述	AWS Config 规则	指南
8.I	基本安全方面，例如物理/逻辑访问控制和明确定义的密码策略。	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
8.II	明确定义的用户角色。	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。
8.II	明确定义的用户角色。	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。

控制 ID	控制描述	AWS Config 规则	指南
8.II	明确定义的用户角色。	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、 PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	控制描述	AWS Config 规则	指南
8.II	明确定义的用户角色。	iam-policy-no-statements-with-admin-access	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，限制策略包含 “效果”：“允许” 和 “操作”：“*” 而不是 “资源”：“*”。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
8.II	明确定义的用户角色。	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
8.II	明确定义的用户角色。	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	控制描述	AWS Config 规则	指南
8.II	明确定义的用户角色。	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为“ maxCredentialUsage年龄”设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
8.III	Maker-Checker 概念，旨在降低错误和滥用风险，并确保数据/信息的可靠性。	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	控制描述	AWS Config 规则	指南
8.IX	安排数据备份并进行定期测试。	db-instance-backup-enabled	Amazon RDS 的备份功能可创建数据库和事务日志的备份。Amazon RDS 会自动创建数据库实例的存储卷快照，备份整个数据库实例。系统允许您设置特定的保留期以满足您的弹性要求。
8.IX	安排数据备份并进行定期测试。	dynamodb-in-backup-plan	为了帮助完成数据备份流程，请确保备份计划中包含您的 Amazon DynamoDB 表。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.IX	安排数据备份并进行定期测试。	dynamodb-pitr-enabled	启用此规则可检查信息是否已备份。它还通过确保在 Amazon DynamoDB 中启用 point-in-time 恢复功能来维护备份。恢复过程会维持表在过去 35 天的连续备份。

控制 ID	控制描述	AWS Config 规则	指南
8.IX	安排数据备份并进行定期测试。	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.IX	安排数据备份并进行定期测试。	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。

控制 ID	控制描述	AWS Config 规则	指南
8.IX	安排数据备份并进行定期测试。	elasticache-redis-cluster-automatic-backup-check	启用自动备份后，Amazon ElastiCache 会每天创建集群的备份。备份可保留的天数由贵组织规定。自动备份可以帮助防止数据丢失。发生故障时，您可以通过从最新的备份还原数据来创建新集群。
8.IX	安排数据备份并进行定期测试。	rds-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊关系数据库服务 (Amazon RDS) 实例包含在 AWS 备份计划中。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
8.IX	安排数据备份并进行定期测试。	s3-bucket-replication-enabled	Amazon Simple Storage Service (Amazon S3) 跨区域复制 (CRR) 支持保持足够的容量和可用性。CRR 可在 Amazon S3 存储桶间自动异步复制对象，以帮助确保数据的可用性。

控制 ID	控制描述	AWS Config 规则	指南
8.IX	安排数据备份并进行定期测试。	redshift-backup-enabled	为了帮助完成数据备份流程，请确保您的 Amazon Redshift 集群具有自动快照。当某个集群的自动快照处于启用状态时，Redshift 会定期拍摄该集群的快照。默认情况下，Redshift 每八小时或每 5 GB 为每个数据更改节点（或以先到者为准）拍摄一次快照。

控制 ID	控制描述	AWS Config 规则	指南
8.IX	安排数据备份并进行定期测试。	backup-plan-min-frequency-and-min-retention-check	为了帮助完成数据 AWS 备份流程，请确保将 Backup 计划设置为最低频率和保留期限。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredFrequencyValue（配置默认：1）、 requiredRetentionDays（配置默认值：35）和 requiredFrequencyUnit（配置默认值：天）参数。实际值应反映贵组织的需求。
8.IX	安排数据备份并进行定期测试。	backup-recovery-point-manual-deletion-disabled	确保您的 AWS Backup 恢复点附有基于资源的策略，以防止删除恢复点。使用基于资源的策略来防止删除恢复点有助于防止意外或故意删除。

控制 ID	控制描述	AWS Config 规则	指南
8.IX	安排数据备份并进行定期测试。	backup-recovery-point-minimum-retention-check	为了帮助完成数据 AWS 备份流程，请确保您的 Backup 恢复点设置了最短保留期。 AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。此规则允许您设置 requiredRetentionDays（配置默认值：35）参数。实际值应反映贵组织的需求。

模板

该模板可在以下网址获得 GitHub：印度储备银行 MD-ITF 运营最佳实践。

安全性、身份和合规性操作最佳实践

此一致性包包含基于安全、身份和合规服务的 AWS Config 规则。有关更多信息，请参阅上的 “安全、身份和合规性” AWS。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：安全、身份和合规服务的运营最佳实践。

无服务器操作最佳实践

此一致性包包含基于无服务器解决方案的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：无服务器操作最佳实践。

存储服务操作最佳实践

此一致性包包含基于存储服务的 AWS Config 规则。有关更多信息，请参阅上的 “云存储” AWS。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：存储服务最佳操作实践。

SWIFT CSP 操作最佳实践

Conformance Pack 提供了一个通用的合规框架，旨在使您能够使用托管或自定义 AWS Config 规则和 AWS Config 补救措施来创建安全、运营或成本优化治理检查。作为示例模板，合规包并不是为了完全确保遵守特定的治理或合规标准而设计的。您有责任自行评估自己对服务的使用是否符合适用的法律和监管要求。

下面提供了 SWIFT 的客户安全计划 (CSP) 和 AWS 托管 Config 规则之间的映射示例。每 AWS Config 条规则都适用于特定的 AWS 资源，并与一个或多个 SWIFT CSP 控制措施有关。一个 SWIFT CSP 控件可以与多个 AWS Config 规则相关联。有关这些映射的更多详细信息和指导，请参阅下表。

控制 ID	AWS Config 规则	指南
1.1	ec2-instance-managed-by-systems-manager	通过使用 Systems Man AWS ager 管理亚马逊弹性计算云 (Amazon EC2) 实例，可以清点组织内的软件平台和应用程序。使用 AWS Systems Manager 提供详细的系统配置、操作系统补丁级别、服务名称和类型、软件安装、应用程序名称、发行商和版本以及有关您的环境的其他详细信息。
1.1	ec2-instance-no-public-ip	通过确保无法公开访问亚马逊弹性计算云 (Amazon EC2) 实

控制 ID	AWS Config 规则	指南
		例来管理对云的访问。 AWS Amazon EC2 实例可能包含敏感信息，因此需要对此类账户进行访问控制。
1.1	ec2-no-amazon-key-pair	此规则检查正在运行的 Amazon Elastic Compute Cloud (Amazon EC2) 实例是否是使用亚马逊密钥对启动的。这可以帮助降低凭证泄露的风险。仍然可以通过 AWS 控制台使用会话管理器或基于浏览器的 SSH 连接访问没有密钥对的 Amazon EC2 实例。
1.1	ec2-instances-in-vpc	在 Amazon Virtual Private Cloud (Amazon VPC) 内部署 Amazon Elastic Compute Cloud (Amazon EC2) 实例，以实现实例与 Amazon VPC 内其他服务之间的安全通信，而无需互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。将 Amazon EC2 实例分配给 Amazon VPC 以正确管理访问权限。

控制 ID	AWS Config 规则	指南
1.1	vpc-default-security-group-closed	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 限制默认安全组上的所有流量有助于限制对 AWS 资源的远程访问。
1.1	vpc-network-acl-unused-check	此规则可确保 Amazon Virtual Private Cloud (VPC) 网络访问控制列表正在使用中。监控未使用的网络访问控制列表有助于准确清点和管理您的环境。
1.1	vpc-sg-open-only-to-authorized-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。通过限制从互联网 (0.0.0.0/0) 访问安全组内的资源，可以控制对内部系统的远程访问。

控制 ID	AWS Config 规则	指南
1.2	iam-customer-policy-blocked-kms-actions	AWS Identity and Access Management (IAM) 可以帮助您将最低权限和职责分离原则与访问权限和授权相结合，从而限制策略包含对 AWS 所有密钥管理服务密钥的封锁操作。拥有超过完成任务所需的权限可能会违反最低权限和职责分离的原则。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略
1.2	iam-group-has-users-check	AWS Identity and Access Management (IAM) 可以确保 IAM 群组至少有一个用户，从而帮助您将最低权限和职责分离原则与访问权限和授权相结合。根据用户的相关权限或工作职能将用户分组，是纳入最低权限的一种方法。

控制 ID	AWS Config 规则	指南
1.2	iam-inline-policy-blocked-kms-actions	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有允许对 AWS 所有密钥管理服务密钥执行阻止操作的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。此规则允许您设置 blockedActionsPatterns 参数。（AWS 基础安全最佳实践值：kms: decrypt，kms：From）。ReEncrypt实际值应反映贵组织的策略。
1.2	iam-no-inline-policy-check	确保 AWS 身份和访问管理 (IAM) Access Management 用户、IAM 角色或 IAM 群组没有控制系统和资产访问权限的内联策略。 AWS 建议使用托管策略而不是内联策略。托管策略允许可重用性、版本控制、回滚和委托权限管理。
1.2	iam-user-no-policies-check	该规则确保 AWS 身份和访问管理 (IAM) Access Management 策略仅附加到组或角色以控制对系统和资产的访问权限。在组或角色级别分配权限有助于减少身份获得或保留过多权限的机会。

控制 ID	AWS Config 规则	指南
1.2	restricted-ssh	Amazon Elastic Compute Cloud (Amazon EC2) 安全组可以对资源的入口和出口网络流量进行状态筛选，从而帮助管理网络访问。 AWS 不允许您资源上的入口（或远程）流量从 0.0.0.0/0 进入端口 22 有助于限制远程访问。
1.2	nacl-no-unrestricted-ssh-rdp	网络访问控制列表 (NACL) 中的远程服务器管理端口（例如端口 22 (SSH) 和端口 3389 (RDP)）不应设为可公开访问，因为这可能会允许对您的 VPC 内的资源进行意外访问。
1.2	s3-bucket-acl-prohibited	此规则检查访问控制列表 (ACL) 是否用于对 Amazon S3 存储桶进行访问控制。ACL 是 Amazon S3 存储桶的传统访问控制机制，早于 AWS 身份和访问管理 (IAM) Access Management。最佳实践是使用 IAM 策略或 S3 存储桶策略来更轻松地管理对 S3 存储桶的访问权限，而不是使用 ACL。

控制 ID	AWS Config 规则	指南
1.2	s3-bucket-logging-enabled	Amazon Simple Storage Service (Amazon S3) 服务器访问日志记录可提供一种监控网络中是否存在潜在网络安全事件的方法。通过捕获向 Amazon S3 存储桶发出的请求的详细记录，来监控事件。每条访问日志记录都提供有关单个访问请求的详细信息。这些详细信息包括请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果相关）。
1.2	s3-bucket-policy-grantee-check	启用 s3_ bucket_policy_grantee_check 来管理对 AWS 云的访问权限。该规则检查 Amazon S3 存储桶授予的访问权限是否受到您提供的任何 AWS 委托人、联合用户、服务委托人、IP 地址或亚马逊虚拟私有云 (Amazon VPC) ID 的限制。

控制 ID	AWS Config 规则	指南
1.2	sns-topic-message-delivery-notification-enabled	为了帮助满足环境中的日志记录要求，请确保在 Amazon Simple Notification Service (Amazon SNS) 主题中启用传送状态通知。记录消息传送状态有助于提供更好的操作见解，例如：了解消息是否已传送到 Amazon SNS 端点，识别从 Amazon SNS 端点发送到 Amazon SNS 的响应，以及确定消息停留时间（发布时间戳到移交给 Amazon SNS 端点之前的时间）。
1.4	internet-gateway-authorized-vpc-only	通过确保互联网网关仅连接到授权的亚马逊虚拟私有 AWS 云（Amazon VPC），来管理对云中资源的访问。互联网网关允许进出 Amazon VPC 的双向互联网访问，这可能会导致未经授权访问 Amazon VPC 资源。
1.4	restricted-common-ports	通过确保限制亚马逊弹性计算 AWS 云 (Amazon EC2) 安全组的常用端口，管理对云中资源的访问。如果不将端口访问限制为可信来源，可能会导致针对系统可用性、完整性和机密性的攻击。此规则允许您选择设置 blockedPort1 - blockedPort5 参数（Config 默认值：20,21,3389,3306,4333）。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
1.4	lambda-function-public-access-prohibited	通过确保无法公开访问 AWS Lambda 函数来管理对 AWS 云中资源的访问。公开访问可能导致资源可用性下降。
1.4	s3-account-level-public-access-blocks-periodic	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。此规则允许您选择设置（配置默认值：True）、 ignorePublicAcls（配置默认值：True）、blockPublicPolicy（配置默认值：True）和参数 blockPublicAcls（配置默认值：True）和 restrictPublicBuckets 参数（配置默认值：True）。实际值应反映贵组织的策略。
1.4	s3-bucket-level-public-access-prohibited	确保无法公开访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。该规则通过在存储桶级别防止公众访问，来帮助保护敏感数据免受未经授权的远程用户的访问。

控制 ID	AWS Config 规则	指南
1.4	s3-bucket-public-read-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.4	s3-bucket-public-write-prohibited	仅允许授权用户、进程和设备访问亚马逊简单存储服务 (Amazon S3) 存储桶，从而管理对 AWS 云端资源的访问权限。访问管理应与数据的分类保持一致。
1.4	ssm-document-not-public	确保 S AWS ystems Manager (SSM) 文档不公开，因为这可能会允许意外访问您的 SSM 文档。公开 SSM 文档可能会公开有关您的账户、资源和内部流程的信息。
2.3	ec2-imdsv2-check	确保启用实例元数据服务版本 2 (IMDSv2) 方法，以帮助保护对 Amazon Elastic Compute Cloud (Amazon EC2) 实例元数据的访问和控制。IMDSv2 方法使用基于会话的控制。使用 IMDSv2，可以实施控制来限制对实例元数据的更改。

控制 ID	AWS Config 规则	指南
2.3	ec2-instance-multiple-eni-check	此规则检查您的 Amazon Elastic Cloud (Amazon EC2) 实例是否有多个 ENI。拥有多个 ENI 可能会导致双宿主实例，即具有多个子网的实例。这可能会增加网络安全的复杂性，并引入意想不到的网络路径和访问。
2.3	ec2-token-hop-limit-check	确保实例元数据服务 (IMDS) HTTP PUT 响应仅限于 Amazon Elastic Compute Cloud (Amazon EC2) 实例。在 IMDSv2 中，默认情况下包含密钥令牌的 PUT 响应无法传送到实例之外，因为元数据响应跃点限制设置为 1（Config 默认值）。如果此值大于 1，则令牌可以离开 EC2 实例。
2.3	ec2-volume-inuse-check	此规则可确保附加到 Amazon Elastic Compute Cloud (Amazon EC2) 实例上的 Amazon Elastic Block Store 卷在实例终止时标记为删除。如果在附加到 Amazon EBS 卷的实例终止时，卷没有被删除，则可能违反最少功能的概念。
2.3	account-part-of-organizations	Organiz AWS ations AWS 账户 内部的集中管理有助于确保账户合规。缺乏集中式账户管理可能会导致账户配置不一致，从而可能泄露资源和敏感数据。

控制 ID	AWS Config 规则	指南
2.3	lambda-inside-vpc	在亚马逊虚拟私有云（亚马逊 VPC）中部署 AWS Lambda 函数，以便在亚马逊 VPC 内的函数与其他服务之间进行安全通信。使用此配置时，不需要互联网网关、NAT 设备或 VPN 连接。所有流量都安全地保存在 AWS 云中。由于进行了逻辑隔离，与使用公共终端节点的域相比，驻留在 Amazon VPC 中的域有一层额外的安全保护。为了正确管理访问权限，应 AWS 将 Lambda 函数分配给 VPC。
2.3	kms-cmk-not-scheduled-for-deletion	为了帮助保护静态数据，请确保在密钥管理服务 (KMS) 中没有计划删除必要的客户主 AWS 密AWS 钥 (CMK)。由于有时需要删除密钥，因此此规则可以帮助检查所有计划删除的密钥，以防密钥被无意中安排删除。
2.3	s3-bucket-versioning-enabled	Amazon Simple Storage Service (Amazon S3) 存储桶版本控制有助于将对象的多个变体保存在同一 Amazon S3 存储桶中。对于 Amazon S3 存储桶中存储的每个对象，使用版本控制功能来保存、检索和还原它们的各个版本。版本控制功能可帮助您轻松地从用户意外操作和应用程序故障中恢复。

控制 ID	AWS Config 规则	指南
2.3	secretsmanager-secret-unused	如果 S AWS ecrets Manager 中存在未使用的凭证，则应禁用和/或删除凭证，因为这可能违反最低权限原则。此规则允许您将值设置为 unusedForDays （ Config 默认值：90 ）。实际值应反映贵组织的策略。
2.5A	ebs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性区块存储 (Amazon EBS) 卷包含在备份计划中。 AWS AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2.5A	ec2-ebs-encryption-by-default	为了帮助保护静态数据，请确保为您的 Amazon Elastic Block Store (Amazon EBS) 卷启用加密。由于这些卷中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2.5A	efs-encrypted-check	由于可能存在敏感数据，并且为了帮助保护静态数据，请确保为您的 Amazon Elastic File System (EFS) 启用加密。

控制 ID	AWS Config 规则	指南
2.5A	efs-in-backup-plan	为了帮助完成数据备份流程，请确保您的亚马逊弹性文件系统（Amazon EFS）文件系统包含在 AWS 备份计划中。AWS Backup 是一项完全托管的备份服务，具有基于策略的备份解决方案。该解决方案可简化您的备份管理，使您能够满足业务和监管备份合规性要求。
2.5A	encrypted-volumes	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Elastic Block Store (Amazon EBS) 卷启用了加密。
2.5A	kinesis-stream-encrypted	由于可能存在敏感数据，并且为了帮助保护静态数据，应确保您的 Amazon Kinesis Streams 启用了加密。
2.5A	s3-bucket-server-side-encryption-enabled	为了帮助保护静态数据，请确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
2.5A	s3-default-encryption-kms	确保您的 Amazon Simple Storage Service (Amazon S3) 存储桶启用了加密。由于 Amazon S3 存储桶中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
2.5A	sns-encrypted-kms	为了帮助保护静态数据，请确保您的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题需要 AWS 使用密钥管理服务AWS (KMS) 进行加密。由于已发布的消息中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。

控制 ID	AWS Config 规则	指南
4.1	iam-password-policy	身份和凭证是根据组织 IAM 密码策略颁发、管理和验证的。它们符合或超过了 NIST SP 800-63 和密码强度 AWS 基础安全最佳实践标准规定的要求。此规则允许您选择为自己的 IAM 设置 RequireUppercaseCharacters（AWS 基础安全最佳实践值：true）、RequireLowercaseCharacters（AWS 基础安全最佳实践值：true）、 RequireSymbols（AWS 基础安全最佳实践值：true）、 RequireNumbers（AWS 基础安全最佳实践值：true）、 MinimumPasswordLength（AWS 基础安全最佳实践值：14）、PasswordReusePrevention（AWS 基础安全最佳实践值：24）和 MaxPasswordAge（AWS 基础安全最佳实践值：90）密码政策。实际值应反映贵组织的策略。

控制 ID	AWS Config 规则	指南
4.1	access-keys-rotated	通过确保按照组织策略的规定轮换 IAM 访问密钥，对授权设备、用户和流程的证书进行审计。定期更改访问密钥是一种安全最佳实践。它会缩短访问密钥的有效期，并降低密钥泄露时对业务的影响。此规则需要访问密钥轮换值（配置默认值：90）。实际值应反映贵组织的策略。
4.2	iam-user-mfa-enabled	启用此规则可限制对 AWS 云中资源的访问。此规则可确保为所有用户启用多重身份验证 (MFA)。MFA 在登录凭证之上添加一层额外的保护。要求用户进行多重身份验证，从而减少账户被盗事件。
4.2	mfa-enabled-for-iam-console-access	确保所有拥有控制台密码的 AWS 身份和访问管理 (IAM) Access Management 用户都启用 MFA，从而管理对 AWS 云中资源的访问权限。MFA 在登录凭证之上添加一层额外的保护。通过要求用户进行 MFA，您可以减少账户被盗事件，防止未经授权的用户访问敏感数据。

控制 ID	AWS Config 规则	指南
4.2	root-account-hardware-mfa-enabled	通过确保为根用户启用硬件 MFA 来管理对 AWS 云中资源的访问。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
4.2	root-account-mfa-enabled	通过确保为根用户启用 MFA 来管理对 AWS 云中资源的访问权限。根用户是 AWS 账户中权限最高的用户。MFA 为登录凭证增加了一层额外的保护。通过要求根用户进行 MFA，可以减少泄露事件。 AWS 账户
5.1	ec2-instance-profile-attached	EC2 实例配置文件将 IAM 角色传递给 EC2 实例。将实例配置文件附加到您的实例可以帮助实现最低权限和权限管理。
5.1	iam-policy-no-statements-with-full-access	确保 IAM 操作仅限于需要的那些操作。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。

控制 ID	AWS Config 规则	指南
5.1	iam-root-access-key-check	通过检查根用户的 AWS 身份和访问管理 (IAM) 角色是否没有附加访问密钥，可以控制对系统和资产的访问权限。确保删除根访问密钥。相反，创建和使用基于角色的 AWS 账户方法来帮助整合功能最少的原则。
5.1	iam-user-group-membership-check	AWS 身份与访问管理 (IAM) Access Management 可通过确保用户至少属于一个群组来帮助您限制访问权限和授权。允许用户拥有超过完成任务所需的权限，可能会违反最低权限和职责分离的原则。
5.1	iam-user-unused-credentials-check	AWS 身份与访问管理 (IAM) Access Management 可以通过检查指定时间段内未使用的 IAM 密码和访问密钥来帮助您获得访问权限和授权。如果发现这些未使用的凭证，则应禁用和/或删除这些凭证，因为这可能违反最低权限原则。此规则要求您为 “ maxCredentialUsage年龄” 设置一个值（Config 默认值：90）。实际值应反映贵组织的策略。
5.4	secretsmanager-rotation-enabled-check	此规则可确保 S AWS ecrets Manager 密钥已启用轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。

控制 ID	AWS Config 规则	指南
5.4	secretsmanager-scheduled-rotation-success-check	此规则可确保 S AWS ecrets Manager 密钥已根据轮换计划成功轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。
5.4	secretsmanager-secret-periodic-rotation	此规则可确保 S AWS ecrets Manager 密钥启用定期轮换。定期轮换机密可以缩短机密的有效期，并有可能减少机密泄露时对业务的影响。默认值为 90 天。
5.4	secretsmanager-using-cmk	为了帮助保护静态数据，请确保为 S AWS ecrets Manager 密 AWS 钥启用密钥管理服务 (AWS KMS) 加密。由于 Secrets Manager 机密中可能存在敏感的静态数据，因此应启用静态加密以帮助保护这些数据。
6.4	ec2-instance-detailed-monitoring-enabled	启用此规则可帮助改进 Amazon EC2 控制台上的 Amazon Elastic Compute Cloud (Amazon EC2) 实例监控，该控制台以 1 分钟为周期显示实例的监控图。
6.4	cloudwatch-log-group-encrypted	为帮助保护静态敏感数据，请确保您的 Amazon CloudWatch 日志组启用了加密。

控制 ID	AWS Config 规则	指南
6.4	cloud-trail-cloud-watch-logs-enabled	使用 Amazon CloudWatch 集中收集和管理日志事件活动。包含 AWS CloudTrail 数据可提供您内部的 API 调用活动的详细信息 AWS 账户。
6.4	cloudtrail-enabled	AWS CloudTrail 可以通过记录 AWS 管理控制台操作和 API 调用来帮助实现不可否认性。您可以识别用户和 AWS 账户调用 AWS 服务的用户、生成呼叫的源 IP 地址以及呼叫的时间。捕获数据的详细信息可在 “ AWS CloudTrail 记录内容” 中查看。
6.4	cloud-trail-encryption-enabled	由于可能存在敏感数据，为了帮助保护静态数据，请确保为您的 AWS CloudTrail 跟踪启用了加密。
6.4	cloud-trail-log-file-validation-enabled	利用 AWS CloudTrail 日志文件验证来检查 CloudTrail 日志的完整性。日志文件验证有助于确定日志文件在 CloudTrai l 传送后是否被修改、删除或未更改。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这使得在没有检测到的情况下修改、删除或伪造 CloudTrail 日志文件在计算上是不可行的。

控制 ID	AWS Config 规则	指南
6.4	ec2-stopped-instance	根据组织的标准，启用此规则可检查 Amazon EC2 实例停止运行的天数是否超过允许的天数，从而帮助进行 Amazon Elastic Compute Cloud (Amazon EC2) 实例的基线配置。
6.4	vpc-flow-logs-enabled	VPC 流日志详细记录进出 Amazon Virtual Private Cloud (Amazon VPC) 网络接口的 IP 流量信息。默认情况下，流日志记录包括 IP 流的不同组件的值，包括源、目标和协议。
6.5A	guardduty-enabled-centralized	Amazon GuardDuty 可以通过使用威胁情报源来帮助监控和检测潜在的网络安全事件。其中包括恶意 IP 列表和机器学习，用于识别 AWS 云环境中意外、未经授权和恶意的活动。

控制 ID	AWS Config 规则	指南
6.5A	securityhub-enabled	AWS Security Hub 有助于监控未经授权的人员、连接、设备和软件。 AWS Security Hub 汇总、整理来自多个服务的安全警报或发现，并对其进行优先排序。 AWS 其中一些服务包括Amazon Security Hub、Amazon Inspector、Amazon Macie、 AWS 身份和访问管理 (IAM) Access Analyzer、Firewall Manager 以及 AWS 合作伙伴解决方案。 AWS

模板

该模板可在以下网址获得 GitHub：SWIFT CSP 运营最佳实践。

Amazon Elastic Container Service (Amazon ECS) 安全最佳实践

此一致性包包含基于 Amazon ECS 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon ECS 安全最佳实践。

Amazon Elastic File System (Amazon EFS) 安全最佳实践

该合规包包含基于 Amazon EFS 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon EFS 安全最佳实践。

Amazon Elastic Kubernetes Service (Amazon EKS) 安全最佳实践

此一致性包包含基于 Amazon EKS 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon EKS 安全最佳实践。

Amazon 安全最佳实践 CloudFront

此合规包包含基于 Amazon CloudFront 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon 安全最佳实践 CloudFront。

Amazon OpenSearch 服务安全最佳实践

该合规包包含基于亚马逊 OpenSearch 服务的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon OpenSearch 服务安全最佳实践。

Amazon Redshift 安全最佳实践

此合规包包含基于亚马逊 Redshift 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：亚马逊 Redshift 安全最佳实践。

Amazon Relational Database Service (Amazon RDS) 安全最佳实践

此合规包包含基于 Amazon RDS 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon RDS 安全最佳实践。

AWS Auto Scaling安全最佳实践

此一致性包包含基于 AWS Auto Scaling的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：的安全最佳实践 AWS Auto Scaling。

AWS CloudTrail安全最佳实践

此一致性包包含基于 AWS CloudTrail的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：的安全最佳实践 AWS CloudTrail。

AWS CodeBuild安全最佳实践

此一致性包包含基于 AWS CodeBuild的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：的安全最佳实践 AWS CodeBuild。

Amazon ECR 安全最佳实践

该合规包包含基于亚马逊弹性容器注册表 (Amazon ECR) Container Registry 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon ECR 安全最佳实践。

AWS Lambda安全最佳实践

此一致性包包含基于 AWS Lambda的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：的安全最佳实践 AWS Lambda。

AWS Network Firewall安全最佳实践

此一致性包包含基于 AWS Network Firewall的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：的安全最佳实践 AWS Network Firewall。

Amazon 安全最佳实践 SageMaker

此合规包包含基于 Amazon SageMaker 的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：Amazon 安全最佳实践 SageMaker。

AWS Secrets Manager安全最佳实践

此一致性包包含基于 AWS Secrets Manager的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：的安全最佳实践 AWS Secrets Manager。

AWS WAF安全最佳实践

此一致性包包含基于 AWS WAF的 AWS Config 规则。有关支持的所有托管规则的列表 AWS Config，请参阅AWS Config 托管规则列表。

有关所需参数的名称和说明，请参阅以下模板中的`Parameters`部分。

该模板可在以下网址获得 GitHub：的安全最佳实践 AWS WAF。

具有修正操作的示例模板

具有修正功能的 Amazon DynamoDB 操作最佳实践

此模板可在 GitHub 上找到：具有修正功能的 Amazon DynamoDB 操作最佳实践。

具有修正功能的 Amazon S3 操作最佳实践

此模板可在 GitHub 上找到：具有修正功能的 Amazon S3 操作最佳实践。

有关模板结构的更多信息，请参阅《AWS CloudFormation 用户指南》中的模板剖析。

自定义合规包

自定义一致性包是唯一的 AWS Config 规则和补救措施集合，您可以将它们一起部署到一个账户和一个 AWS 区域，或者跨组织部署。 AWS Organizations

要创建自定义合规包，请按照以下自定义模板部分中的步骤创建一个 YAML 文件，其中包含要使用的 AWS Config 托管规则或 AWS Config 自定义规则列表。

术语

AWS Config 托管规则是所有者的预定义规则 AWS Config。

AWS Config 自定义规则是您从头开始创建的规则。

有两种方法可以创建 AWS Config 自定义规则：使用 Lambda 函数（AWS Lambda 开发者指南）和使用 Guard（Guard GitHub存储库）（一种 policy-as-code 语言）。 AWS Config 使用创建的 AWS Lambda 自定义规则称为AWS Config 自定义 Lambda 规则，使用 Guard 创建的 AWS Config 自定义规则称为AWS Config 自定义策略规则。

自定义模板

创建 YAML 文件

要创建 YAML 文件，请打开文本编辑器并将该文件另存为 .yaml。

> **Note**
>
> 您的文件将包含参数和资源部分。

参数

YAML 文件中的`Parameters`部分用于您将在本`Resources`节稍后添加的一组 AWS Config 规则的规则参数。通过将以下代码块复制并粘贴到您的 YAML 文件中，根据需要对其进行自定义，然后对每个规则参数重复此操作来创建 `Parameters` 部分。

```
Parameters:
    NameOfRuleParamNameOfRuleParameter:
        Default: Parameter value
        Type: Type
    ...
```

例如：

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
```

> **Note**
>
> 在选择 AWS Config 规则来构建您的自定义一致性包时，请检查您的账户中是否预配置了将根据规则进行评估的 AWS Config 资源。

1. 后面的参数部分的第一行`Parameters:`是 + Param *`NameOfRule`*+ 的串联字符串。*`NameOfRuleParameter`*

   a. 用您为该规则创建的一致名称替换 *`NameOfRule`*。例如，这可能是IamPasswordPolicy为了iam-password-policy 规则。

   b. 键入 `Param`。

   c. 然后，将 *`NameOfRuleParameter`* 替换为特定规则的规则参数名称。对于 AWS Config 托管规则，规则参数的名称位于AWS Config 托管规则列表中（例

如，MinimumPasswordLength是规则的规则参数的iam-password-policy名称）。对于 AWS Config 自定义规则，规则参数名称是您在创建该规则时选择的名称。

2. 如果您使用的是 AWS Config 托管规则，请在托管 AWS Config 规则列表中找到相应的规则，这样您就可以知道特定规则的接受值`Default`和`Type`可接受的值。对于 AWS Config 自定义规则，请使用您在创建规则时选择的值。

> **Note**
>
> `Type`必须为每个参数指定。 `Type`可以是 “字符串”、“int”、“double”、“CSV”、“布尔值” 和 “StringMap” 之一。

资源

`Resources` 部分列出了要添加到您的自定义合规包中的规则。在 `Parameters` 部分正下方添加以下 `Resources` 块，根据需要对其进行自定义，然后对每条规则重复此操作。有关规格的更多信息，请参阅AWS::Config::ConfigRule。

```
Resources:
     NameOfRule:
        Properties:
            ConfigRuleName: ActualConfigRuleName
            InputParameters:
                NameOfRuleParameter: NameOfRuleParamNameOfRuleParameter
            Source:
                Owner: Owner
                SourceIdentifier: SOURCE_IDENTIFIER
        Type: AWS::Config::ConfigRule
     ...
```

例如：

```
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
```

```
        Type: AWS::Config::ConfigRule
```

> **Note**
>
> 在选择用于构建自定义一致性包的 AWS Config 规则时，请检查您的账户中是否有资源可以根据预置的 AWS Config 规则进行评估。有关更多信息，请参阅支持的资源类型。

1. 将 *NameOfRule* 替换为您在 `Parameters` 部分中创建的相同名称。
2. 对于 AWS Config 托管规则，请*ActualConfigRuleName*替换为托AWS Config 管规则列表中相应规则页面的标题。对于 AWS Config 自定义规则，请使用您在创建规则时选择的 Config 规则名称。
3. 将 *NameOfRuleParameter* 替换为您在 `Parameters` 部分中使用的相同名称。在冒号之后，复制并粘贴您在小节中创建的 *NameOfRule*+ Param + *NameOfRuleParameter*的相同串联字符串。`Parameters`
4. 将 *Owner* 更改为相应的值。

   > **Note**
   >
   > AWS Config 托管规则
   > 对于 AWS Config 托管规则，的值`Owner`将为`AWS`。
   > AWS Config 自定义规则
   > 对于使用 Guard 创建的 AWS Config 自定义规则，的值`Owner`将为`CUSTOM_POLICY`。对于使用 Lambda 创建的 AWS Config 自定义规则，的值`Owner`将为。`CUSTOM_LAMBDA`

5. 将 *SOURCE_IDENTIFIER* 更改为相应的值。

   > **Note**
   >
   > AWS Config 托管规则
   > 对于 AWS Config 托管规则，请通过从托AWS Config 管规则列表中选择的规则中的链接复制标识符（例如，规则的源标识符是 ACCESS_KEYS_ RO access-keys-rotatedTATED）。
   > AWS Config 自定义规则
   > 对于使用 Lambda 创建的 AWS Config 自定义规则，`SourceIdentifier`是规则 AWS Lambda 函数的亚马逊资源名称 (ARN)，例如。`arn:aws:lambda:us-`

east-2:123456789012:function:*ActualConfigRuleName*对于使用 Guard 创建的 AWS Config 自定义规则，不需要此字段。

总而言之，您填写的自定义一致性包应开始看起来与以下内容类似，这是一个使用这些 AWS Config 托管规则的示例：iam-password-policyaccess-keys-rotated、和 iam-user-unused-credentials- check。

```
Parameters:
    IamPasswordPolicyParamMinimumPasswordLength:
        Default: '14'
        Type: String
    AccessKeysRotatedParamMaxAccessKeyAge:
        Default: '90'
        Type: String
    IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge:
        Default: '45'
        Type: String
Resources:
    IamPasswordPolicy:
        Properties:
            ConfigRuleName: iam-password-policy
            InputParameters:
                MinimumPasswordLength: IamPasswordPolicyParamMinimumPasswordLength
            Source:
                Owner: AWS
                SourceIdentifier: IAM_PASSWORD_POLICY
        Type: AWS::Config::ConfigRule
    AccessKeysRotated:
        Properties:
            ConfigRuleName: access-keys-rotated
            InputParameters:
                maxAccessKeyAge: AccessKeysRotatedParamMaxAccessKeyAge
            Source:
                Owner: AWS
                SourceIdentifier: ACCESS_KEYS_ROTATED
        Type: AWS::Config::ConfigRule
    IamUserUnusedCredentialsCheck:
        Properties:
            ConfigRuleName: iam-user-unused-credentials-check
            InputParameters:
                maxCredentialUsageAge:
 IamUserUnusedCredentialsCheckParamMaxCredentialUsageAge
            Source:
```

```
                Owner: AWS
                SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
        Type: AWS::Config::ConfigRule
```

部署自定义合规包

要部署您的自定义一致性包，请参阅使用部署一致性包 AWS Config 控制台和使用 AWS Config 命令行界面部署一致性包。

在“合规包”控制面板中查看合规性数据

合规包的主页显示您的 AWS 账户中当前拥有的所有合规包。此页面还包含每个合规包的名称、部署状态和合规性分数。合规性分数是合规包中的合规规则资源组合数量与合规包中可能的规则资源组合总数的百分比。

您可以使用此控制面板来了解合规包的合规性级别，并使用合规性分数来跟踪修复进度，对不同的需求集进行比较，并查看特定更改或部署对合规包的影响。

浏览合规包主页

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Config 控制台：https://console.aws.amazon.com/config/。
2. 导航至合规包页面。查看您的合规包及其合规性分数。您还可以执行以下操作：
   - 要添加和配置新的合规包，请选择部署合规包。
   - 要删除合格性包及其数据、更改配置设置或查看其他详细信息（例如传输位置或参数），请选择合规包，然后选择操作。

     > **Note**
     > 您无法编辑已部署的合规包。您可以随时修改其他选择，方法是选择合规包的名称，然后从操作下拉列表中选择编辑。

   - 要查看合规状态变更历史记录，请选择合规包，然后选择合规包时间线。有关更多信息，请参阅查看合规包的合规性历史记录时间线。
   - 要在详细视图中查看合规包的部署状态、合规性分数、合规性分数时间线和规则，请选择合规包，然后选择查看。

了解更多信息

合规包的先决条件

合规包示例模板

部署合规包

AWS 服务限制

查看合规包的合规性历史记录时间线

AWS Config 支持将合规性状态更改存储到您的一致性包中。这允许您查看合规性状态更改的历史记录。这些合规性状态更改以时间线的形式呈现。时间线将一段时间内的更改捕获为 `ConfigurationItems`。您还可以使用此功能在一致性包中查找不合规的特定规则。

您可以选择加入或选择退出记录 AWS Config中的所有资源类型。如果您选择记录所有资源类型，则 AWS Config 会自动开始记录 AWS Config 规则评估的合规包合规性历史记录。默认情况下， AWS Config 记录所有受支持资源的配置更改。您也可以仅选择特定的合规包的合规性历史记录资源类型：`AWS::Config::ConformancePackCompliance`。`AWS::Config::ConformancePackCompliance` 资源类型的记录不收取额外费用。有关更多信息，请参阅选择 AWS Config 记录哪些资源。

如果合规包中的所有规则都合规，则合规包即为合规。如果有任何规则不合规，则合规包为不合规。仅当由于数据不足而无法评估合规包中的所有规则时，合规包的合规性状态才为 INSUFFICIENT_DATA。如果合规包中的某些规则合规，但同一合规包中其他规则的合规状态为 INSUFFICIENT_DATA，则合规包将显示为合规。合规包的合规性不是一次性全部评估的。有些规则可能需要比其他规则更长的评估时间。一次对一组规则的合规性进行评估，分阶段持续进行，直到合规包中的所有规则都经过评估。

主题

- 查看合规性时间线
- 查询合规性历史记录

查看合规性时间线

从合规包主页中选择具体合规包，即可访问合规性时间表。

1. 导航至合规包页面。
2. 在合规包主页上，选择具体的合规包，然后选择合规包时间线。

> **Note**
>
> 或者，也可以使用合规包详细信息页面中的合规性时间线。选择合规包，然后在操作下拉列表中选择查看详细信息。在此页面中，选择合规包时间线。

时间线显示合规包的合规状态变化历史记录。您可执行以下操作：

1. 展开合规性变更以查看一致 line-by-line 性包中每条规则的合规性状态。
2. 从展开的视图中，选择特定规则以查看其详细信息页面。

查询合规性历史记录

get-resource-config-history 使用资源类型查询合规性历史记录`AWS::Config::ConformancePackCompliance`。

```
aws configservice get-resource-config-history --resource-type
 AWS::Config::ConformancePackCompliance --resource-id conformance-pack-ID
```

您应该可以看到类似于如下所示的输出内容：

```
{
    "configurationItems": [
        {
            "version": "1.3",
            "accountId": "Account ID",
            "configurationItemCaptureTime": 1614641951.442,
            "configurationItemStatus": "OK",
            "configurationStateId": "1614641951442",
            "configurationItemMD5Hash": "",
            "arn": "arn:aws:config:us-east-1:Account ID:conformance-
pack/MyConformancePack1/conformance-pack-ID",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
```

```
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        },
        {
            "version": "1.3",
            "accountId": "768311917693",
            "configurationItemCaptureTime": 1605551029.515,
            "configurationItemStatus": "ResourceDiscovered",
            "configurationStateId": "1605551029515",
            "configurationItemMD5Hash": "",
            "resourceType": "AWS::Config::ConformancePackCompliance",
            "resourceId": "conformance-pack-ID",
            "resourceName": "MyConformancePack1",
            "awsRegion": "us-east-1",
            "tags": {},
            "relatedEvents": [],
            "relationships": [],
            "configuration": "{\"compliantRuleCount\":1,\"configRuleList\":
[{\"configRuleName\":\"RuleName1-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-nnnnnn\",\"complianceType\":\"INSUFFICIENT_DATA\"},
{\"configRuleName\":\"RuleName2-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-mmmmmm\",\"complianceType\":\"COMPLIANT\"},
{\"configRuleName\":\"RuleName3-conformance-pack-ID\",\"controls\":[],\"configRuleArn
\":\"arn:aws:config:us-east-1:Account ID:config-rule/aws-service-rule/config-
conforms.amazonaws.com/config-rule-pppppp\",\"complianceType\":\"INSUFFICIENT_DATA\"}],
\"totalRuleCount\":3,\"nonCompliantRuleCount\":0,\"complianceType\":\"COMPLIANT\"}",
            "supplementaryConfiguration": {}
        }
    ]
}
```

有关更多信息，请参阅支持的资源类型 (AWS Config) 和 API 参考GetResourceConfigHistory中。

使用 AWS Config 控制台部署一致性包

在 Conformance packs (一致性包) 页面上，您可以为区域中的账户部署一致性包。您还可以编辑和删除已部署的一致性包。

使用模板部署合规包

您可以使用 AWS Config 示例模板或自己的自定义模板部署合规包。有关如何创建个性化合规包的说明，请参阅自定合规包。

1. 登录到 AWS Management Console，然后通过以下网址打开 AWS Config 控制台：https://console.aws.amazon.com/config/。
2. 导航到 Conformance packs (一致性包) 页面并选择 Deploy conformance pack (部署一致性包)。
3. 在 Specify template (指定模板) 页面上，选择示例模板或者使用现有模板。有关更多信息，请参阅合规包示例模板。

   - 如果您选择使用示例模板，请从示例模板的下拉列表中选择一个示例模板。

     有关每个模板内容的更多信息，请参阅“一致性包示例模板”。
   - 如果选择 模板已准备就绪，请指定模板源。示例模板可以是 Amazon S3 URI、AWS Systems Manager 文档（SSM 文档）或您上传的模板。

     如果您的模板大小超过 50 KB，请将其上传到 S3 存储桶并选择该 S3 存储桶位置。例如：s3://*bucketname/prefix*。

     > **Important**
     > 如果您基于自定义合规包从头开始创建合规包 YAML 文件，请选择模板已就绪。

4. 选择 Next（下一步）。
5. 在 Specify conformance pack details (指定一致性包详细信息) 页面上，键入您的一致性包的名称。

   一致性包名称必须是唯一的名称，最多有 256 个字母数字字符。名称可以包含连字符，但不能包含空格。
6. 可选：添加参数。

参数在模板中定义，可帮助您管理和组织资源。

7. 选择 Next（下一步）。
8. 在 Review and deploy (查看和部署) 页面上，查看所有信息。

   您可以通过选择 Edit (编辑) 来编辑模板详细信息和一致性包详细信息。

9. 选择 Deploy conformance pack (部署一致性包)。

   AWS Config 在一致性包页面上显示一致性包及其相应的状态。

   如果您的一致性包部署失败，请检查您的权限，验证您是否执行了先决条件步骤，然后重试。也可以联系 AWS Support。

要使用带有修正功能的示例模板部署一致性包，请参阅将一致性包与修正结合使用的先决条件以及上述过程。

要部署具有一个或多个 AWS Config 规则的一致性包，请参阅使用带有一条或多 AWS Config 条规则的一致性包的先决条件。

编辑一致性包

1. 要编辑一致性包，请从表中选择一致性包。
2. 选择 Actions，然后选择 Edit。
3. 在 Edit conformance pack (编辑一致性包) 页面上，您可以编辑模板详细信息、示例模板、一致性包和参数部分。

   您不能更改一致性包的名称。

4. 选择 Save changes（保存更改）。

   一致性包与 AWS Config 规则一起显示。

删除一致性包

1. 要删除一致性包，请从表中选择一致性包。
2. 选择 Actions，然后选择 Delete 。
3. 在删除#### 的对话框中，确认您是否希望永久删除此一致性包。

> **Important**
>
> 此操作无法恢复。删除一致性包时，您将删除该一致性包中的所有 AWS Config 规则和修正操作。

4. 输入 Delete (删除) 并选择 Delete (删除)。

   在 Conformance packs (一致性包) 页面上，您可以看到部署状态为 Deleting (正在删除)，直至一致性包删除完成。

使用 AWS Command Line Interface部署一致性包

您可以使用 AWS Command Line Interface (AWS CLI) 部署、查看、更新、查看合规 AWS Config 性状态和删除合规包。

AWS CLI 是一款用于管理您的 AWS 服务的统一工具。只需下载和配置一个工具，您就可以从命令行控制多项 AWS 服务，并使用脚本自动执行这些服务。有关 AWS CLI 和 AWS CLI 工具安装说明的更多信息，请参阅《AWS Command Line Interface 用户指南》中的以下内容。

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

如有必要`aws configure`，键入 AWS CLI 将配置为使用提供一致性包的 AWS 区域。

主题

- 部署一致性包
- 查看一致性包
- 查看一致性包状态
- 查看一致性包的合规状态
- 获取特定一致性包的合规详细信息
- 删除一致性包

部署一致性包

1. 打开命令提示符或终端窗口。

2. 键入以下命令以部署名为 **MyConformancePack** 的合规包。模板源可以是 Amazon S3 URI、您上传的模板或 AWS Systems Manager 文档（SSM 文档）。

   Amazon S3 URI

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-s3-uri "s3://AmazonS3BucketName/templateName.yaml"
   --delivery-s3-bucket AmazonS3BucketName
   ```

   本地目录中的 YAML 模板

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-body template body
   ```

   AWS Systems Manager 文档（Systems Manager 文档）

   ```
   aws configservice put-conformance-pack
   --conformance-pack-name MyConformancePack
   --template-ssm-document-details
    DocumentName=SSMDocumentName,DocumentVersion=SSMDocumentVersion
   --delivery-s3-bucket AmazonS3BucketName
   ```

3. 按 Enter 键运行命令。

   您应该可以看到类似于如下所示的输出内容。

   ```
   {
       "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
   MyConformancePack1/conformance-pack-ID"
   }
   ```

> **Note**
>
> 有关为合规包创建 YAML 模板的更多信息，请参阅自定义合规包。

查看一致性包

1. 输入以下 命令。

```
aws configservice describe-conformance-packs
```

或

```
aws configservice describe-conformance-packs --conformance-pack-
name="MyConformancePack1"
```

2. 您应该可以看到类似于如下所示的输出内容。

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "conformancePackInputParameters": [],
    "lastUpdateRequestedTime": "Thu Jul 18 16:07:05 PDT 2019"
}
```

查看一致性包状态

1. 输入以下 命令。

```
aws configservice describe-conformance-pack-status --conformance-pack-
name="MyConformancePack1"
```

2. 您应该可以看到类似于如下所示的输出内容。

```
{
    "stackArn": "arn:aws:cloudformation:us-west-2:AccountID:stack/
awsconfigconforms-MyConformancePack1-conformance-pack-ID/d4301fe0-
a9b1-11e9-994d-025f28dd83ba",
    "conformancePackName": "MyConformancePack1",
    "conformancePackId": "conformance-pack-ID",
    "lastUpdateCompletedTime": "Thu Jul 18 16:15:17 PDT 2019",
    "conformancePackState": "CREATE_COMPLETE",
```

```
    "conformancePackArn": "arn:aws:config:us-west-2:AccountID:conformance-pack/
MyConformancePack1/conformance-pack-ID",
    "lastUpdateRequestedTime": "Thu Jul 18 16:14:35 PDT 2019"
}
```

查看一致性包的合规状态

1. 输入以下 命令。

```
aws configservice describe-conformance-pack-compliance --conformance-pack-
name="MyConformancePack1"
```

2. 您应该可以看到类似于如下所示的输出内容。

```
{
    "conformancePackName": "MyConformancePack1",
    "conformancePackRuleComplianceList": [
        {
            "configRuleName": "awsconfigconforms-RuleName1-conformance-pack-ID",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "configRuleName": "awsconfigconforms-RuleName2-conformance-pack-ID",
            "complianceType": "COMPLIANT"
        }
    ]
}
```

获取特定一致性包的合规详细信息

1. 输入以下 命令。

```
aws configservice get-conformance-pack-compliance-details --conformance-pack-
name="MyConformancePack1"
```

2. 您应该可以看到类似于如下所示的输出内容。

```
{
    "conformancePackRuleEvaluationResults": [
        {
```

```
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Tue Jul 16 23:07:35 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName1-conformance-
pack-ID",
                    "resourceType": "AWS::::Account"
                }
            },
            "configRuleInvokedTime": "Tue Jul 16 23:07:50 PDT 2019",
            "resultRecordedTime": "Tue Jul 16 23:07:51 PDT 2019",
            "complianceType": "NON_COMPLIANT"
        },
        {
            "evaluationResultIdentifier": {
                "orderingTimestamp": "Thu Jun 27 15:16:36 PDT 2019",
                "evaluationResultQualifier": {
                    "resourceId": "resourceID",
                    "configRuleName": "awsconfigconforms-RuleName2-conformance-
pack-ID",
                    "resourceType": "AWS::EC2::SecurityGroup"
                }
            },
           "configRuleInvokedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "resultRecordedTime": "Thu Jul 11 23:08:06 PDT 2019",
            "complianceType": "COMPLIANT"
        }
    ],
    "conformancePackName": "MyConformancePack1"
}
}
```

删除一致性包

输入以下 命令。

```
aws configservice delete-conformance-pack --conformance-pack-name MyConformancePack1
```

如果成功，则命令会运行，而没有附加输出。

> **Important**
>
> 此操作无法恢复。删除一致性包时，即删除该一致性包中的所有 AWS Config 规则和补救操作。

管理合规包 (API)

使用以下 AWS Config API 操作来管理一致性包：

- DeleteConformance打包，删除指定的一致性包以及该一致性包中的所有 AWS Config 规则和所有评估结果。
- DescribeConformancePackCompliance，返回该一致性包中每条规则的合规性信息。
- DescribeConformance包，返回一个或多个一致性包的列表。
- DescribeConformancePackStatus，提供一个或多个一致性包部署状态。
- GetConformancePackCompliance详细信息，返回一致性包监控的所有 AWS 资源的一致性包的合规性详细信息。
- GetConformancePackCompliance摘要，根据一致性包中所有规则的累积合规结果返回该合规包的合规性信息。
- ListConformancePackCompliance分数，返回一致性包合规性分数列表。
- PutConformance打包、创建或更新一致性包。

跨组织中的所有账户管理一致性包

AWS Config 用于管理组织 AWS 账户 内所有的一致性包。您可执行以下操作：

- 在 AWS Organizations中，跨成员账户集中部署、更新和删除一致性包。
- 在所有账户中部署一组通用的 AWS Config 规则和修正操作，并指定不应在其中创建 AWS Config 规则和修正操作的帐户。
- 使用中的 AWS Organizations 管理账户通过确保组织的成员账户无法修改基础 AWS Config 规则和补救措施来实施治理。

注意事项

对于跨不同区域的部署

跨账户部署规则和一致性包的 API 调用因 AWS 区域而异。在组织级别，如果您想在其他区域部署规则，需要将 API 调用的上下文更改为其他区域。例如，要在美国东部（弗吉尼亚州北部）部署规则，应将区域更改为美国东部（弗吉尼亚州北部），然后调用 `PutOrganizationConfigRule`。

对用于组织内的账户

如果有新账户加入组织，会将相关的规则或合规包部署到该账户中。当账户离开组织时，相关的规则或合规包将被删除。

如果您在组织管理员账户中部署组织规则或合规包，然后建立委派管理员，并在委派管理员账户中部署组织规则或合规包，您将无法通过委派管理员账户在组织管理员账户中查看组织规则或合规包，也无法通过组织管理员账户查看委派管理员账户中的组织规则或合规包。DescribeOrganizationConfigRules和 DescribeOrganizationConformancePacksAPI 只能查看从调用这些 API 的账户内部部署的组织相关资源并与之交互。

添加到组织的新账户的重试机制

如果没有记录器，则只有在向组织添加账户后，才会重试部署现有组织规则和合规包 7 小时。如果在向组织添加账户后的 7 小时内没有记录器，则需要创建一个记录器。

组织管理账户、委派管理员和服务相关角色

如果您使用的是组织管理帐户并打算使用委派管理员进行组织部署，请注意这 AWS Config 不会自动创建服务相关角色 (SLR)。您必须使用 IAM 单独手动创建服务相关角色 (SLR)。

如果您的管理账户没有 SLR，则无法从委托管理员账户向该账户部署资源。您仍然可以从管理账户和委托管理员账户向成员账户部署一致性包。有关更多信息，请参阅 AWS Identity and Access Management (IAM) 用户指南中的使用服务相关角色。

部署

To deploy with the AWS Management Console

要通过 AWS 控制台在整个组织中部署一致性包，请使用 AWS Systems Manager。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的部署 AWS Config 一致性包。

To deploy with the AWS API

有关如何 AWS Config 与集成的信息 AWS Organizations，请参阅AWS Organizations 用户指南 AWS Organizations中的AWS Config 和。在使用以下 API 管理组织 AWS 账户 内所有合规包规则之前，请确保 AWS Config 录制已开启：

- DeleteOrganizationConformancePack，从该组织的所有成员账户中删除指定的组织一致性包以及所有配置规则和修正操作。
- DescribeOrganizationConformancePacks，返回组织一致性包列表。
- DescribeOrganizationConformancePack状态，提供组织的组织合规包部署状态。
- GetOrganizationConformancePackDetailedStatus，返回给定组织合规包中组织内每个成员帐户的详细状态。
- PutOrganizationConformancePack，在组织中的成员账户中部署一致性包。 AWS

区域支持

以下区域支持跨 AWS 组织成员账户部署合规包。

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS
美国西部（加利福尼亚北部）	us-west-1	config.us-west-1.amazonaws.com	HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS

区域名称	区域	端点	协议
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

故障排除

一致性包的失败状态

如果在创建、更新或删除一致性包时收到指示操作失败的错误，则可以检查一致性包的状态。

```
aws configservice describe-conformance-pack-status --conformance-pack-name
 MyConformancePack1
```

您应该可以看到类似于如下所示的输出内容。

```
"ConformancePackStatusDetails": [
    {
        "ConformancePackName": "ConformancePackName",
        "ConformancePackId": "ConformancePackId",
        "ConformancePackArn": "ConformancePackArn",
        "ConformancePackState": "CREATE_FAILED",
        "StackArn": "CloudFormation stackArn",
```

```
        "ConformancePackStatusReason": "Failure Reason",
        "LastUpdateRequestedTime": 1573865201.619,
        "LastUpdateCompletedTime": 1573864244.653
    }
]
```

有关故障的信息 ConformancePackStatusReason，请查看。

响应中有 stackArn 时

如果错误消息不明确，或者由于内部错误造成失败，请转到 AWS CloudFormation 控制台并执行以下操作：

1. 在输出中搜索 stackArn。
2. 选择 CloudFormation 堆栈的 “事件” 选项卡并检查是否有失败的事件。

   状态原因指示一致性包失败的原因。

响应中没有 stackArn 时

如果您在创建一致性包时收到失败，但状态响应中不存在 StackArn，则可能的原因是堆栈创建失败 CloudFormation 并回滚并删除了堆栈。前往 CloudFormation 控制台，搜索处于 “已删除” 状态的堆栈。失败的堆栈可能在那里可用。 CloudFormation 堆栈包含一致性包名称。如果找到失败的堆栈，请选择堆 CloudFormation 栈的 “事件” 选项卡并检查失败的事件。

如果这些步骤都不起作用，并且失败原因是内部服务错误，请重试操作或联系AWS Support 中心。

一致性包中的悬挂规则

部署一致性包涉及在后台创建底层 AWS CloudFormation 堆栈，以部署一致性包模板中的规则。这些规则是与服务相关的规则，不能在合规包之外更新或删除。

如果您对底层 CloudFormation 堆栈进行更改，则会导致一致性包及其规则变得难以管理。这些难以管理的规则是悬而未决的规则。

在 CloudFormation 堆栈和一致性包之间漂移

您可以直接从 CloudFormation 控制台更新一致性包模板中的规则名称。如果您直接从 CloudFormation 控制台更新模板，则不会更新已部署的一致性包。

这种漂移会产生悬空规则。如果您尝试从一致性包中删除规则，则会收到类似以下内容的错误：

```
"An AWS service owns ServiceLinkedConfigRule. You do not have permissions to
 take action on this rule. (Service: AmazonConfig; Status Code: 400; Error Code:
 AccessDeniedException; Request ID: my-request-ID; Proxy: null)".
```

如果您尝试删除一致性包，则无法删除悬挂规则，并且会收到类似以下内容的错误：

```
"User: arn:aws:sts::111122223333:assumed-role/AWSServiceRoleForConfigConforms/
AwsConfigConformsWorkflow is not authorized to perform: config:DeleteConfigRule on
 resource: my-dangling-rule
```

要修复此问题，请执行以下步骤：

1. 删除 堆栈。有关更多信息，请参阅《CloudFormation 用户指南》中的在 AWS CloudFormation 控制台上删除堆栈。
2. 使用 AWS Config 控制台或 Pack API 删除一致性DeleteConformance包。如果它是组织合规包，并且您使用的是管理账户或委托管理员账户，请使用 DeleteOrganizationConformancePackAPI。
3. 使用一致性包中悬挂规则的 Amazon 资源名称 (ARN) 联系AWS Support 中心，以帮助清理您的账户。

为避免出现此问题，请记住以下最佳实践：

- 切勿对一致性包 CloudFormation 堆栈进行任何直接更新。
- 切勿尝试进行在一致性包与其底层 CloudFormation 堆栈之间造成偏差的更改。
- 无法修改一致性包的服务关联角色 (SLR)。确保您正在更新的资源是 SLR 权限策略的一部分。

已删除一致性包的 CloudFormation 堆栈

除非 CloudFormation 堆栈和一致性包之间存在偏差，否则不建议直接从控制台删除一致性包或其 CloudFormation 堆栈中的规则。 CloudFormation

要解决此问题，请使用一致性包中悬挂规则的 Amazon 资源名称 (ARN) 联系AWS Support 中心，以帮助清理您的账户。

为避免出现此问题，请记住以下最佳实践：

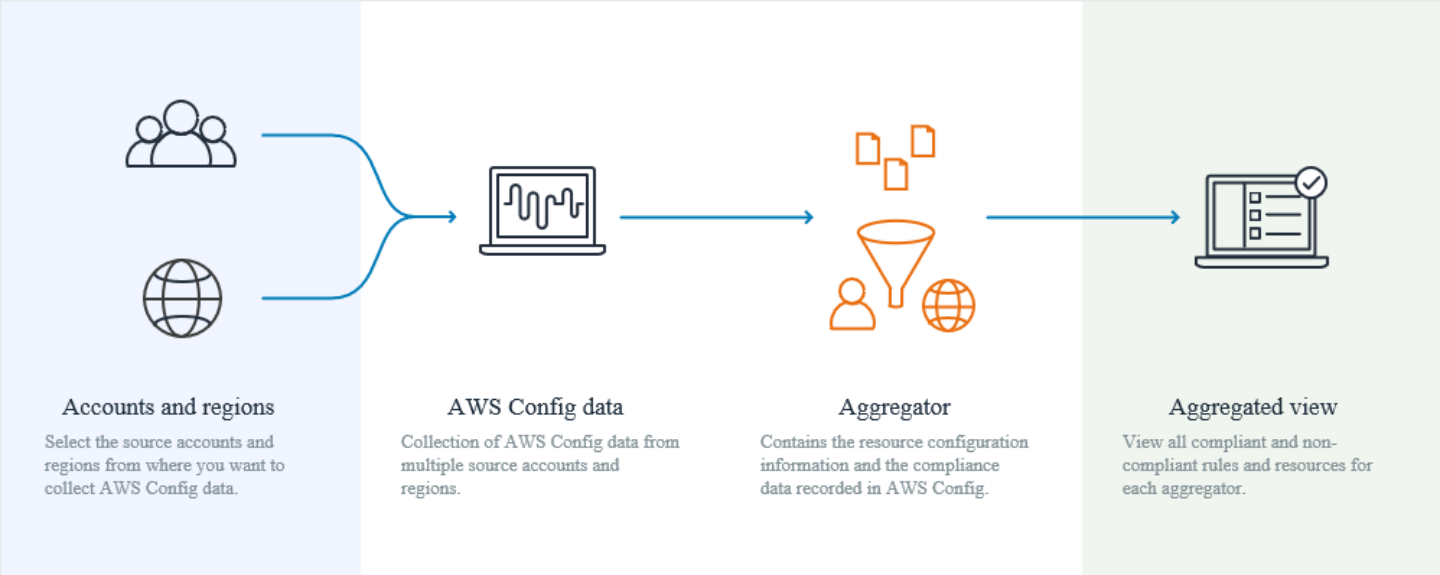
- 切勿删除一致性包的底层 CloudFormation 堆栈。
- 使用 DeleteConformancePack API 删除一致性包。如果它是组织合规包，并且您使用的是管理账户或委托管理员账户，请使用 DeleteOrganizationConformancePackAPI。

多账户多区域数据聚合

聚合器是一种从以下来源收集 AWS Config 配置和合规性数据的 AWS Config 资源类型：

- 多个账户和多个 AWS 区域。
- 单个账户和多个 AWS 区域。
- 一个组织中的一个组织 AWS Organizations 以及该组织中所有已 AWS Config 启用的账户。

使用聚合器查看在 AWS Config中记录的资源配置和合规性数据。聚合器使用 Amazon S3 存储桶来存储聚合数据。它会定期从源账户检索配置快照并将其存储在指定的 S3 存储桶中。下图显示了聚合器如何从多个账户和地区收集 AWS Config 数据。



应用场景

- 合规性监控：您可以汇总合规性数据，以评估组织或跨账户和地区的整体合规状况。
- 变更跟踪：您可以跟踪组织内或不同账户和地区的资源随时间推移而发生的变化。
- 资源关系：您可以分析整个组织或不同账户和地区的资源依赖关系和关系。

> **Note**
>
> 通过将数据从源账户复制到聚合器账户，聚合器可以提供源账户和区域的只读视图，聚合器有权查看这些视图。聚合器不提供对源账户或区域的变更访问权限。例如，这意味着您不能通过聚合器部署规则，也不能通过聚合器将快照文件推送到源账户或区域。
> 使用聚合器不会产生任何额外费用。

术语

源账户是您要 AWS 账户 从中汇总 AWS Config 资源配置和合规性数据的账户。源账户可以是 AWS Organizations中的个人账户或组织。您可以单独提供源帐户，也可以通过它们进行检索 AWS Organizations。

来源区域是您要从中汇总 AWS Config 配置和合规性数据的 AWS 区域。

聚合器账户是您在其中创建聚合器的账户。

授权是指您向聚合器账户和地区授予的收集 AWS Config 配置和合规性数据的权限。如果要聚合的源账户是 AWS Organizations的一部分，则不需要授权。

如何聚合数据

要汇总来自来源账户和地区的 AWS Config 数据，请从以下内容开始：

1. 添加聚合器以聚合来自多个账户和地区的 AWS Config 配置和合规性数据。有关更多信息，请参阅、使用控制台设置聚合器和使用设置聚合器 AWS Command Line Interface。
2. 授权聚合器账户收集 AWS Config 配置和合规性数据。有关更多信息，请参阅 使用控制台授权聚合器账户收集 AWS Config 配置和合规性数据 和 授权聚合器账户使用收集 AWS Config 配置和合规性数据 AWS Command Line Interface。

> **Note**
>
> 聚合器有两种类型：个人账户聚合器和组织聚合器
> 对于个人账户聚合器，任何包含的来源账户区域（包括外部账户区域或组织成员账户区域）都需要授权。
> 对于组织聚合器，组织成员账户区域不需要授权，因为授权已与 Organizations 服务集成。

3. 在聚合视图中监控规则和账户的合规性数据。有关更多信息，请参阅 在聚合器控制面板中查看合规性和清单数据。

区域支持

目前，以下区域支持多账户多区域数据聚合：

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS
美国西部（北加利福尼亚）	us-west-1	config.us-west-1.amazonaws.com	HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

多账户多区域数据聚合的故障排除

AWS Config 由于以下原因之一，可能无法聚合来自源帐户的数据：

如果发生这种情况	请执行该操作
AWS Config 未在组织内帐户的来源帐户中启用。	AWS Config 在源账户中启用并授权聚合器账户收集数据。
未给予聚合器账户授权。	登录来源账户并向聚合器账户授予收集 AWS Config 数据的授权。
可能存在阻止数据聚合的暂时性问题。	数据聚合可能会发生延迟。请等待几分钟。

AWS Config 由于以下原因之一，可能无法聚合来自组织的数据：

如果发生这种情况	请执行该操作
AWS Config 由于 IAM 角色无效，无法访问您的组织详细信息。	创建一个 IAM 角色，或从 IAM 角色列表中选择一个有效的 IAM 角色。

如果发生这种情况	请执行该操作
	Note 如果 IAM 角色的失效时间超过 24 小时，则 AWS Config 会删除整个组织的数据。
AWS Config 您的组织中已禁用服务访问权限。	您可以在 API 之间启用集成 AWS Config ，也可以 AWS Organizations 通过 `EnableAWSServiceAccess` API 实现集成。如果您选择在控制台中添加我的组织，则 AWS Config 会自动启用 AWS Config 和之间的集成 AWS Organizations。
AWS Config 无法访问您的组织详细信息，因为您的组织中未启用所有功能。	启用 AWS Organizations 控制台中的所有功能。
中东（巴林）和亚太地区（香港）区域不会立即更新组织变更，例如添加账户、删除账户、启用服务访问权限和禁用服务访问权限。	组织变更可能会有 2 小时的延迟。请等待 2 小时以查看所有组织变更。

在聚合器控制面板中查看合规性和清单数据

聚合器页面上的仪表板显示聚合 AWS 资源的配置数据。这些数据概述了您的规则、一致性包及其合规状态。

控制面板提供资源的总 AWS 资源数量。资源类型和源账户按最大数量的资源排列。还提供合规和不合规规则以及合规包的计数。不合规规则按不合规资源的最大数量进行排名。不合规的合规包和源账户按不合规规则的最大数量进行排名。

设置完成后 AWS Config，它开始将来自指定源帐户的数据聚合到聚合器中。显示规则的合规性状态可能需要几分钟时间。

使用聚合器控制面板

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。

2. 导航到聚合器页面。您可以查看：

   - 您的规则及其合规性状态。
   - 您的合规包及其合规性状态。
   - 您的 AWS 资源及其配置数据。

3. 从控制面板中选择聚合器。按聚合器名称筛选聚合器。您可以查看以下小组件：

   - 资源清单

     按资源计数降序查看所选聚合器中排名前 10 的资源类型。选择所选聚合器的资源总数（显示在资源清单后的括号中），以转到聚合资源页面，您可以在此页面上查看聚合器的所有资源。或者，也可以在小组件中选择一种资源类型，以转到使用指定资源类型筛选的聚合资源页面。

   - 按资源计数列出的账户

     按资源计数降序查看所选聚合器中排名前 5 的资源类型。在小组件中选择一个账户，以进入使用指定账户筛选的资源页面。

   - 不合规规则

     按照不合规资源的数量降序查看所选聚合器中排名前 5 的不合规规则。在小组件中选择一条规则，以进入指定规则的详细信息页面。选择查看所有不合规规则，以转至聚合规则页面，您可以在此页面上查看聚合器的所有规则。

   - 按不合规规则列出的账户

     按照不合规规则的数量降序查看所选聚合器中排名前 5 的账户。在小组件中选择一个账户，以进入聚合规则页面，您可以在此页面上查看使用指定账户筛选的聚合器的所有规则。

   - 按不合规的合规包列出的账户

     按照不合规的合规包数量降序查看所选聚合器中排名前 5 的账户。在小组件中选择一个账户，以进入聚合规则页面，您可以在此页面上查看使用指定账户筛选的聚合器的所有合规包。

4. 在左侧导航窗格中，从下拉菜单中选择下列选项之一：

   - 合规性控制面板

     使用汇总聚合器内资源合规性见解的小组件查看自动合规性控制面板。您可以查看数据，例如按不合规资源列出的排名前 10 的资源类型，以及按不合规规则列出的排名前 10 的账户级合规包。有关这些图形和图表的信息，请参阅合规性控制面板。

   - 一致性包

查看在聚合器中创建并链接到不同 AWS 账户 内容的所有一致性包。合规包页面显示一个表，其中列出每个合规包的名称、区域、账户 ID 和合规性状态。您可以在此页面中选择合规包，还可以查看详细信息，以了解有关其规则和资源及其合规性状态的更多信息。

- 规则

  查看在聚合器中创建并关联到不同 AWS 账户的所有规则。规则页面显示一个表，其中列出每条规则的名称、合规性状态、区域和账户。您可以在此页面中选择规则，还可以查看详细信息，以了解有关其聚合器、区域、账户 ID 和范围内资源的信息。

- 清单控制面板

  使用汇总聚合器内资源配置数据见解的小组件查看自动清单控制面板。您可以查看一些数据，例如，按资源计数排名前 10 的资源类型，以及按资源计数排名前 10 的账户。有关这些图形和图表的信息，请参阅清单控制面板。

- 资源

  查看在聚合器中记录并关联到不同 AWS 账户的所有资源。在资源页面中选择一个资源，然后选择查看详细信息，以查看其详细信息、与之关联的规则，以及当前的资源配置。您还可以查看有关资源的信息，例如其聚合器、区域、账户 ID、资源名称、资源类型和资源 ID。

- 授权

  查看并管理当前已授权或待授权的所有账户。在授权页面中，选择添加授权以提供对其他账户的访问权限。选择删除授权以撤消账户 ID 的访问权限。

> **Note**
>
> 故障排除
>
> 在聚合视图中会显示从所有源账户和区域收集的数据不完整消息，原因如下：
>
> - 正在传输不合规的 AWS Config 规则和 AWS 资源配置数据。
> - AWS Config 找不到与您应用的过滤器相匹配的规则。选择适当的账户或区域，然后重试。
>
> 您可能会在聚合视图中看到以下消息：从您的组织收集的数据不完整。您只能查看 24 小时的以下数据。显示此消息是由于以下原因：
>
> - AWS Config 由于 IAM 角色无效，无法访问您的组织详细信息。如果 IAM 角色无效的时间超过 24 小时， AWS Config 将会删除整个组织的数据。

- AWS Config 您的组织中已禁用服务访问权限。

合规性控制面板

使用汇总聚合器内资源合规性见解的小组件查看自动合规性控制面板。此控制面板只显示具有合规性结果的规则。

> **Note**
>
> 限制
>
> 合规性控制面板中的见解由的高级查询功能提供 AWS Config，此功能不支持嵌套结构或解压缩嵌套数组。这意味着合规性控制面板显示的是资源的总体合规性，而不是报告资源的每条特定规则的合规性状态。
>
> 例如，如果您检查资源类型的配置项目 (CI)`AWS::Config::ResourceCompliance`，控制面板将显示报告该资源的所有规则的合规性结果。如果有 10 条规则报告资源，其中 9 条合规，只有 1 条不合规，则该资源的总体合规性将不合规。

按资源列出的合规性摘要

显示一个饼图，将选定聚合器的合规资源数量与不合规资源的数量进行比较。将鼠标悬停在图表上可查看合规和不合规资源的确切数量和百分比。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按不合规资源排列的前 10 种资源类型

显示一个水平条形图，按不合规资源的数量降序比较选定聚合器中最多 10 种资源类型。将鼠标悬停在图表上，可查看每种资源类型不合规资源的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按不合规资源排列的前 10 个账户

按不合规资源排列的前 10 个账户会显示一个水平条形图，按不合规资源的数量降序比较选定聚合器中最多 10 个账户。将鼠标悬停在图表上可查看每个账户的不合规资源的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

不合规资源排名前 10 的地区

显示一个水平条形图，比较最多 10 个区域，在这些区域中，选定的聚合器按不合规资源的数量降序收集数据。将鼠标悬停在图表上可查看每个区域的不合规资源的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置。

不合规规则排名前十的账户级别合规包

显示一个水平条形图，按不合规规则的数量降序比较来自选定聚合商的最多 10 个账户级别一致性包。将鼠标悬停在图表上，查看每个账户级别一致性包中合规和不合规规则的百分比。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按不合规规则排列的十大组织级别合规包

显示一个水平条形图，按不合规规则的数量降序比较选定聚合器中最多 10 个组织级别的一致性包。将鼠标悬停在图表上可查看每个组织级别一致性包中合规和不合规规则的百分比。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

合规包中按不合规规则排列的前 10 个账户

合规@@ 包中按不合规规则排列的前 10 个账户会显示一个水平条形图，按所有一致性包中不合规规则的数量降序比较选定聚合器中最多 10 个账户。将鼠标悬停在图表上可查看每个账户中不合规规则的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

清单控制面板

使用汇总聚合器内资源配置数据见解的小组件查看自动清单控制面板。

按资源计数列出的排名前 10 的资源类型

显示一个水平条形图，按资源计数降序比较选定聚合器中最多 10 种资源类型。将鼠标悬停在图表上，可查看每种资源类型的确切资源数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按区域列出的资源计数

显示一个水平条形图，按资源计数降序比较选定聚合器收集数据的最多 10 个区域。将鼠标悬停在图表上，可查看每个区域的确切资源数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置。

按资源计数列出的排名前 10 的账户

显示一个水平条形图，按资源计数降序比较选定聚合器中最多 10 个账户。将鼠标悬停在图表上，可查看每种资源类型的确切资源数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。

按 Amazon EC2 服务资源类型列出的资源计数

显示一个水平条形图，按资源计数降序比较选定聚合器中的 Amazon EC2 资源类型。将鼠标悬停在图表上，可查看每种 Amazon EC2 资源类型的确切资源数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。要使用此图表，您必须将记录器配置为记录 Amazon EC2 资源类型。有关更多信息，请参阅选择 AWS Config 记录哪些资源。

使用的排名前 10 的 EC2 实例类型

显示一个水平条形图，按使用情况降序比较选定聚合器中最多 10 个 Amazon EC2 实例类型。将鼠标悬停在图表上，可查看每种 EC2 实例类型的使用情况。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。要使用此图表，您必须将记录器配置为记录 EC2 实例资源类型。有关更多信息，请参阅重新编码 AWS 资源。

按卷类型和大小列出的 EBS 卷计数

显示一个垂直条形图，按资源计数比较选定聚合器中的 EBS 卷。将鼠标悬停在图表上，可查看每种类型的 EBS 卷的计数和大小明细。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。要使用此图表，您必须将记录器配置为记录 EC2 卷资源类型。有关更多信息，请参阅选择 AWS Config 记录哪些资源。

按类型列出的正在运行的 EC2 实例数量与已停止的 EC2 实例数量

显示一个水平条形图，按实例类型比较选定聚合器中正在运行的 EC2 实例类型与已停止的 EC2 实例。将鼠标悬停在图表上，可查看每种类型已停止的 EC2 实例和正在运行的 EC2 实例的确切数量。

显示的数据取决于所选聚合器中每个账户的配置记录器设置，以及所选聚合器配置为收集数据的区域。要使用此图表，您必须将记录器配置为记录 EC2 实例资源类型。有关更多信息，请参阅重新编码 AWS 资源。

使用控制台设置聚合器

在 Aggregator 页面上，可以执行以下操作：

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

主题

- 创建聚合器
- 编辑聚合器
- 删除聚合器

创建聚合器

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 导航到聚合器页面，然后选择创建聚合器。
3. 允许数据复制，允许将数据从源帐户复制 AWS Config 到聚合器帐户。

   选择 AWS Config 允许将数据从源帐户复制到聚合器帐户。您须选中此复选框，才能继续添加聚合器。
4. 对于 Aggregator name，键入聚合器的名称。

   聚合器名称必须是唯一的名称，最多有 64 个字母数字字符。此名称可以包含连字符和下划线。
5. 对于 Select source accounts，选择您要从中聚合数据的 Add individual account IDs 或 Add my organization。

> **Note**
> 使用添加单个账户 ID 来选择源账户时，需要获得授权。

- 如果您选择 Add individual account IDs，则可以为聚合器账户添加个人账户 ID。
  1. 选择 Add source accounts 以添加账户 ID。
  2. 选择 “添加 AWS 账户 ID” 以手动添加以逗号分隔 AWS 账户 的 ID。如果您想要从当前账户中聚合数据，请键入账户的账户 ID。

     或

     选择 “上传文件”，上传以逗号 AWS 账户 分隔 ID 的文件（.txt 或.csv）。
  3. 选择 Add source accounts 以确认您的选择。
- 如果您选择 Add my organization，则可以将您组织中的所有账户添加到聚合器账户。

> **Note**
> 您必须登录到管理账户或注册的委派管理员，并且所有功能都必须在组织中处于启用状态。如果来电者是管理账号，则 AWS Config 调用 `EnableAwsServiceAccess` API 以启用 AWS Config 和之间的集成 AWS Organizations。如果来电者是注册的委托管理员，则 AWS Config 调用 `ListDelegatedAdministrators` API 来验证来电者是否是有效的委托管理员。
> 在授权的管理员创建聚合器之前，请确保管理账户注册 AWS Config 服务主体名称 (config.amazonaws.com) 的委派管理员。要注册委派管理员，请参阅注册委派管理员。

您必须分配一个 IAM 角色 AWS Config 才能允许您为组织调用只读 API。

1. 选择从您的账户选择一个角色，以选择现有 IAM 角色。

> **Note**
> 在 IAM 控制台中，将 `AWSConfigRoleForOrganizations` 托管策略附加到您的 IAM 角色。附加此政策 AWS Config 允许调用 AWS Organizations `DescribeOrganization`、`ListAWSServiceAccessForOrganization`、和

> `ListAccounts` API。默认情况下，`config.amazonaws.com` 会被自动指定为可信实体。

2. 或者，选择创建角色，然后键入 IAM 角色名称以创建 IAM 角色。

6. 对于 Regions，选择您要为其聚合数据的区域。
   - 选择一个区域或多个区域或所有 AWS 区域。
   - 选择 In clude fut AWS 区域 ure 可聚合所有 AWS 区域 启用多账户多区域数据聚合的未来数据。
7. 选择 “保存”。 AWS Config 显示聚合器。

编辑聚合器

1. 要对聚合器进行更改，请选择聚合器名称。
2. 选择 Actions，然后选择 Edit。
3. 使用编辑聚合器页面上的相关部分来更改聚合器的源账户、IAM 角色或区域。

> **Note**
>
> 您无法将源类型从个人账户更改为组织，反之亦然。

4. 选择保存。

删除聚合器

1. 要删除聚合器，请选择聚合器名称。
2. 选择 操作，然后选择 删除。

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

使用设置聚合器 AWS Command Line Interface

您可以使用 AWS Command Line Interface (AWS CLI) 创建、查看、更新和删除 AWS Config 聚合器数据。

AWS CLI 是用于管理您的 AWS 服务的统一工具。只需下载和配置一个工具，您就可以从命令行控制多项 AWS 服务，并使用脚本自动执行这些服务。有关 AWS CLI 和 AWS CLI 工具安装说明的更多信息，请参阅《AWS Command Line Interface 用户指南》中的以下内容。

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

如有必要，`aws configure`请输入配置 AWS CLI 为使用有聚合器的 AWS 区域。

主题

- 使用个人账户添加聚合器
- 使用 AWS Organizations 添加聚合器
- 注册委派管理员
- 查看聚合器
- 编辑聚合器
- 删除聚合器

使用个人账户添加聚合器

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

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

   对于 `account-aggregation-sources`，输入以下内容之一。

   - 要聚合其数据的 AWS 账户 ID 的逗号分隔列表。用方括号将账户 ID 括起来，并确保对引号进行转义 (例如，`"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`)。

- 您也可以上传以逗号分隔 AWS 账户 的 ID 的 JSON 文件。上传文件使用以下语法：`--account-aggregation-sources` *`MyFilePath/MyFile.json`*

  JSON 文件必须为以下格式：

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

3. 按 Enter 执行命令。

   您应该可以看到类似于如下所示的输出内容：

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3"
                ]
            }
        ],
        "LastUpdatedTime": 1517942461.442
    }
}
```

使用 AWS Organizations 添加聚合器

在开始本过程之前，您必须先登录到管理账户或注册的委派管理员，并且所有功能都必须在组织中处于启用状态。

> **Note**
>
> 在委派管理员创建聚合器之前，请确保管理账户使用以下两个 AWS Config 服务主体名称（`config.amazonaws.com`和`config-multiaccountsetup.amazonaws.com`）注册委派管理员。要注册委派管理员，请参阅注册委派管理员。

1. 打开命令提示符或终端窗口。
2. 如果尚未为 AWS Config 聚合器创建 IAM 角色，请输入以下命令：

```
aws iam create-role --role-name OrgConfigRole --assume-role-policy-document
 "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":\"\",\"Effect\":\"Allow\",
\"Principal\":{\"Service\":\"config.amazonaws.com\"},\"Action\":\"sts:AssumeRole
\"}]}" --description "Role for organizational AWS Config aggregator"
```

> **Note**
>
> 复制此 IAM 角色中的亚马逊资源名称 (ARN)，以便在创建聚合器时使用。 AWS Config 您可以在响应对象上找到 ARN。

3. 如果尚未将策略附加到您的 IAM 角色，请附加AWSConfigRoleForOrganizations托管策略或输入以下命令：

```
aws iam create-policy --policy-name OrgConfigPolicy --policy-document
 '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Action":
["organizations:ListAccounts","organizations:DescribeOrganization","organizations:ListAWSSe
```

4. 输入以下命令以创建一个名为 **`MyAggregator`** 的聚合器。

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

5. 按 Enter 执行命令。

您应该可以看到类似于如下所示的输出内容：

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

注册委派管理员

委派管理员是指给定 AWS 组织内被授予特定 AWS 服务的额外管理权限的账户。

1. 使用管理账户凭证登录。
2. 打开命令提示符或终端窗口。
3. 输入以下命令以授权管理员的身份为组织启用服务访问权限，以便在整个组织中部署和管理 AWS Config 规则和一致性包：

```
aws organizations enable-aws-service-access --service-principal=config-
multiaccountsetup.amazonaws.com
```

4. 输入以下命令以授权管理员的身份为您的组织启用服务访问权限，以便在整个组织中聚合 AWS Config 数据：

```
aws organizations enable-aws-service-access --service-
principal=config.amazonaws.com
```

5. 要检查启用服务访问权限是否已完成，请输入以下命令并按 Enter 执行此命令。

```
aws organizations list-aws-service-access-for-organization
```

您应该可以看到类似于如下所示的输出内容：

```
{
    "EnabledServicePrincipals": [
        {
            "ServicePrincipal": [
                "config.amazonaws.com",
                "config-multiaccountsetup.amazonaws.com"
        ],
            "DateEnabled": 1607020860.881
        }
    ]
}
```

6. 接下来，输入以下命令以注册一个成员账户作为 AWS Config的委派管理员。

```
aws organizations register-delegated-administrator --service-principal=config-
multiaccountsetup.amazonaws.com --account-id MemberAccountID
```

以及

```
aws organizations register-delegated-administrator --service-
principal=config.amazonaws.com --account-id MemberAccountID
```

7. 要检查委派管理员注册是否已完成，请从管理账户中输入以下命令，然后按 Enter 键执行该命令。

```
aws organizations list-delegated-administrators --service-principal=config-
multiaccountsetup.amazonaws.com
```

以及

```
aws organizations list-delegated-administrators --service-
principal=config.amazonaws.com
```

您应该可以看到类似于如下所示的输出内容：

```
{
    "DelegatedAdministrators": [
        {
            "Id": "MemberAccountID",
```

```
            "Arn": "arn:aws:organizations::MemberAccountID:account/o-
c7esubdi38/MemberAccountID",
            "Email": "name@amazon.com",
            "Name": "name",
            "Status": "ACTIVE",
            "JoinedMethod": "INVITED",
            "JoinedTimestamp": 1604867734.48,
            "DelegationEnabledDate": 1607020986.801
        }
    ]
}
```

查看聚合器

1. 输入以下 命令：

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

2. 根据您的源账户，您应该看到类似于以下内容的输出：

   对于个人账户

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "MyAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
```

```
}
```

或

对于组织

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

编辑聚合器

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

   输入以下命令以向 **MyAggregator** 添加新的账户 ID：

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

2. 根据您的源账户，您应该看到类似于以下内容的输出：

   对于个人账户

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-xz2upuu6",
        "CreationTime": 1517952090.769,
        "ConfigurationAggregatorName": "MyAggregator",
```

```
        "AccountAggregationSources": [
            {
                "AllAwsRegions": true,
                "AccountIds": [
                    "AccountID1",
                    "AccountID2",
                    "AccountID3",
                    "AccountID4"
                ]
            }
        ],
        "LastUpdatedTime": 1517952566.445
    }
}
```

或

对于组织

```
{
    "ConfigurationAggregator": {
        "ConfigurationAggregatorArn": "arn:aws:config:Region:AccountID:config-
aggregator/config-aggregator-floqpus3",
        "CreationTime": 1517942461.442,
        "ConfigurationAggregatorName": "MyAggregator",
        "OrganizationAggregationSource": {
                "AllAwsRegions": true,
                "RoleArn": "arn:aws:iam::account-of-role-to-assume:role/name-of-
role"
         },
        "LastUpdatedTime": 1517942461.442
    }
}
```

删除聚合器

输入以下 命令：

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

如果成功，则命令会执行，而没有附加输出。

使用控制台授权聚合器账户收集 AWS Config 配置和合规性数据

AWS Config 允许您授权账户收集 AWS Config 配置和合规性数据。

在 Authorizations 页面上，可以执行以下操作：

- 添加授权以允许指定聚合器账户和区域从您的当前账户收集 AWS Config 配置和合规性数据。
- 授权来自聚合器账户的待处理请求从您的当前账户收集 AWS Config 配置和合规性数据。
- 删除聚合器账户从您的当前账户收集 AWS Config 配置和合规性数据的授权。

主题

- 注意事项
- 为聚合器账户和区域添加授权
- 授权针对聚合器账户的待处理请求
- 删除对现有聚合器账户的授权

注意事项

聚合器有两种类型：个人账户聚合器和组织聚合器

对于个人账户聚合器，您要包含的所有源账户和区域都需要授权，包括外部账户和区域，以及组织成员账户和区域。

对于组织聚合器，组织成员账户区域无需授权，因为授权已与 AWS Organizations 服务集成。

聚合器不会自动代表您 AWS Config 启用

AWS Config 需要在来源账户和区域中为任一类型的聚合器启用，才能在源账户和区域中生成 AWS Config 数据。

为聚合器账户和区域添加授权

您可以添加授权，向聚合器账户和区域授予收集 AWS Config 配置和合规性数据的权限。

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。

2. 导航到 Authorizations 页面，然后选择 Add authorization。
3. 对于 Aggregator account，键入聚合器账户的 12 位数账户 ID。
4. 对于聚合器区域，选择允许聚合器账户收集 Config AWS 配置和合规性数据 AWS 区域 的位置。
5. 选择 Add authorization 以确认您的选择。

   AWS Config 显示聚合器账户、区域和授权状态。

> **Note**
>
> 您还可以使用 AWS CloudFormation 示例模板以编程方式向聚合器账户和区域添加授权。有关更多信息，请参阅AWS::Config::AggregationAuthorization《AWS CloudFormation 用户指南》。

授权针对聚合器账户的待处理请求

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

1. 选择要授权的聚合器账户，然后选择授权。

   将显示一条确认消息，确认您要向聚合器账户授予从该账户收集 AWS Config 数据的权限。
2. 再次选择授权，以确认您要向此聚合器账户授予权限。

   授权状态从 Requesting for authorization 更改为 Authorized。

授权批准期限

向个人账户聚合器添加源账户需要获得授权批准。在个人账户聚合器添加源账户后，待处理的授权批准请求将在 7 天内有效。

删除对现有聚合器账户的授权

1. 选择要删除授权的聚合器账户，然后选择删除。

   此时会显示一条警告消息。删除此授权后， AWS Config 数据将不再与聚合器帐户共享。
2. 再次选择删除以确认您的选择。

该聚合器账户现已被删除。

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

授权聚合器账户使用收集 AWS Config 配置和合规性数据 AWS Command Line Interface

您可以使用 AWS Command Line Interface ()AWS CLI授权聚合器帐户从源帐户收集 AWS Config 数据并删除聚合器帐户。要使用 AWS 管理控制台，请参阅使用控制台授权聚合器账户收集 AWS Config 配置和合规性数据。

AWS CLI 是一款用于管理您的 AWS 服务的统一工具。只需下载和配置一个工具，您就可以从命令行控制多项 AWS 服务，并使用脚本自动执行这些服务。有关 AWS CLI 和 AWS CLI 工具安装说明的更多信息，请参阅《AWS Command Line Interface 用户指南》中的以下内容。

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

如有必要`aws configure`，键入 AWS CLI 将配置为使用提供 AWS Config 一致性包的 AWS 区域。

主题

- 注意事项
- 为聚合器账户和区域添加授权
- 删除授权账户

注意事项

聚合器有两种类型：个人账户聚合器和组织聚合器

对于个人账户聚合器，您要包含的所有源账户和区域都需要授权，包括外部账户和区域，以及组织成员账户和区域。

对于组织聚合器，组织成员账户区域无需授权，因为授权已与 AWS Organizations 服务集成。

聚合器不会自动代表您 AWS Config 启用

AWS Config 需要在来源账户和区域中为任一类型的聚合器启用，才能在源账户和区域中生成 AWS Config 数据。

为聚合器账户和区域添加授权

1. 打开命令提示符或终端窗口。
2. 输入以下 命令：

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

3. 您应该可以看到类似于如下所示的输出内容：

```
{
    "AggregationAuthorization": {
        "AuthorizedAccountId": "AccountID",
        "AggregationAuthorizationArn":
 "arn:aws:config:Region:AccountID:aggregation-authorization/AccountID/Region",
        "CreationTime": 1518116709.993,
        "AuthorizedAwsRegion": "Region"
    }
}
```

删除授权账户

输入以下 命令：

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

如果成功，则命令会执行，而没有附加输出。

查询 AWS 资源的当前配置状态

为高级查询引入了预览功能，允许您使用生成式人工智能（生成人工智能）功能以通俗易懂的英语输入提示并将其转换为 ready-to-use 查询格式。有关更多信息，请参阅适用于高级查询的自然语言查询处理器。

您可以使用 AWS Config 根据单个账户和区域的配置属性或跨多个账户和区域查询 AWS 资源的当前配置状态。您可以对支持的资源列表中的当前 AWS 资源状态元数据执行基于属性的查询。 AWS Config 有关支持的资源类型列表的更多信息，请参阅支持的高级查询资源类型。

高级查询提供单一查询端点和一种查询语言，无需执行特定于服务的描述 API 调用即可获取当前资源状态元数据。您可以使用配置聚合器从一个中央账户跨多个账户和 AWS 地区运行相同的查询。

主题

- 功能
- 查询组件
- 示例查询
- 关系查询示例
- 限制
- 区域支持
- 查询使用 SQL 查询编辑器进行查询（控制台）
- 使用 SQL 查询编辑器 (AWS CLI) 进行查询
- 适用于高级查询的自然语言查询处理器

功能

AWS Config 使用结构化查询语言 (SQL) `SELECT` 语法的子集对当前配置项 (CI) 数据执行基于属性的查询和聚合。查询的复杂程度各不相同，从与标签和/或资源标识符的匹配到更复杂的查询，例如查看所有禁用版本控制的 Amazon S3 存储桶。这样，您就可以精确地查询您所需的当前资源状态，而无需执行特定于 AWS 服务的 API 调用。

它支持聚合函数，例如 `AVG`、`COUNT`、`MAX`、`MIN` 和 `SUM`。

您可以使用高级查询来实现：

- 清单管理；例如，检索特定大小的 Amazon EC2 实例的列表。
- 安全和运营智能；例如，检索已启用或禁用特定配置属性的资源的列表。
- 成本优化；例如，确定未附加到任何 EC2 实例的 Amazon EBS 卷的列表。
- 合规性数据；例如，检索所有合规包及其合规性状态的列表。

有关如何使用 AWS SQL 查询语言的信息，请参阅什么是 SQL（结构化查询语言）？ 。

查询组件

SQL SELECT 查询组件如下所示。

摘要

```
SELECT property [, ...]
[ WHERE condition ]
[ GROUP BY property ]
[ ORDER BY property [ ASC | DESC ] [, property [ ASC | DESC ] ...] ]
```

参数

[WHERE condition]

根据您指定的 `condition` 筛选结果。

[GROUP BY property]

将结果集聚合到包含与给定的属性匹配的值的行组中。

GROUP BY 子句适用于聚合。

[ORDER BY property [ASC | DESC] [, property [ASC | DESC] ...]]

按一个或多个输出 `properties` 对结果集进行排序。

当该子句包含多个属性时，结果集将根据第一个 `property` 进行排序，然后针对包含与第一个属性匹配的值的行根据第二个 `property` 进行排序，以此类推。

示例

```
SELECT resourceId WHERE resourceType='AWS::EC2::Instance'
```

```
SELECT configuration.complianceType, COUNT(*) WHERE resourceType =
 'AWS::Config::ResourceCompliance' GROUP BY configuration.complianceType
```

示例查询

Query to list all EC2 instances with AMI ID ami-12345

查询：

```
SELECT
    resourceId,
    resourceType,
    configuration.instanceType,
    configuration.placement.tenancy,
    configuration.imageId,
    availabilityZone
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    configuration.imageId = 'ami-12345'
```

结果：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.instanceType"
            },
            {
                "Name": "configuration.placement.tenancy"
            },
            {
                "Name": "configuration.imageId"
            },
```

```
            {
                "Name": "availabilityZone"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t1.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2a\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}",
        "{\"resourceId\":\"resourceid\",\"configuration\":{\"imageId\":
\"ami-12345\",\"instanceType\":\"t2.micro\",\"placement\":{\"tenancy\":\"default
\"}},\"availabilityZone\":\"us-west-2c\",\resourceType\":\"AWS::EC2::Instance\"}"
    ]
}
```

Query for count of resources grouped by their AWS Config rules compliance status

查询：

```
SELECT
    configuration.complianceType,
    COUNT(*)
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
GROUP BY
    configuration.complianceType
```

结果：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "configuration.complianceType"
            },
            {
                "Name": "COUNT(*)"
            }
        ]
    },
    "Results": [
        "{\"COUNT(*)\":163,\"configuration\":{\"complianceType\":\"NON_COMPLIANT
\"}}",
        "{\"COUNT(*)\":2,\"configuration\":{\"complianceType\":\"COMPLIANT\"}}"
    ]
}
```

Query for the compliance status of AWS Conformance packs

查询：

```
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.complianceType
WHERE
    resourceType = 'AWS::Config::ConformancePackCompliance'
```

结果：

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "resourceName"
            },
            {
                "Name": "resourceType"
```

```
            },
            {
                "Name": "configuration.complianceType"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"COMPLIANT\"},\"resourceName\":\"MyConformancePack1\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack2\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}",
        "{\"resourceId\":\"conformance-pack-conformance-pack-ID\",\"configuration
\":{\"complianceType\":\"NON_COMPLIANT\"},\"resourceName\":\"MyConformancePack3\",
\"resourceType\":\"AWS::Config::ConformancePackCompliance\"}"
    ]
}
```

Query to get counts of AWS resources grouped by account ID

查询：

```
aws configservice select-aggregate-resource-config --expression "SELECT COUNT(*),
 accountId group by accountId" --configuration-aggregator-name my-aggregator
```

结果：

```
{
    "Results": [
        "{\"COUNT(*)\":2407,\"accountId\":\"accountId\"}",
        "{\"COUNT(*)\":726,\"accountId\":\"accountId\"}"
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "COUNT(*)"
            },
            {
                "Name": "accountId"
            }
        ]
    }
```

```
}
```

Query to list all EC2 volumes that are not in use

查询：

```
SELECT
    resourceId,
    accountId,
    awsRegion,
    resourceType,
    configuration.volumeType,
    configuration.size,
    resourceCreationTime,
    tags,
    configuration.encrypted,
    configuration.availabilityZone,
    configuration.state.value
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.state.value = 'available'
```

结果：


```
{
    "Results": [
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0174de9c962f6581c\",
\"awsRegion\":\"us-west-2\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-west-2a\"},\"resourceCreationTime\":\"2020-02-21T07:39:43.771Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0cbeb652a74af2f8f\",
\"awsRegion\":\"us-east-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"us-east-1a\"},\"resourceCreationTime\":\"2020-02-21T07:28:40.639Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}"
        "{\"accountId\":\"accountId\",\"resourceId\":\"vol-0a49952d528ec8ba2\",
\"awsRegion\":\"ap-south-1\",\"configuration\":{\"volumeType\":\"gp2\",\"encrypted
\":false,\"size\":100.0,\"state\":{\"value\":\"available\"},\"availabilityZone\":
\"ap-south-1a\"},\"resourceCreationTime\":\"2020-02-21T07:39:31.800Z\",\"tags\":[],
\"resourceType\":\"AWS::EC2::Volume\"}",
```

```
    ],
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            },
            {
                "Name": "accountId"
            },
            {
                "Name": "awsRegion"
            },
            {
                "Name": "resourceType"
            },
            {
                "Name": "configuration.volumeType"
            },
            {
                "Name": "configuration.size"
            },
            {
                "Name": "resourceCreationTime"
            },
            {
                "Name": "tags"
            },
            {
                "Name": "configuration.encrypted"
            },
            {
                "Name": "configuration.availabilityZone"
            },
            {
                "Name": "configuration.state.value"
            }
        ]
    }
}
```

关系查询示例

Find EIPs related to an EC2 instance

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'i-abcd1234'
```

Find EIPs related to an EC2 network interface

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::EIP'
    AND relationships.resourceId = 'eni-abcd1234'
```

Find EC2 instances and network interfaces related to a security group

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkInterface')
    AND relationships.resourceId = 'sg-abcd1234'
```

或

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND relationships.resourceId = 'sg-abcd1234'

SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::NetworkInterface'
    AND relationships.resourceId = 'sg-abcd1234'
```

Find EC2 instances, network ACLs, network interfaces and route tables related to a subnet

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::NetworkACL',
 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable')
    AND relationships.resourceId = 'subnet-abcd1234'
```

Find EC2 instances, internet gateways, network ACLs, network interfaces, route tables, subnets and security groups related to a VPC

```
SELECT
    resourceId
WHERE
    resourceType IN ('AWS::EC2::Instance', 'AWS::EC2::InternetGateway',
 'AWS::EC2::NetworkACL', 'AWS::EC2::NetworkInterface', 'AWS::EC2::RouteTable',
 'AWS::EC2::Subnet', 'AWS::EC2::SecurityGroup')
    AND relationships.resourceId = 'vpc-abcd1234'
```

Find EC2 route tables related to a VPN gateway

```
SELECT
    resourceId
WHERE
    resourceType = 'AWS::EC2::RouteTable'
    AND relationships.resourceId = 'vgw-abcd1234'
```

限制

> **Note**
>
> 高级查询不支持查询尚未配置为由配置记录器记录的资源。 AWS Config 当发现资源但未配置为由配置记录器记录`configurationItemStatus`时，将在`ResourceNotRecorded`中创建配置项目 (CI)。虽然聚合器会聚合这些 CI，但高级查询不支持查询具有 `ResourceNotRecorded` 的 CI。更新您的记录器设置以启用记录要查询的资源类型。

作为 SQL `SELECT` 的一个子集，查询语法有以下限制：

- 查询中不支持 ALL、AS、DISTINCT、FROM、HAVING、JOIN 和 UNION 关键字。不支持 NULL 值查询。
- 不支持查询第三方资源。使用高级查询检索的第三方资源的配置字段将设置为 NULL。
- 不支持使用 SQL 查询解包嵌套结构（例如标签）。
- CIDR 表示法将转换为 IP 范围以供搜索。这意味着，"=" 和 "BETWEEN" 会搜索任何包含所提供的 IP 的范围，而不是精确的范围。要搜索精确的 IP 范围，您需要添加其他条件以排除该范围之外的 IP。例如，要搜索 10.0.0.0/24 且仅搜索该 IP 块，可执行以下操作：

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges BETWEEN '10.0.0.0'
  AND '10.0.0.255'
  AND NOT configuration.ipPermissions.ipRanges < '10.0.0.0'
  AND NOT configuration.ipPermissions.ipRanges > '10.0.0.255'
```

对于 192.168.0.2/32，可以用类似的方式进行搜索：

```
SELECT * WHERE resourceType = 'AWS::EC2::SecurityGroup'
  AND configuration.ipPermissions.ipRanges = '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges > '192.168.0.2'
  AND NOT configuration.ipPermissions.ipRanges < '192.168.0.2'
```

- 当针对对象数组内的多个属性执行查询时，将针对所有数组元素计算匹配项。例如，对于具有规则 A 和 B 的资源 R，该资源符合规则 A 但不符合规则 B。资源 R 存储为：

```
{
    configRuleList: [
        {
            configRuleName: 'A', complianceType: 'compliant'
        },
        {
            configRuleName: 'B', complianceType: 'non_compliant'
        }
    ]
}
```

此查询将返回 R：

```
SELECT configuration WHERE configuration.configRuleList.complianceType =
 'non_compliant'
AND configuration.configRuleList.configRuleName = 'A'
```

第一个条件适用`configuration.configRuleList.complianceType = 'non_compliant'`于 r.config 中的所有元素RuleList，因为 R 有一条 complianceType = 'non_complitive' 的规则（规则 B），因此该条件被评估为真。第二个条件适用`configuration.configRuleList.configRuleName`于 r.config 中的所有元素RuleList，因为 R 的规则（规则 A）为 configRuleName = 'A'，因此该条件被评估为真。由于两个条件均为 True，因此将返回 R。

- 针对所有列的 `SELECT` 简写形式（也就是 `SELECT *`）将仅选择 CI 的顶级标量属性。返回的标量属性为 `accountId`、`awsRegion`、`arn`、`availabilityZone`、`configurationItemCaptureTime`、`resou` 和 `version`。
- 通配符限制：
  - 通配符仅支持属性值，但不支持属性键（例如支持 `...WHERE someKey LIKE 'someValue%'`，但不支持 `...WHERE 'someKey%' LIKE 'someValue%'`）。
  - 仅支持后缀通配符（例如，支持 `...LIKE 'AWS::EC2::%'` 和 `...LIKE 'AWS::EC2::_'`，但不支持 `...LIKE '%::EC2::Instance'` 和 `...LIKE '_::EC2::Instance'`）。
  - 通配符匹配项的长度必须至少为 3 个字符（例如，不允许 `...LIKE 'ab%'` 和 `...LIKE 'ab_'`，但允许 `...LIKE 'abc%'` 和 `...LIKE 'abc_'`）。

> **Note**
>
> “_”（单下划线）也被视为通配符。

- 聚合限制：
  - 聚合函数仅可接受一个参数或属性。
  - 聚合函数无法采用其他函数作为参数。
  - 带有引用聚合函数的 `ORDER BY` 子句的 `GROUP BY` 只能包含一个属性。
  - 对于所有其他聚合，`GROUP BY` 子句最多可以包含三个属性。
  - 除 `ORDER BY` 子句具有聚合函数外，所有聚合查询都支持分页。例如，如果 Y 是聚合函数，则 `GROUP BY X, ORDER BY Y` 不起作用。
  - 不支持聚合中的 `HAVING` 子句。

- 不匹配的标识符限制：

  不匹配的标识符是拼写相同但大小写不同（大写和小写）的属性。高级查询不支持处理包含不匹配标识符的查询。例如：

  - 两个拼写完全相同但大小写不同的属性（`configuration.dbclusterIdentifier` 和 `configuration.dBClusterIdentifier`）。
  - 两个属性，其中一个属性是另一个属性的子集，并且它们的大小写不同（`configuration.ipAddress` 和 `configuration.ipaddressPermissions`）。

区域支持

以下区域支持高级查询：

区域名称	区域	端点	协议
美国东部（俄亥俄州）	us-east-2	config.us-east-2.amazonaws.com	HTTPS
美国东部（弗吉尼亚州北部）	us-east-1	config.us-east-1.amazonaws.com	HTTPS
美国西部（北加利福尼亚）	us-west-1	config.us-west-1.amazonaws.com	HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS
非洲（开普敦）	af-south-1	config.af-south-1.amazonaws.com	HTTPS
亚太地区（香港）	ap-east-1	config.ap-east-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
亚太地区（海得拉巴）	ap-south-2	config.ap-south-2.amazonaws.com	HTTPS
亚太地区（雅加达）	ap-southeast-3	config.ap-southeast-3.amazonaws.com	HTTPS
亚太地区（墨尔本）	ap-southeast-4	config.ap-southeast-4.amazonaws.com	HTTPS
亚太地区（孟买）	ap-south-1	config.ap-south-1.amazonaws.com	HTTPS
亚太地区（大阪）	ap-northeast-3	config.ap-northeast-3.amazonaws.com	HTTPS
亚太地区（首尔）	ap-northeast-2	config.ap-northeast-2.amazonaws.com	HTTPS
亚太地区（新加坡）	ap-southeast-1	config.ap-southeast-1.amazonaws.com	HTTPS
亚太地区（悉尼）	ap-southeast-2	config.ap-southeast-2.amazonaws.com	HTTPS
亚太地区（东京)	ap-northeast-1	config.ap-northeast-1.amazonaws.com	HTTPS
加拿大（中部）	ca-central-1	config.ca-central-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
加拿大西部（卡尔加里）	ca-west-1	config.ca-west-1.amazonaws.com	HTTPS
欧洲地区（法兰克福）	eu-central-1	config.eu-central-1.amazonaws.com	HTTPS
欧洲地区（爱尔兰）	eu-west-1	config.eu-west-1.amazonaws.com	HTTPS
欧洲地区（伦敦）	eu-west-2	config.eu-west-2.amazonaws.com	HTTPS
欧洲地区（米兰）	eu-south-1	config.eu-south-1.amazonaws.com	HTTPS
欧洲地区（巴黎）	eu-west-3	config.eu-west-3.amazonaws.com	HTTPS
欧洲（西班牙）	eu-south-2	config.eu-south-2.amazonaws.com	HTTPS
欧洲地区（斯德哥尔摩）	eu-north-1	config.eu-north-1.amazonaws.com	HTTPS
欧洲（苏黎世）	eu-central-2	config.eu-central-2.amazonaws.com	HTTPS
以色列（特拉维夫）	il-central-1	config.il-central-1.amazonaws.com	HTTPS
中东（巴林）	me-south-1	config.me-south-1.amazonaws.com	HTTPS

区域名称	区域	端点	协议
中东（阿联酋）	me-central-1	config.me-central-1.amazonaws.com	HTTPS
南美洲（圣保罗）	sa-east-1	config.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国东部）	us-gov-east-1	config.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud（美国西部）	us-gov-west-1	config.us-gov-west-1.amazonaws.com	HTTPS

查询使用 SQL 查询编辑器进行查询（控制台）

为高级查询引入了预览功能，允许您使用生成式人工智能（生成人工智能）功能以通俗易懂的英语输入提示并将其转换为 ready-to-use 查询格式。有关更多信息，请参阅适用于高级查询的自然语言查询处理器。

您可以使用 AWS 示例查询，也可以创建自己的名为自定义查询的查询。

注意事项

先决条件

如果您使用的是以下 AWS 托管策略之一，则您将拥有运行和保存查询所需的权限：AWSServiceRoleForConfig（服务相关角色）或 AW ConfigRole S_。

否则，您必须拥有AWSConfigUserAccess AWS 托管策略中包含的权限。

您可以查询的属性列表

中提供了更新的属性及其数据类型列表GitHub。

高级查询和聚合器

要在聚合器上运行查询，请创建聚合器。有关更多信息，请参阅 使用控制台设置聚合器。

如果您已经设置了聚合器，则在查询范围中，选择聚合器以在该聚合器上运行高级查询。选择聚合器时，请考虑在查询语句中添加 AWS 账户 ID 和 AWS 区域，以便在结果中查看该信息。

使用 AWS 示例查询

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 从左侧导航中选择 Advanced queries (高级查询)，以查询针对单个账户和区域或针对多个账户和区域的资源配置。
3. 在高级查询页面上，从查询列表中选择适当的查询。您可以按名称、描述、创建者或标签在查询列表中筛选。要筛选 AWS 查询，请选择创建者，并输入 AWS。您输入的查询将显示在 SQL 查询编辑器中。您可以根据需要编辑所选查询。
4. 要将此查询保存到新查询，请选择另存为。
   - 在查询名称字段中，更新查询的名称。
   - 在描述字段中，更新查询的描述。
   - 为此查询输入最多 50 个唯一标签。
   - 选择保存。
5. 选择运行。查询结果将显示在查询编辑器下方的表中。
6. 选择 Export as (导出为)，以 CSV 或 JSON 格式导出查询结果。

> **Note**
>
> 查询结果将进行分页。选择导出时，最多可导出 500 个结果。
> 您还可以使用 API 检索所有结果。结果会进行分页，您可以一次检索 100 个结果。

创建您的自定义查询

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。

2. 从左侧导航中选择 Advanced queries (高级查询)，以查询针对单个账户和区域或针对多个账户和区域的资源配置。
3. 要创建您的自定义查询，请选择新建查询。

   要查看或编辑自定义查询，可以按名称、描述、创建者或标签筛选查询。要筛选自定义查询，请选择创建者并输入自定义。
4. 在查询编辑器页面上，为此账户和区域创建您自己的查询。您还可以选择合适的聚合器来创建针对多个账户和区域的查询。
5. 如果您希望对此查询进行更改，请进行编辑。选择保存查询以保存此查询。
   - 在查询名称字段中，更新查询的名称。
   - 在描述字段中，更新查询的描述。
   - 为此查询输入最多 50 个唯一标签。
   - 选择保存。
6. 选择运行。查询结果将显示在查询编辑器下方的表中。
7. 选择 Export as (导出为)，以 CSV 或 JSON 格式导出查询结果。

   查询结果将进行分页。选择导出时，最多可导出 500 个结果。

   您还可以使用 API 检索所有结果。结果会进行分页，您可以一次检索 100 个结果。

使用 SQL 查询编辑器 (AWS CLI) 进行查询

AWS CLI 是用于管理您的 AWS 服务的统一工具。只需下载和配置一个工具，您就可以从命令行控制多项 AWS 服务，并使用脚本自动执行这些服务。有关 AWS CLI 和 AWS CLI 工具安装说明的更多信息，请参阅《AWS Command Line Interface 用户指南》中的以下内容。

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

如有必要，`aws configure`请输入配置 AWS CLI 为使用提供高级查询的 AWS 区域。

注意事项

先决条件

如果您使用的是以下 AWS 托管策略之一，则您将拥有运行和保存查询所需的权限：AWSServiceRoleForConfig（服务相关角色）或 AW ConfigRole S_。

否则，您必须拥有AWSConfigUserAccess AWS 托管策略中包含的权限。

您可以查询的属性列表

中提供了更新的属性及其数据类型列表GitHub。

高级查询和聚合器

要在聚合器上运行查询，请创建聚合器。有关更多信息，请参阅 使用控制台设置聚合器。

如果您已经设置了聚合器，则在查询范围中，选择聚合器以在该聚合器上运行高级查询。选择聚合器时，请考虑在查询语句中添加 AWS 账户 ID 和 AWS 区域，以便在结果中查看该信息。

查询资源配置数据

使用查询编辑器 (AWS CLI) 查询针对单个账户和区域的资源配置数据

1. 打开命令提示符或终端窗口。
2. 输入以下命令以查询您的资源配置数据。

```
aws configservice select-resource-config --expression "SELECT resourceId WHERE
 resourceType='AWS::EC2::Instance'"
```

根据您的查询，输出将如下所示。

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
```

```
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

使用查询编辑器 (AWS CLI) 查询针对多个账户和区域的资源配置数据

1. 打开命令提示符或终端窗口。
2. 输入以下命令以查询您的资源配置数据。

```
aws configservice select-aggregate-resource-config --expression "SELECT resourceId
 WHERE resourceType='AWS::EC2::Instance'" --configuration-aggregator-name my-
aggregator
```

根据您的查询，输出将如下所示。

```
{
    "QueryInfo": {
        "SelectFields": [
            {
                "Name": "resourceId"
            }
        ]
    },
    "Results": [
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}",
        "{\"resourceId\":\"ResourceId\"}"
    ]
}
```

> **Note**
>
> 在高级查询中使用`AWS::IAM::User``AWS::IAM::Group`、`AWS::IAM::Role`、和`AWS::IAM::Policy`资源类型时，使用`awsRegion = 'global'`。

保存查询

1. 打开命令提示符或终端窗口。
2. 输入以下命令以保存查询。

```
aws configservice put-stored-query --stored-query "{\"QueryName\": \"cli-test\",
 \"Expression\": \"SELECT *\", \"Description\": \"cli test query\" }"
        --tags "[{ \"Key\": \"first-tag\", \"Value\": \"\" }, { \"Key\": \"second-
tag\", \"Value\": \"non-empty-tag-value\" }]"
```

3. 根据您的查询，输出将如下所示。

```
{
    "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab"
}
```

> **Note**
>
> `--tags` 为可选项。传递标签时，`list-stored-queries` 或 `get-stored-query` 都不会返回保存的标签。必须使用 `list-tag-for-resources` 检索已保存查询的相关标签。
>
> 在创建或更新查询时，`--description` 是可选的。

查看所有已保存的查询

1. 输入以下命令以查看所有已保存查询的列表。

```
aws configservice list-stored-queries
```

2. 根据您的查询，输出将如下所示。

```
{
    "StoredQueryMetadata": [
        {
            "QueryId": "query-e65mijt4rmam5pab",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test/query-e65mijt4rmam5pab",
```

```
            "QueryName": "cli-test"
        },
        {
            "QueryId": "query-rltwlewlqfivadxq",
            "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-
test-2/query-rltwlewlqfivadxq",
            "QueryName": "cli-test-2",
            "Description": "cli test query"
        }
    ]
}
}
```

获取已保存的查询的详细信息

1. 输入以下命令以获取已保存的特定查询的详细信息。

```
aws configservice get-stored-query --query-name cli-test
```

2. 根据您的查询，输出将如下所示。

```
{
    "StoredQuery": {
        "QueryId": "query-e65mijt4rmam5pab",
        "QueryArn": "arn:aws:config:eu-central-1:Account ID:stored-query/cli-test/
query-e65mijt4rmam5pab",
        "QueryName": "cli-test",
        "Description": "cli test query",
        "Expression": "SELECT *"
    }
}
```

删除已保存的查询

- 输入以下命令以删除您保存的查询。

```
aws configservice delete-stored-query --query-name cli-test
```

如果成功，则命令会运行，而没有附加输出。

适用于高级查询的自然语言查询处理器

用于高级查询的自然语言查询处理器处于预览版 AWS Config ，可能会发生变化。

用于高级查询的自然语言查询处理器使用 Amazon Bedrock，这是一种生成式人工智能（生成式 AI）技术，它允许您以通俗易懂的英语输入提示并将其转换为 ready-to-use 查询格式。使用自然语言查询处理器，您可以对您的组织 AWS 账户 或整个 AWS 组织进行查询。

提示可以是问题或陈述。例如，您可以输入诸如 “哪些负载均衡器是在 2024 年 1 月 1 日之后创建的？” 之类的提示 和 “列出我所有运行节点 js 16 的 lambda 函数。”

注意事项

自然语言查询处理器无法执行以下操作：

- 使用英语以外的语言生成查询。
- 根据与高级查询无关的提示生成查询。
- 根据超过 1000 个字符的提示生成查询。
- 根据后续更正或以前的会话生成查询。
- 解释已生成的代码。

使用自然语言查询处理器进行查询

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 从左侧导航中选择 Advanced queries (高级查询)，以查询针对单个账户和区域或针对多个账户和区域的资源配置。
3. 在高级查询页面上，选择新建查询，进入 查询编辑器。
   - （可选）要在聚合器上运行查询，请创建聚合器。有关更多信息，请参阅 使用控制台设置聚合器。
   - 如果您已经设置了聚合器，则在查询范围中，选择聚合器以在该聚合器上运行高级查询。选择聚合器时，请考虑在查询语句中添加 AWS 账户 ID 和 AWS 区域，以便在结果中查看该信息。

4. 在查询编辑器中，转到自然语言查询处理器部分。用通俗易懂的英语输入提示，然后选择 “生成”。有关示例，请参阅示例提示。
5. 您生成查询后，可以选择复制（功能上等同于 Ctrl+C）将查询复制到剪贴板，也可以选择填充到编辑器。如果已填充到编辑器中，您可以根据需要编辑生成的查询。
6. 要将此查询保存到新查询，请选择另存为。
   - 在查询名称字段中，更新查询的名称。
   - 在描述字段中，更新查询的描述。
   - 为此查询输入最多 50 个唯一标签。
   - 选择保存。
7. 选择运行。查询结果会显示在查询编辑器下方的表中。
8. 选择 Export as (导出为)，以 CSV 或 JSON 格式导出查询结果。

> **Note**
>
> 查询结果将进行分页。导出时，最多可导出 500 个结果。
> 您还可以使用 API 检索所有结果。结果会进行分页，您可以一次检索 100 个结果。

提示示例

以下是提示和生成查询，您可以将其用作示例。

Example: 2024 年 1 月 1 日之后创建了哪些负载均衡器？

提示：What load balancers were created after January 1, 2024?

生成的查询：

```
SELECT
    resourceId,
    resourceType,
    resourceCreationTime
WHERE
    resourceType IN ('AWS::ElasticLoadBalancing::LoadBalancer',
 'AWS::ElasticLoadBalancingV2::LoadBalancer')
AND
    resourceCreationTime > '2024-01-01T00:00:00.0Z'
ORDER BY
```

```
    resourceCreationTime
DESC
```

Example: 我的哪个 RDS 数据库实例可以公开访问？

提示：Which of my RDS database instances are publicly accessible?

生成的查询：

```
SELECT
    resourceId,
    resourceType,
    configuration.publiclyAccessible
WHERE
    resourceType = 'AWS::RDS::DBInstance'
AND
    configuration.publiclyAccessible = true
```

Example: 在过去一年中创建了多少 EC2 实例？

提示：How many EC2 instances were created in last one year?

生成的查询：

```
SELECT
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
AND
    resourceCreationTime
BETWEEN
    '2023-05-10T16:56:25.000Z'
AND
    '2024-05-10T16:56:25.000Z'
```

Example: 我的每个实例中有多少 EC2 实例 AWS 账户？

提示：How many EC2 instances do I have in each of my AWS 账户?

生成的查询：

```
SELECT
    accountId,
```

```
    COUNT(*)
WHERE
    resourceType = 'AWS::EC2::Instance'
GROUP BY
    accountId'
```

Example: 托管策略 AdministratorAccess 附加了哪些 IAM 角色？

提示：Which IAM roles have the managed policy AdministratorAccess attached?

生成的查询：

```
SELECT
    resourceId,
    resourceName,
    resourceType
WHERE
    resourceType = 'AWS::IAM::Role'
AND
    configuration.attachedManagedPolicies.policyName = 'AdministratorAccess'
```

Example: 未加密的 EBS 卷

提示：EBS volumes without encryption

生成的查询：

```
SELECT
    accountId
WHERE
    resourceType = 'AWS::EC2::Volume'
AND
    configuration.encrypted = false
```

Example: 获取不合规的资源

提示：Get noncompliant resources

生成的查询：

```
SELECT
    resourceId,
    resourceType
```

```
WHERE
    resourceType = 'AWS::Config::ResourceCompliance'
AND
    configuration.complianceType = 'NON_COMPLIANT'
```

Example: 列出我所有正在运行节点 js 16 的 lambda 函数

提示：List all my lambda function that is running node js 16

生成的查询：

```
SELECT
    accountId,
    resourceName
WHERE
    resourceType = 'AWS::Lambda::Function'
AND
    configuration.runtime = 'nodejs16.x'
```

Example: 哪些 ACM 证书将在接下来的 30 天内过期？

提示：What ACM certificates expire the next 30 days?

生成的查询：

```
SELECT
    resourceId,
    configuration.domainName,
    configuration.notAfter
WHERE
    resourceType = 'AWS::ACM::Certificate'
AND
    configuration.notAfter
BETWEEN
    '2024-05-10 16:59:53'
AND
    '2024-06-10 16:59:53’
```

> **Note**
>
> 生成的查询中的时间取决于您输入提示的时间。

提供反馈

您可以提供有关自然语言查询处理器的总体反馈或有关生成的特定查询的反馈。

提供有关自然语言查询处理器的反馈

选择右侧自然语言查询处理器上方显示的 “提供反馈” 按钮。您可以输入您的满意度或不满意度，并提供有关 AWS Config 如何使自然语言查询更有用的反馈。

> **Note**
>
> 请勿透露任何个人、商业敏感或机密信息。

就生成的特定查询提供反馈

您可以通过选择生成的查询下方显示的 “竖起大拇指” 或 “竖起大拇指” 按钮，对生成的查询提供反馈。

区域支持

自然语言查询处理器在以下区域受支持。

区域名称	区域	端点	协议
美国东部 (弗吉尼亚北部)	us-east-1	config.us-east-1.amazonaws.com	HTTPS
美国西部（俄勒冈州）	us-west-2	config.us-west-2.amazonaws.com	HTTPS

删除 AWS Config 数据

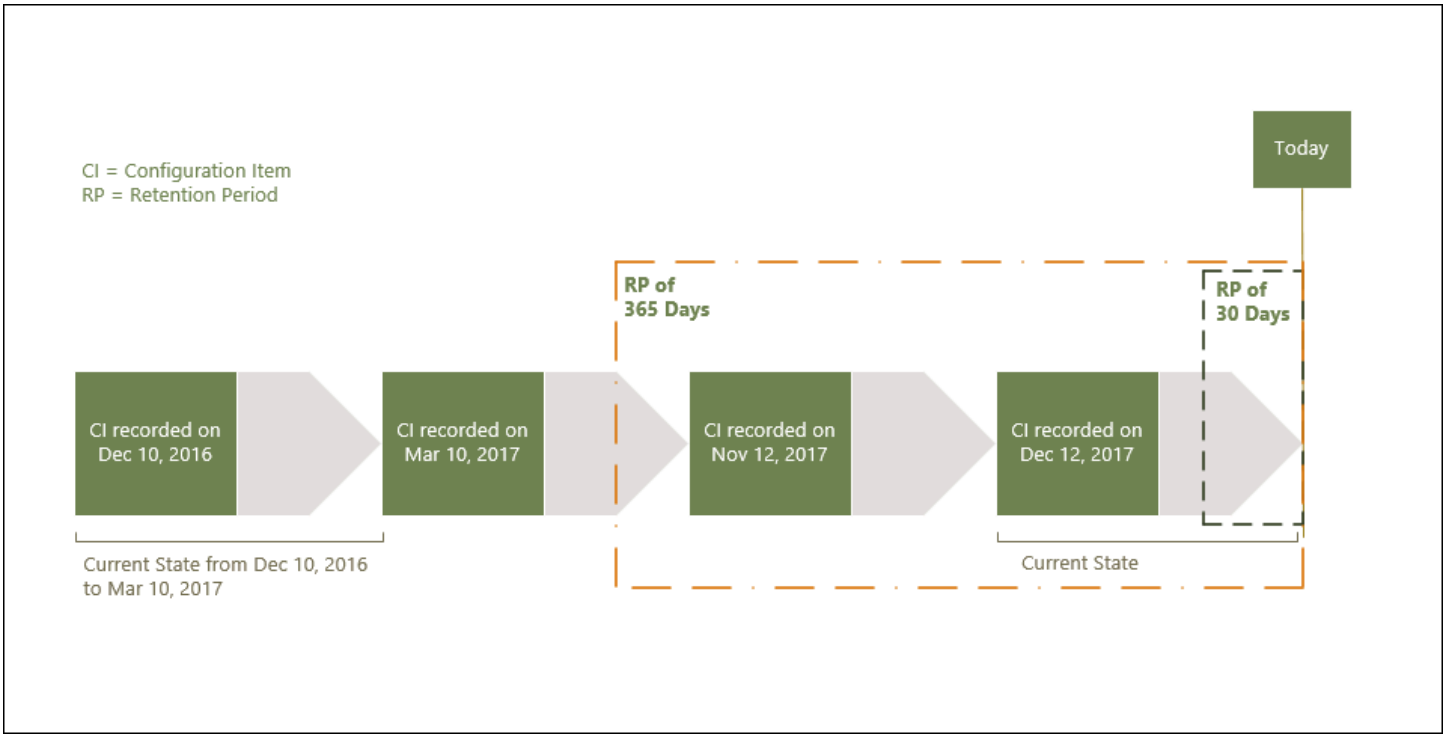
> **Note**
>
> 虽然 AWS Config 使用亚马逊简单存储服务 (Amazon S3) 和亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 发送配置快照和配置历史记录 AWS Config 文件，但有自己的数据存储和保留策略。此页面上的信息是专门针对的 AWS Config。Amazon S3 和 Amazon SNS 有各自独立的数据存储和保留策略。

AWS Config 允许您通过为自己的数据指定保留期来删除数据`ConfigurationItems`。当您指定保留期时，将在该指定期限内 AWS Config 保留您的`ConfigurationItems`保留期。您可以选择最少 30 天到最长 7 年（2557 天）之间的时间段。 AWS Config 删除早于您指定保留期的数据。如果您未指定保留期， AWS Config 将继续在默认保留期 7 年（2557 天）内存储 `ConfigurationItems`。当记录功能打开时，资源的当前状态是 `ConfigurationItem` 被记录，直到记录下一个更改（新的 `ConfigurationItem`）。

为了理解保留期的行为，我们来看一下时间表。

- 当记录功能打开时，资源的当前状态始终存在，无法删除，无论记录 `ConfigurationItem` 的日期如何都是如此。
- 当 AWS Config 记录为新记录时`ConfigurationItems`，将根据指定的保留期限删除之前`ConfigurationItems`的记录。

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



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

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

指定保留期后，不会再返回`ConfigurationItems`表示早于指定保留期的状态的 AWS Config API。

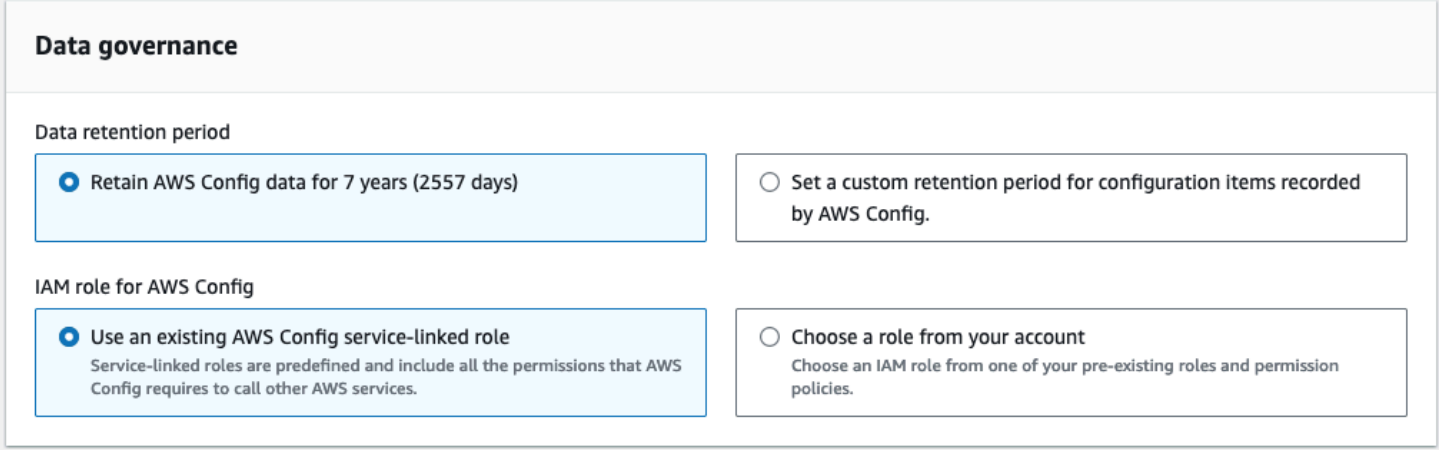
> **Note**
>
> - AWS Config `ConfigurationItems`如果关闭录音，则无法录制您的录音。
> - AWS Config `ConfigurationItems`如果您的 IAM 角色权限不足，则无法记录您的权限。有关更多信息，请参阅分配给的 IAM 角色的权限 AWS Config。

在中设置数据保留期 AWS Management Console

在中 AWS Management Console，如果您未选择数据保留期，则默认期限为 7 年或 2557 天。

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

下图显示了您可以在 “数据治理” 中设置数据保留期限的位置。您可以从 AWS Config 控制台的 “编辑设置” 页面访问数据治理，方法是选择左侧导航栏中的 “设置”，然后选择 “编辑”。



安全性 AWS Config

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

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

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

本文档可帮助您了解在使用时如何应用分担责任模型 AWS Config。以下主题向您介绍如何进行配置 AWS Config 以满足您的安全和合规性目标。

主题

- 中的数据保护 AWS Config
- 适用于 Identity and Access Managem AWS Config
- 中的事件响应 AWS Config
- 合规性验证 AWS Config
- 韧性在 AWS Config
- 中的基础设施安全 AWS Config
- 防止跨服务混淆座席
- 的安全最佳实践 AWS Config

中的数据保护 AWS Config

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

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

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

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

静态数据加密

使用透明的服务器端加密，加密静态数据。这样可以帮助减少在保护敏感数据时涉及的操作负担和复杂性。通过静态加密，您可以构建符合加密合规性和法规要求的安全敏感型应用程序。

传输中的数据的加密

收集和访问的数据只能通过 AWS Config 受传输层安全 (TLS) 保护的通道进行。

适用于 Identity and Access Managem AWS Config

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

主题

- 受众

- 使用身份进行身份验证
- 使用策略管理访问
- 如何 AWS Config 与 IAM 配合使用
- 基于身份的策略示例 AWS Config
- AWS 的托管策略 AWS Config
- 分配给的 IAM 角色的权限 AWS Config
- 更新分配给的 IAM 角色 AWS Config
- AWS Config 传送渠道的 Amazon S3 存储桶的权限
- AWS Config 交付渠道 KMS 密钥的权限
- Amazon SNS 主题的权限
- 对 AWS Config 身份和访问进行故障排除
- 将服务相关角色用于 AWS Config

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您所做的工作 AWS Config。

服务用户-如果您使用 AWS Config 服务完成工作，则管理员会为您提供所需的凭证和权限。当你使用更多 AWS Config 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 AWS Config中的特征，请参阅 对 AWS Config 身份和访问进行故障排除。

服务管理员-如果您负责公司的 AWS Config 资源，则可能拥有完全访问权限 AWS Config。您的工作是确定您的服务用户应访问哪些 AWS Config 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解您的公司如何使用 IAM AWS Config，请参阅如何 AWS Config 与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 AWS Config的访问权限的详细信息。要查看您可以在 IAM 中使用的 AWS Config 基于身份的策略示例，请参阅。基于身份的策略示例 AWS Config

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的 多重身份验证和《IAM 用户指南》中的 在 AWS中使用多重身份验证（MFA）。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的 权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅 IA M 用户指南中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service (Amazon S3) 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。

- 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
- 服务相关角色-服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

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

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM policy，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

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

基于身份的策略可以进一步归类为内联策略或托管策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南中的在托管式策略与内联策略之间进行选择。

基于资源的策略

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

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

访问控制列表 (ACL)

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

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问控制列表（ACL）概览。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。

- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

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

如何 AWS Config 与 IAM 配合使用

在使用 IAM 管理访问权限之前 AWS Config，请先了解有哪些 IAM 功能可供使用 AWS Config。

您可以搭配使用的 IAM 功能 AWS Config

IAM 功能	AWS Config 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACL	否
ABAC（策略中的标签）	是
临时凭证	是

IAM 功能	AWS Config 支持
转发访问会话（FAS）	是
服务角色	是
服务相关角色	是

要全面了解 AWS Config 以及其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

基于身份的策略 AWS Config

支持基于身份的策略	是

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

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

基于身份的策略示例 AWS Config

要查看 AWS Config 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS Config

内部基于资源的政策 AWS Config

支持基于资源的策略	否

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

要启用跨账户存取，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅 IAM 用户指南中的跨账户访问 IAM 中的资源。

的政策行动 AWS Config

支持策略操作	是

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

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 AWS Config 操作列表，请参阅《服务授权参考》 AWS Config中定义的操作。

正在执行的策略操作在操作前 AWS Config 使用以下前缀：

```
config
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，包括以下操作：

```
"Action": "config:Describe*"
```

要查看 AWS Config 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS Config

的政策资源 AWS Config

支持策略资源	是

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

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 AWS Config 资源类型及其 ARN 的列表，请参阅《服务授权参考》 AWS Config中定义的资源。要了解可以在哪些操作中指定每个资源的 ARN，请参阅 AWS Config定义的操作。

要查看 AWS Config 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS Config

的策略条件密钥 AWS Config

支持特定于服务的策略条件键	是

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

在 `Condition` 元素（或 `Condition` 块）中，可以指定语句生效的条件。`Condition` 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 `Condition` 元素，或在单个 `Condition` 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM policy 元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 AWS Config 条件密钥列表，请参阅《服务授权参考》 AWS Config中的条件密钥。要了解可以使用条件键的操作和资源，请参阅由定义的操作 AWS Config。

要查看 AWS Config 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS Config

输入的 ACL AWS Config

支持 ACL	否

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

ABAC with AWS Config

支持 ABAC（策略中的标签）	是

基于属性的访问控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

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

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

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

有关标记 AWS Config 资源的更多信息，请参阅标记您的 AWS Config 资源。

将临时证书与 AWS Config

支持临时凭证	是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

转发访问会话 AWS Config

支持转发访问会话 (FAS)	是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详细信息，请参阅转发访问会话。

AWS Config的服务角色

支持服务角色	是

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

> **Warning**
> 更改服务角色的权限可能会中断 AWS Config 功能。只有在 AWS Config 提供操作指导时才编辑服务角色。

的服务相关角色 AWS Config

支持服务相关角色	是

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

有关创建或管理 AWS Config 服务相关角色的详细信息，请参阅将服务相关角色用于 AWS Config。

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

基于身份的策略示例 AWS Config

默认情况下，用户和角色没有创建或修改 AWS Config 资源的权限。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM 策略。

有关由定义的操作和资源类型的详细信息 AWS Config，包括每种资源类型的 ARN 格式，请参阅《服务授权参考》 AWS Config中的操作、资源和条件密钥。

主题

- 策略最佳实践
- 注册获取 AWS 账户
- 创建具有管理访问权限的用户
- 使用 AWS Config 控制台

- 允许用户查看他们自己的权限
- 只读访问权限 AWS Config
- 完全访问权限 AWS Config
- AWS Config 规则 API 操作支持的资源级权限
- 支持多账户多区域数据聚合的资源级别权限

策略最佳实践

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

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

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

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

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

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

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

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

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

保护你的 AWS 账户根用户

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

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

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

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

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

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

以具有管理访问权限的用户身份登录

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

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

将访问权限分配给其他用户

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

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

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加组。

使用 AWS Config 控制台

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

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

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

您必须向用户授予与之交互的权限 AWS Config。对于需要完全访问托管权限的用户 AWS Config，请使用对 AWS Config托管的完全访问权限策略。

要提供访问权限，请为您的用户、组或角色添加权限：

- 中的用户和群组 AWS IAM Identity Center：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中创建权限集的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

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

- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

允许用户查看他们自己的权限

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

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

```
            "Resource": "*"
        }
    ]
}
```

只读访问权限 AWS Config

以下示例显示了一个 AWS 托管策略，`AWSConfigUserAccess`该策略授予对的只读访问权限 AWS Config。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "config:Get*",
        "config:Describe*",
        "config:Deliver*",
        "config:List*",
        "config:Select*",
        "tag:GetResources",
        "tag:GetTagKeys",
        "cloudtrail:DescribeTrails",
        "cloudtrail:GetTrailStatus",
        "cloudtrail:LookupEvents"
      ],
      "Resource": "*"
    }
  ]
}
```

在这些策略语句中，`Effect` 元素指定是允许还是拒绝操作。`Action` 元素列出了允许用户执行的特定操作。`Resource` 元素列出允许用户对其执行这些操作的 AWS 资源。对于控制 AWS Config 操作访问权限的策略，`Resource`元素始终设置为`*`，通配符表示 “所有资源”。

`Action` 元素中的值对应于服务支持的 API。操作前附加了 `config:` 以表示其指的是 AWS Config 操作。您可以在 `*` 元素中使用 `Action` 通配符，如以下示例所示：

- `"Action": ["config:*ConfigurationRecorder"]`

这允许所有以 “ConfigurationRecorder” (`StartConfigurationRecorder` , `StopConfigurationRecorder`) 结尾的 AWS Config 操作。

- `"Action": ["config:*"]`

  这允许所有 AWS Config 操作，但不允许对其他 AWS 服务执行操作。

- `"Action": ["*"]`

  这允许所有 AWS 操作。此权限适用于担任您账户 AWS 管理员的用户。

只读策略不对用户授予执行 `StartConfigurationRecorder`、`StopConfigurationRecorder` 和 `DeleteConfigurationRecorder` 操作的权限。不允许使用此策略的用户启动配置记录器、停止配置记录器或删除配置记录器。有关 AWS Config 操作列表，请参阅 AWS Config API 参考。

完全访问权限 AWS Config

以下示例显示了授予对的完全访问权限的策略 AWS Config。它授予用户执行所有 AWS Config 操作的权限。它还允许用户管理 Amazon S3 存储桶中的文件，以及管理与用户关联的账户中的 Amazon SNS 主题。

> **Important**
>
> 此策略授予广泛的权限。在授予完全访问权限之前，请考虑从最低权限集开始，并根据需要授予其他权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说是更好的做法。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sns:AddPermission",
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:GetTopicAttributes",
                "sns:ListPlatformApplications",
                "sns:ListTopics",
```

```
                "sns:SetTopicAttributes"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketNotification",
                "s3:GetBucketPolicy",
                "s3:GetBucketRequestPayment",
                "s3:GetBucketVersioning",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListBucketVersions",
                "s3:PutBucketPolicy"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreatePolicyVersion",
                "iam:DeletePolicyVersion",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": [
                        "config.amazonaws.com",
                        "ssm.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:LookupEvents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:*",
                "tag:Get*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeDocument",
                "ssm:GetDocument",
                "ssm:DescribeAutomationExecutions",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:StartAutomationExecution"
            ],
            "Resource": "*"
        }

    ]
}
```

AWS Config 规则 API 操作支持的资源级权限

资源级权限是指能够指定允许用户对哪些资源执行操作。 AWS Config 支持某些 AWS Config 规则 API 操作的资源级权限。这意味着，对于某些 AWS Config 规则操作，您可以控制何时允许用户使用这些操作的条件。这些条件可以是必须满足的操作，也可以是允许用户使用的特定资源。

下表描述了当前支持资源级权限的 AWS Config 规则 API 操作。还介绍了每个操作支持的资源及其 ARN。指定 ARN 时，您可以在路径中使用 * 通配符；例如，在无法或不希望指定确切资源 ID 的时候可以这样做。

> **Important**
>
> 如果此表中未列出 AWS Config 规则 API 操作，则该操作不支持资源级权限。如果 AWS Config 规则操作不支持资源级权限，则可以授予用户使用该操作的权限，但必须为策略语句的资源元素指定*。

API 操作	资源
DeleteConfig规则	Config 规则 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DeleteEvaluation结果	Config 规则 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeComplianceByConfig规则	Config 规则 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
DescribeConfigRuleEvaluation状态	Config 规则 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
GetComplianceDetailsByConfigRule	Config 规则 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutConfig规则	Config 规则

API 操作	资源
	arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
StartConfigRulesEvaluation	Config 规则 arn:aws:config:*region:accountID* :config-rule/config-rule-*ID*
PutRemediation配置	修复配置 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediation配置	修复配置 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DeleteRemediation配置	修复配置 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
PutRemediation例外情况	修复配置 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*
DescribeRemediation例外情况	修复配置 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

API 操作	资源
DeleteRemediation例外情况	修复配置 arn:aws:config:*region:accountId* :remediation-configuration/*config rule name/remediation configuration id*

例如，您希望允许特定用户对特定规则进行的读访问，但拒绝特定用户对特定规则进行的写访问。

在第一个策略中，您可以允许 AWS Config 规则读取操作，例如`DescribeConfigRuleEvaluationStatus`对指定规则的读取操作。

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "config:StartConfigRulesEvaluation",
                    "config:DescribeComplianceByConfigRule",
                    "config:DescribeConfigRuleEvaluationStatus",
                    "config:GetComplianceDetailsByConfigRule"
                ],
                "Resource": [
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID",
                    "arn:aws:config:region:accountID:config-rule/config-rule-ID"
                ]
            }
        ]
    }
```

在第二个策略中，您拒绝对特定 AWS Config 规则执行规则写入操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
```

```
            "Action": [
                "config:PutConfigRule",
                "config:DeleteConfigRule",
                "config:DeleteEvaluationResults"
               ],
            "Resource": "arn:aws:config:region:accountID:config-rule/config-rule-ID"
           }
      ]
   }
```

使用资源级权限，您可以允许读取权限和拒绝写入权限，以便对 AWS Config 规则 API 操作执行特定操作。

支持多账户多区域数据聚合的资源级别权限

您可以使用资源级权限控制用户对多账户多区域数据聚合执行特定操作的能力。以下 AWS Config `Aggregator` API 支持资源级权限：

- BatchGetAggregateResourceConfig
- DeleteConfiguration聚合器
- DescribeAggregateComplianceByConfigRules
- DescribeAggregateComplianceByConformancePacks
- DescribeConfigurationAggregatorSources状态
- GetAggregateComplianceDetailsByConfig规则
- GetAggregateConfigRuleComplianceSummary
- GetAggregateConformancePackComplianceSummary
- GetAggregateDiscoveredResource计数
- GetAggregateResourceConfig
- ListAggregateDiscoveredResources
- PutConfiguration聚合器
- SelectAggregateResourceConfig

例如，您可以通过创建两个聚合器 `AccessibleAggregator` 和 `InAccessibleAggregator`，并附加允许访问 `AccessibleAggregator` 但拒绝访问 `InAccessibleAggregator` 的 IAM 策略来限制特定用户对资源数据的访问。

适用于 IAM 的政策 AccessibleAggregator

在此策略中，您允许访问您指定的 AWS Config Amazon 资源名称 (ARN) 支持的聚合器操作。在此示例中， AWS Config ARN 是。`arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigAllow",
            "Effect": "Allow",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-mocpsqhs"
        }
    ]
}
```

适用于 IAM 的政策 InAccessibleAggregator

在此策略中，您拒绝访问您指定的 AR AWS Config N 支持的聚合器操作。在此示例中， AWS Config ARN 是。`arn:aws:config:ap-northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx`

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

```
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

如果开发者组的用户尝试对您指定的 AWS Config ARN 执行任何此类操作，则该用户将收到拒绝访问的异常。

检查用户访问权限

要显示您创建的聚合器，请运行以下 AWS CLI 命令：

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

命令成功完成后，您将能够看到与您的账户关联的所有聚合器的详细信息。在此示例中，这些聚合器是 `AccessibleAggregator` 和 `InAccessibleAggregator`：

```
{
    "ConfigurationAggregators": [
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-mocpsqhs",
            "CreationTime": 1517942461.442,
```

```
            "ConfigurationAggregatorName": "AccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        },
        {
            "ConfigurationAggregatorArn": "arn:aws:config:ap-
northeast-1:AccountID:config-aggregator/config-aggregator-pokxzldx",
            "CreationTime": 1517942461.442,
            "ConfigurationAggregatorName": "InAccessibleAggregator",
            "AccountAggregationSources": [
                {
                    "AllAwsRegions": true,
                    "AccountIds": [
                        "AccountID1",
                        "AccountID2",
                        "AccountID3"
                    ]
                }
            ],
            "LastUpdatedTime": 1517942461.455
        }
    ]
}
```

> **Note**
>
> 对于 `account-aggregation-sources`，输入要为其聚合数据的 AWS 账户 ID 的逗号分隔的列表。用方括号将账户 ID 括起来，并确保对引号进行转义 (例如，`"[{\"AccountIds\": [\"AccountID1\",\"AccountID2\",\"AccountID3\"],\"AllAwsRegions\": true}]"`)。

附加以下 IAM 策略以拒绝访问 `InAccessibleAggregator` 或您要拒绝访问的聚合器。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ConfigDeny",
            "Effect": "Deny",
            "Action": [
                "config:BatchGetAggregateResourceConfig",
                "config:DeleteConfigurationAggregator",
                "config:DescribeAggregateComplianceByConfigRules",
                "config:DescribeAggregateComplianceByConformancePacks",
                "config:DescribeConfigurationAggregatorSourcesStatus",
                "config:GetAggregateComplianceDetailsByConfigRule",
                "config:GetAggregateConfigRuleComplianceSummary",
                "config:GetAggregateConformancePackComplianceSummary",
                "config:GetAggregateDiscoveredResourceCounts",
                "config:GetAggregateResourceConfig",
                "config:ListAggregateDiscoveredResources",
                "config:PutConfigurationAggregator",
                "config:SelectAggregateResourceConfig"
            ],
            "Resource": "arn:aws:config:ap-northeast-1:AccountID:config-aggregator/
config-aggregator-pokxzldx"
        }
    ]
}
```

接下来，您可以确认 IAM 策略是否适用于限制对特定聚合器规则的访问：

```
aws configservice get-aggregate-compliance-details-by-config-rule --configuration-
aggregator-name InAccessibleAggregator --config-rule-name rule name --account-
id AccountID --aws-region AwsRegion
```

此命令应返回拒绝访问异常：

```
An error occurred (AccessDeniedException) when calling the
 GetAggregateComplianceDetailsByConfigRule operation: User:
 arn:aws:iam::AccountID:user/ is not
authorized to perform: config:GetAggregateComplianceDetailsByConfigRule on resource:
 arn:aws:config:AwsRegion-1:AccountID:config-aggregator/config-aggregator-pokxzldx
```

AWS 的托管策略 AWS Config

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管策略：AWSConfigServiceRolePolicy

AWS Config 使用名AWSServiceRoleForConfig为的服务关联角色代表您呼叫其他 AWS 服务。使用 AWS Management Console 进行设置时 AWS Config， AWS Config 如果您选择使用 SLR 而不是您自己的 AWS Identity and Access Management (IAM) 服务角色，则会自动创建此 AWS Config SLR。

AWSServiceRoleForConfig SLR 包含托管策略 `AWSConfigServiceRolePolicy`。此托管策略包含 AWS Config 资源的只读和只写权限，以及其他支持的服务中资源的只读权限。 AWS Config 有关更多信息，请参阅 支持的资源类型 和 将服务相关角色用于 AWS Config。

查看政策:AWSConfigServiceRolePolicy.

AWS 托管策略：AWS_ConfigRole

要记录您的 AWS 资源配置， AWS Config 需要 IAM 权限才能获取有关您的资源的配置详细信息。如果要为 AWS Config创建 IAM 角色，可以使用管理型策略 `AWS_ConfigRole` 并将其附加到 IAM 角色。

每次 AWS Config 添加对 AWS 资源类型的支持时，此 IAM 策略都会更新。这意味着，只要 AWS_ConfigRole 角色附加了此托管策略，它 AWS Config 将继续拥有记录所支持资源类型的配置数据所需的权限。有关更多信息，请参阅 支持的资源类型 和 分配给的 IAM 角色的权限 AWS Config。

查看政策：AWS_ConfigRole。

AWS 托管策略：AWSConfigUserAccess

此 IAM 政策提供使用权限 AWS Config，包括按资源标签搜索和读取所有标签。这不提供配置权限 AWS Config，而配置权限需要管理权限。

查看政策:AWSConfigUserAccess.

AWS 托管策略：ConfigConformsServiceRolePolicy

要部署和管理一致性包， AWS Config 需要 IAM 权限和其他 AWS 服务的特定权限。它们允许您部署和管理具有完整功能的一致性包，并且每次都会更新，为一致性包 AWS Config 添加新功能。有关合规包的更多信息，请参阅合规包。

查看政策：ConfigConformsServiceRole政策。

AWS 托管策略：AWSConfigRulesExecutionRole

要部署 AWS 自定义 Lambda 规则， AWS Config 需要 IAM 权限和其他 AWS 服务的特定权限。它们允许 AWS Lambda 函数访问定期发送到 Amazon S3 的 AWS Config AWS Config API 和配置快照。评估 AWS 自定义 Lambda 规则的配置更改的函数需要此访问权限，并且每次 AWS Config 添加新功能时都会更新。有关 AWS 自定义 Lambda 规则的更多信息，请参阅创建自定义 AWS Config Lambda 规则和规则组件。 AWS Config 有关配置快照的更多信息，请参阅概念 | 配置快照。有关传输配置快照的更多信息，请参阅管理传输通道。

查看政策:AWSConfigRulesExecutionRole.

AWS 托管策略：AWSConfigMultiAccountSetupPolicy

要在组织中的成员账户中集中部署、更新和删除 AWS Config 规则和合规包 AWS Organizations， AWS Config 需要 IAM 权限和其他 AWS 服务的特定权限。每次为多账户设置 AWS Config 添加新功能时，都会更新此托管政策。有关更多信息，请参阅管理组织中所有账户的 AWS Config 规则和管理组织中所有账户的合规包。

查看政策:AWSConfigMultiAccountSetupPolicy.

AWS 托管策略：AWSConfigRoleForOrganizations

AWS Config 要允许调用只读 AWS Organizations API， AWS Config 需要 IAM 权限和其他 AWS 服务的特定权限。每次为多账户设置 AWS Config 添加新功能时，都会更新此托管政策。有关更多信息，请参阅管理组织中所有账户的 AWS Config 规则和管理组织中所有账户的合规包。

查看政策:AWSConfigRoleForOrganizations.

AWS 托管策略：AWSConfigRemediationServiceRolePolicy

AWS Config 要允许代表您修复`NON_COMPLIANT`资源， AWS Config 需要 IAM 权限和其他 AWS 服务的特定权限。每次 AWS Config 添加新的补救功能时，都会更新此托管策略。有关修复的更多信息，请

参阅使用规则修复不合规的 AWS Config 资源。有关启动可能的 AWS Config 评估结果的条件的更多信息，请参阅概念 | AWS Config 规则。

查看政策:AWSConfigRemediationServiceRolePolicy.

AWS ConfigAWS 托管策略的更新

查看 AWS Config 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。要获得有关此页面更改的自动提醒，请订阅 “ AWS Config 文档历史记录” 页面上的 RSS feed。

更改	描述	日期
AWS_ConfigRole – 添加 elasticfilesystem:DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource"	该政策现在支持亚马逊弹性文件系统（亚马逊 EFS）、亚马逊 Redshift 和的额外权限。适用于 SAP 的 AWS Systems Manager	2024年6月17日
AWSConfigServiceRolePolicy – 添加 elasticfilesystem:DescribeTags," "redshift:DescribeTags", and "ssm-sap:ListTagsForResource"	该政策现在支持亚马逊弹性文件系统（亚马逊 EFS）、亚马逊 Redshift 和的额外权限。适用于 SAP 的 AWS Systems Manager	2024年6月17日
AWS_ConfigRole – 添加 "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "	该政策现在支持亚马逊托管服务 Prometheus、亚马逊、亚马逊 Cognito CloudWatch、亚马逊、亚马逊 FSx、AWS Identity and Access Management （IAM）、、ElastiCache、、Amazon Redshi AWS Glue ft Serverless AWS Lambda、 AWS RAM 亚马逊和亚马逊简单通知服务 (Amazon SNS) 的额外权限。SageMaker	2024年2月22日

更改	描述	日期
glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments," and "sns:GetSMSSandboxAccountStatus"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "aps:DescribeAlertManagerDefinition," "cloudwatch:DescribeAlarmsForMetric," "cognito-identity:DescribeIdentityPool, "cognito-identity:GetPrincipalTagAttributeMap," "elasticache:DescribeCacheSecurityGroups," "elasticache:DescribeUserGroups," "elasticache:DescribeUsers," "elasticache:DescribeGlobalReplicationGroups," "fsx:DescribeDataRepositoryAssociations," "glue:GetDatabase," "glue:GetDatabases," "iam:ListUsers," "lambda:GetLayerVersion," "lambda:ListLayers," "lambda:ListLayerVersions," "ram:GetPermission," "ram:ListPermissionAssociations," "ram:ListPermissions," "ram:ListPermissionVersions," "redshift-serverless:GetNamespace," "redshift-serverless:GetWorkgroup," "redshift-serverless:ListNamespaces," "redshift-serverless:ListTagsForResource," "redshift-serverless:ListWorkgroups," "sagemaker:DescribeInferenceExperiment," "sagemaker:ListInferenceExperiments,	该政策现在支持亚马逊托管服务 Prometheus、亚马逊、亚马逊 Cognito CloudWatch、亚马逊、亚马逊 FSx、AWS Identity and Access Management（IAM）、、ElastiCache、、Amazon Redshi AWS Glue ft Serverless AWS Lambda、 AWS RAM 亚马逊和亚马逊简单通知服务 (Amazon SNS) 的额外权限。SageMaker	2024年2月22日

更改	描述	日期
" and "sns:GetSMSSandboxAccountStatus"		
AWSConfigUserAccess—AWS Config 开始跟踪此 AWS 托管策略的更改	此政策提供使用权限 AWS Config，包括按资源标签搜索和读取所有标签。这不提供配置权限 AWS Config，而配置权限需要管理权限。	2024年2月22日
AWS_ConfigRole – 添加 "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	该政策现在支持适用于 Prometheus 的亚马逊托管服务 AWS AppConfig 、AWS DMS()、() IAM AWS Database Migration Service 、适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK AWS Identity and Access Management）、亚马逊 AWS Organizations日志和亚马逊简单存储服务 (Amazon S3) Simple Storage Service 的额外权限。 CloudWatch	2023 年 12 月 5 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "appconfig:GetExtensionAssociation," "appconfig:ListExtensionAssociations," "aps:DescribeLoggingConfiguration," "dms:DescribeReplicationTaskAssessmentRuns," "iam:GetOpenIDConnectProvider," "iam:ListOpenIDConnectProviders," "kafka:DescribeVpcConnection," "kafka:GetClusterPolicy," "kafka:ListVpcConnections," "logs:DescribeMetricFilters," "organizations:ListDelegatedAdministrators," "s3:GetBucketPolicyStatus," "s3express:GetBucketPolicy," and "s3express:ListAllMyDirectoryBuckets"	该政策现在支持适用于 Prometheus 的亚马逊托管服务 AWS AppConfig 、AWS DMS()、() IAM AWS Database Migration Service 、适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK AWS Identity and Access Management）、亚马逊 AWS Organizations日志和亚马逊简单存储服务 (Amazon S3) Simple Storage Service 的额外权限。 CloudWatch	2023 年 12 月 5 日

更改	描述	日期
AWS_ConfigRole – 添加 "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA	该政策现在支持亚马逊 Cognito、Amazon Connect、亚马逊 EMR、、、适用于 Redis 的 Amazon MemoryDB AWS Ground Station、、AWS Mainframe Modernization亚马逊、亚马逊 AWS Organizations关系数据库服务（亚马逊 RDS）、亚马逊 Redshift、 QuickSight亚马逊 Redshift、Amazon Route 53 和。 AWS Service Catalog AWS Transfer Family	2023 年 11 月 17 日

更改	描述	日期
ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations,"		

更改	描述	日期
"serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWS_ConfigRole – 添加 "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	此策略现在为 `AWSConfigServiceRolePolicyStatementID` 、`AWSConfigSLRLogStatementID` 、`AWSConfigSLRLogEventStatementID` 和 `AWSConfigSLRApiGatewayStatementID` 添加了安全标识符 (SID)。	2023 年 11 月 17 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "backup:DescribeProtectedResource," "cognito-identity:GetIdentityPoolRoles," "cognito-identity:ListIdentityPools," "cognito-identity:ListTagsForResource," "cognito-idp:DescribeIdentityProvider," "cognito-idp:DescribeResourceServer," "cognito-idp:DescribeUserPool," "cognito-idp:DescribeUserPoolClient," "cognito-idp:DescribeUserPoolDomain," "cognito-idp:GetGroup," "cognito-idp:GetUserPoolMfaConfig," "cognito-idp:ListGroups," "cognito-idp:ListIdentityProviders," "cognito-idp:ListResourceServers," "cognito-idp:ListUserPoolClients," "cognito-idp:ListUserPools," "cognito-idp:ListTagsForResource," "connect:DescribeEvaluationForm," "connect:DescribeInstanceStorageConfig," "connect:DescribePrompt," "connect:DescribeRule," "connect:DescribeUser," "connect:GetTaskTemplate," "connect:ListApprovedOrigins," "connect:ListEvaluationForms," "connect:ListInstanceStorageConfigs," "connect:ListIntegrationA	该政策现在支持亚马逊 Cognito、Amazon Connect、亚马逊 EMR、、、适用于 Redis 的 Amazon MemoryDB AWS Ground Station、、AWS Mainframe Modernization亚马逊、亚马逊 AWS Organizations关系数据库服务（亚马逊 RDS）、亚马逊 Redshift、 QuickSight亚马逊 Redshift、Amazon Route 53 和。 AWS Service Catalog AWS Transfer Family	2023 年 11 月 17 日

更改	描述	日期
ssociations," "connect:ListPrompts," "connect:ListRules," "connect:ListSecurityKeys," "connect:ListTagsForResource," "connect:ListTaskTemplates," "connect:ListUsers," "emr-containers:DescribeVirtualCluster," "emr-containers:ListVirtualClusters," "emr-serverless:GetApplication," "emr-serverless:ListApplications," "groundstation:GetDataflowEndpointGroup," "groundstation:ListDataflowEndpointGroups," "m2:GetEnvironment," "m2:ListEnvironments," "m2:ListTagsForResource," "memorydb:DescribeAcls," "memorydb:DescribeClusters," "memorydb:DescribeParameterGroups," "memorydb:DescribeParameters," "memorydb:DescribeSubnetGroups," "organizations:ListRoots," "quicksight:DescribeAccountSubscription," "quicksight:DescribeDataSetRefreshProperties," "rds:DescribeEngineDefaultClusterParameters," "redshift:DescribeEndpointAccess," "redshift:DescribeEndpointAuthorization," "route53:GetChange," "route53:ListCidrBlocks," "route53:ListCidrLocations,"		

更改	描述	日期
"serviceCatalog:DescribePortfolioShares," "transfer:DescribeProfile," and "transfer:ListProfiles"		
AWSConfigServiceRolePolicy – 添加 "Sid": "AWSConfigServiceRolePolicyStatementID," "Sid": "AWSConfigSLRLogStatementID," "Sid": "AWSConfigSLRLogEventStatementID," and "Sid": "AWSConfigSLRApiGatewayStatementID"	此策略现在为 `AWSConfigServiceRolePolicyStatementID` 、`AWSConfigSLRLogStatementID` 、`AWSConfigSLRLogEventStatementID` 和 `AWSConfigSLRApiGatewayStatementID` 添加了安全标识符 (SID)。	2023 年 11 月 17 日

更改	描述	日期
AWS_ConfigRole – 添加 "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags,	该政策现在支持、、Amazon Connect AWS Private CA AWS App Mesh、亚马逊弹性容器服务 (Amazon ECS)、Amazon Evicently、Ama CloudWatch zon Managed Grafana、亚马逊、Amazon Insp AWS IoT TwinMaker ector、 GuardDuty、、、Amazon Kafka Managed Streaming（ AWS IoT亚马逊 MSK）、、、和亚马逊的额外权限。 AWS Lambda AWS Network Manager AWS Organizations SageMaker	2023 年 10 月 4 日

更改	描述	日期
" "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "acm-pca:GetCertificateAuthorityCertificate," "appmesh:DescribeMesh," "appmesh:ListGatewayRoutes," "connect:DescribeInstance," "connect:DescribeQuickConnect," "connect:ListQuickConnects," "ecs:DescribeCapacityProviders," "evidently:GetSegment," "evidently:ListSegments," "grafana:DescribeWorkspace," "grafana:DescribeWorkspaceAuthentication," "grafana:DescribeWorkspaceConfiguration," "grafana:DescribeWorkspaceConfiguration," "guardduty:GetMemberDetectors," "inspector2:BatchGetAccountStatus," "inspector2:GetDelegatedAdminAccount," "inspector2:ListMembers," "iot:DescribeCACertificate," "iot:ListCACertificates," "iot:ListTagsForResource," "iottwinmaker:GetSyncJob," "iottwinmaker:ListSyncJobs," "kafka:ListTagsForResource," "kafkaconnect:DescribeConnector," "kafkaconnect:ListConnectors," "lambda:GetCodeSigningConfig," "lambda:ListCodeSigningConfigs," "lambda:ListTags,	该政策现在支持、、Amazon Connect AWS Private CA AWS App Mesh、亚马逊弹性容器服务 (Amazon ECS)、Amazon Evicently、Ama CloudWatch zon Managed Grafana、亚马逊、Amazon Insp AWS IoT TwinMaker ector、 GuardDuty、、、Amazon Kafka Managed Streaming（ AWS IoT亚马逊 MSK）、、、和亚马逊的额外权限。 AWS Lambda AWS Network Manager AWS Organizations SageMaker	2023 年 10 月 4 日

更改	描述	日期
" "networkmanager:GetConnectPeer," "organizations:DescribeOrganization," "organizations:ListTargetsForPolicy," "sagemaker:DescribeDataQualityJob," "sagemaker:DescribeModelExplainabilityJob," "sagemaker:ListDataQualityJob," and "sagemaker:ExplainabilityJob"		
AWSConfigServiceRolePolicy— 移除 "ssm:GetParameter"	此策略现在会移除 AWS Systems Manager（Systems Manager）的权限。	2023 年 9 月 6 日

更改	描述	日期
AWS_ConfigRole – 添加 "appmesh:DescribeGatewayRoute","appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets",	该政策现在支持、、亚马逊、、、Amazon Connect AWS App Mesh AWS CloudFormation、 CloudFront AWS CodeArtifact、亚马逊 AWS CodeBuild、AWS Identity and Access Management (IAM) AWS Glue、Amazon Inspector GuardDuty、、、、Amazon Inspector AWS IoT、 AWS IoT TwinMaker、、 AWS IoT Wireless、Amazon Macie、、、、、Amazon Route 53、亚马逊简单存储服务 (Amazon S3) AWS Elemental MediaConnect AWS Network Manager AWS Organizations AWS 资源探索器、亚马逊简单存储服务 (Amazon S3) 和亚马逊简单通知服务 (Amazon SNS) 的额外权限) Simple Service Amazon。	2023 年 7 月 28 日

更改	描述	日期
"macie2:ListTagsForResource", "mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", and "sns:GetDataProtectionPolicy"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "appmesh:DescribeGatewayRoute", "appstream:DescribeStacks", "aps:ListTagsForResource", "cloudfront:GetFunction", "cloudfront:GetOriginAccessControl", "cloudfront:ListFunctions", "cloudfront:ListOriginAccessControls", "codeartifact:ListPackages", "codeartifact:ListPackageVersions", "codebuild:BatchGetReportGroups", "codebuild:ListReportGroups", "connect:ListInstanceAttributes", "connect:ListInstances", "glue:GetPartition", "glue:GetPartitions", "guardduty:GetAdministratorAccount", "iam:ListInstanceProfileTags", "inspector2:ListFilters", "iot:DescribeJobTemplate", "iot:DescribeProvisioningTemplate", "iot:ListJobTemplates", "iot:ListProvisioningTemplates", "iottwinmaker:GetComponentType", "iottwinmaker:ListComponentTypes", "iotwireless:GetFuotaTask", "iotwireless:GetMulticastGroup", "iotwireless:ListFuotaTasks", "iotwireless:ListMulticastGroups", "kafka:ListScramSecrets", "macie2:ListTagsForResource",	该政策现在支持亚马逊 AppStream 2.0 AWS App Mesh、、、亚马逊、、、AWS CloudFormation、Amazon Connect CloudFront AWS CodeArtifact AWS CodeBuild、、亚马逊 AWS Glue、AWS Identity and Access Management (IAM) GuardDuty、Amazon Inspector、 AWS IoT、、 AWS IoT TwinMaker、 AWS IoT Wireless、Amazon Macie、、、、、、、Amazon Route 53 AWS Elemental MediaConnect AWS Network Manager AWS Organizations AWS 资源探索器、亚马逊简单存储服务 (Amazon S3)、亚马逊简单通知服务的额外权限（亚马逊 SNS）Service 和亚马逊 EC2 Systems Manager (SSM)。	2023 年 7 月 28 日

更改	描述	日期
"mediaconnect:ListTagsForResource", "networkmanager:GetConnectPeer", "networkmanager:ListConnectPeers", "organizations:DescribeEffectivePolicy", "organizations:DescribeResourcePolicy", "resource-explorer-2:GetIndex", "resource-explorer-2:ListIndexes", "resource-explorer-2:ListTagsForResource", "route53:ListCidrCollections", "s3:GetMultiRegionAccessPointPolicy", "s3:GetMultiRegionAccessPointPolicyStatus", "sns:GetDataProtectionPolicy", "ssm:DescribeParameters", "ssm:GetParameter", and "ssm:ListTagsForResource"		

更改	描述	日期
AWS_ConfigRole – 添加 "amplify:GetBranch", "amplify: ListBranches", "app-integrat ions:GetEventIntegration", "app-integrations:ListEventI ntegrationAssociations", "ap p-integrations:ListEventInt egrations", "appmesh: DescribeRoute", "ap pmesh:ListRoutes", "aps:List RuleGroupsNamespaces", "athena:GetPreparedStat ement", "athena:ListPrepar edStatements", "batch:Descri beSchedulingPolicies", "batch:ListSchedulingPolici es", "cloudformation:ListTyp es", "cloudtrail:ListTrails", "co deartifact:ListDomains", "co deguru-profiler:DescribePro filingGroup", "codeguru-prof iler:GetNotificationConfigu ration", "codeguru-profiler: GetPolicy", "codeguru-profil er:ListProfilingGroups", "ds:DescribeDomainCon trollers", “dynamodb:Describ eTableReplicaAutoScaling" "dynamodb:DescribeTi meToLive", "ec2:Desc ribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDa	该政策现在支持 Amazon Connect、Amazon Connect AWS Amplify、Prometheus 的亚马逊托管服务 AWS App Mesh、亚马逊 Athena、、、、、、、、、、亚马逊、、、、、（IAM）、亚马逊弹性计算云 (Amazon EC2)、AWS Batch Amazon Evicently AWS CloudFormation、AWS CloudTrail Amazon Forecast AWS CodeArtif act、 CodeGuru、、（IAM）AWS Directory Service、A mazon Evisently、Amazon Forecast、、（IAM）、Am azon E AWS Organizat ions visently、Amazon Forecast、、（ AWS Ground Station IAM） CloudWatc h 、Amazon Managed Streaming for Apazon Managed Kafka Kafka（亚马逊 MSK AWS Identity and Access Managemen t ）、亚马逊 Lightsail 、Amazon Logs、、、Am azon Pinpoint、亚马逊虚拟私有云（亚马逊 AWS IoT Greengrass CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor VPC)、Amazon Personalize QuickSight AWS Migration	2023 年 6 月 13 日

更改	描述	日期
tasetGroup", "forecast :ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases" "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "org	Hub Refactor Spaces、亚马逊、、亚马逊简单存储服务 (Amazon S3)、亚马逊 SageMaker、。 AWS Transfer Family	

更改	描述	日期
anizations:ListAccountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 "amplify:GetBranch", "amplify:ListBranches", "app-integrations:GetEventIntegration", "app-integrations:ListEventIntegrationAssociations", "app-integrations:ListEventIntegrations", "appmesh:DescribeRoute", "appmesh:ListRoutes", "aps:ListRuleGroupsNamespaces", "athena:GetPreparedStatement", "athena:ListPreparedStatements", "batch:DescribeSchedulingPolicies", "batch:ListSchedulingPolicies", "cloudformation:ListTypes", "cloudtrail:ListTrails", "codeartifact:ListDomains", "codeguru-profiler:DescribeProfilingGroup", "codeguru-profiler:GetNotificationConfiguration", "codeguru-profiler:GetPolicy", "codeguru-profiler:ListProfilingGroups", "ds:DescribeDomainControllers", "dynamodb:DescribeTableReplicaAutoScaling", "dynamodb:DescribeTimeToLive", "ec2:DescribeTrafficMirrorFilters", "evidently:GetLaunch", "evidently:ListLaunches", "forecast:DescribeDatasetGroup", "forecast	该政策现在支持 Amazon Connect、Amazon Connect AWS Amplify、Prometheus 的亚马逊托管服务 AWS App Mesh、亚马逊 Athena、、、、、、、、、、亚马逊、、、、、（IAM）、亚马逊弹性计算云 (Amazon EC2)、AWS Batch Amazon Evicently AWS CloudFormation、AWS CloudTrail Amazon Forecast AWS CodeArtifact、 CodeGuru、、（IAM）AWS Directory Service、Amazon Evisently、Amazon Forecast、、（IAM）、Amazon E AWS Organizations visently、Amazon Forecast、、（ AWS Ground Station IAM） CloudWatch 、Amazon Managed Streaming for Apazon Managed Kafka Kafka（亚马逊 MSK AWS Identity and Access Management ）、亚马逊 Lightsail 、Amazon Logs、、、Amazon Pinpoint、亚马逊虚拟私有云（亚马逊 AWS IoT Greengrass CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor VPC)、Amazon Personalize QuickSight AWS Migration	2023 年 6 月 13 日

更改	描述	日期
:ListDatasetGroups", "greengrass:DescribeComponent", "greengrass:GetComponent", "greengrass:ListComponents", "greengrass:ListComponentVersions", "groundstation:GetMissionProfile", "groundstation:ListMissionProfiles", "iam:ListGroups", "iam:ListRoles", "kafka:DescribeConfiguration", "kafka:DescribeConfigurationRevision", "kafka:ListConfigurations", "lightsail:GetRelationalDatabases", "logs:ListTagsLogGroup", "mediaconnect:DescribeFlow", "mediaconnect:ListFlows", "mediatailor:GetPlaybackConfiguration", "mediatailor:ListPlaybackConfigurations", "mobiletargeting:GetApplicationSettings", "mobiletargeting:GetEmailTemplate", "mobiletargeting:GetEventStream", "mobiletargeting:ListTemplates", "networkmanager:GetCustomerGatewayAssociations", "networkmanager:GetLinkAssociations", "organizations:DescribeAccount", "organizations:DescribeOrganizationalUnit", "organizations:ListAccounts", "organizations:ListAcc	Hub Refactor Spaces、亚马逊、、亚马逊简单存储服务 (Amazon S3)、亚马逊 SageMaker、。 AWS Transfer Family	

更改	描述	日期
ountsForParent", "organizations:ListOrganizationalUnitsForParent", "organizations:ListTagsForResource", "personalize:DescribeDataset", "personalize:DescribeDatasetGroup", "personalize:DescribeSchema", "personalize:DescribeSolution", "personalize:ListDatasetGroups", "personalize:ListDatasetImportJobs", "personalize:ListDatasets", "personalize:ListSchemas", "personalize:ListSolutions", "personalize:ListTagsForResource", "quicksight:ListTemplates", "refactor-spaces:GetEnvironment", "refactor-spaces:GetService", "refactor-spaces:ListApplications", "refactor-spaces:ListEnvironments", "refactor-spaces:ListServices", "s3:GetAccessPointPolicyStatusForObjectLambda", "sagemaker:DescribeDeviceFleet", "sagemaker:DescribeFeatureGroup", "sagemaker:ListDeviceFleets", "sagemaker:ListFeatureGroups", "sagemaker:ListModels", and "transfer:ListTagsForResource"		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 amplify:GetApp, amplify:ListApps, appmesh:DescribeVirtualGateway, appmesh:DescribeVirtualNode, appmesh:DescribeVirtualRouter, appmesh:DescribeVirtualService, appmesh:ListMeshes, appmesh:ListTagsForResource, appmesh:ListVirtualGateways, appmesh:ListVirtualNodes, appmesh:ListVirtualRouters, appmesh:ListVirtualServices, apprunner:DescribeVpcConnector, apprunner:ListVpcConnectors, cloudformation:ListTypes, cloudfront:ListResponseHeadersPolicies, codeartifact:ListRepositories, ds:DescribeEventTopics, ds:ListLogSubscriptions, GetInstanceTypesFromInstanceRequirement ec2:GetManagedPrefixListEntries, kendra:DescribeIndex, kendra:ListIndices, kendra:ListTagsForResource, logs:DescribeDestinations, logs:GetDataProtectionPolicy, macie2:DescribeOrganizationConfiguration, macie2:GetAutomatedDiscoveryConfigurat	该政策现在支持亚马逊托管工作流程的额外权限，包括、、、亚马逊 AWS Amplify、、亚马逊弹性计算云 AWS App Mesh AWS App Runner、亚马逊 Kendra CloudFront AWS CodeArtifact、亚马逊 Macie、亚马逊 Route 53、亚马逊、、Amazon Pinpoint、、 SageMaker Resilience Hub、亚马逊 AWS Migration Hub AWS 、Di AWS rectory Service 和。 AWS Transfer Family CloudWatch AWS WAF	2023 年 4 月 13 日

更改	描述	日期
ion，macie2:GetClassificationExportConfiguration，macie2:GetCustomDataIdentifier，macie2:GetFindingsPublicationConfiguration，macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel，refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments，resiliencehub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition，sagemaker:DescribeModelQualityJobDefinition，sagemaker:DescribePipeline, sagemaker:DescribeProject，sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions，sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines，sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

更改	描述	日期
AWS_ConfigRole – 添加 amplify:GetApp，amplify:ListApps，appmesh:DescribeVirtualGateway，appmesh:DescribeVirtualNode，appmesh:DescribeVirtualRouter，appmesh:DescribeVirtualService，appmesh:ListMeshes, appmesh:ListTagsForResource， appmesh:ListVirtualGateways，appmesh:ListVirtualNodes， appmesh:ListVirtualRouters，appmesh:ListVirtualServices，apprunner:DescribeVpcConnector，apprunner:ListVpcConnectors，cloudformation:ListTypes，cloudfront:ListResponseHeadersPolicies，codeartifact:ListRepositories， ds:DescribeEventTopics， ds:ListLogSubscriptions， ec2:GetInstanceTypesFromInstanceRequirement， ec2:GetManagedPrefixListEntries，kendra:DescribeIndex，kendra:ListIndices，kendra:ListTagsForResource， logs:DescribeDestinations， logs:GetDataProtectionPolicy，macie2:DescribeOrganizationConfiguration，macie2:GetAutomatedDiscoveryConfiguration，macie2:GetClassificati	该政策现在支持亚马逊托管工作流程的额外权限，包括、、、亚马逊 AWS Amplify、、亚马逊弹性计算云 AWS App Mesh AWS App Runner、亚马逊 Kendra CloudFront AWS CodeArtifact、亚马逊 Macie、亚马逊 Route 53、亚马逊、、Amazon Pinpoint、、 SageMaker Resilience Hub、亚马逊 AWS Migration Hub AWS 、Di AWS rectory Service 和。 AWS Transfer Family CloudWatch AWS WAF	2023 年 4 月 13 日

更改	描述	日期
onExportConfiguration, macie2:GetCustomDataIdentifier, macie2:GetFindingsPublicationConfiguration, macie2:ListCustomDataIdentifiers, mobiletargeting:GetEmailChannel, refactor-spaces:GetEnvironment, refactor-spaces:ListEnvironments, resilienchub:ListTagsForResource, route53:GetDNSSEC, sagemaker:DescribeDomain, sagemaker:DescribeModelBiasJobDefinition, sagemaker:DescribeModelQualityJobDefinition, sagemaker:DescribePipeline, sagemaker:DescribeProject, sagemaker:ListDomains, sagemaker:ListModelBiasJobDefinitions, sagemaker:ListModelQualityJobDefinitions, sagemaker:ListPipelines, sagemaker:ListProjects, transfer:DescribeAgreement, transfer:DescribeCertificate, transfer:ListAgreements, transfer:ListCertificates, and waf-regional:ListLoggingConfigurations		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 appflow:DescribeFlow，appflow:ListFlows，appflow:ListTagsForResource，apprunner:DescribeService，apprunner:ListServices，apprunner:ListTagsForResource，appstream:DescribeApplications，appstream:DescribeFleets，cloudfront:GetResponseHeadersPolicy，cloudwatch:ListTagsForResource，codeartifact:DescribeRepository，codeartifact:GetRepositoryPermissionsPolicy，codeartifact:ListTagsForResource，codecommit:GetRepository，codecommit:GetRepositoryTriggers， codecommit:ListRepositories，codecommit:ListTagsForResource，devicefarm:GetInstanceProfile，devicefarm:ListInstanceProfiles，devicefarm:ListProjects，evidently:GetProject，evidently:ListProjects，evidently:ListTagsForResource，forecast:DescribeDataset，forecast:ListDatasets，forecast:ListTagsForResource，groundstation:GetConfig，groundstation:ListConfigs，groundstation:ListTagsForResource，iam:GetInstanceProfile，iam:GetSAML	该政策现在支持亚马逊、亚马逊 AppStream 2.0、亚马逊、亚马逊 AppFlow、、、、亚马逊、、 AWS App Runner、Amazon CloudWatch Evicently CloudFront、Amazon F CloudWatch orecast AWS CodeCommit AWS Device Farm、 AWS Identity and Access Management (IAM)、适用于 Redis 的 Amazon MemoryDB AWS IoT、Amazon Pinpoint、、、、亚马逊关系 AWS Network Manager 数据库 AWS Panorama服务 (Amazon RDS)、Amazon Redshift 和亚马逊的额外权限。 AWS CodeArtifact AWS Ground Station SageMaker	2023 年 3 月 30 日

更改	描述	日期
Provider, iam:GetServerCertificate, iam:ListAccessKeys, iam:ListGroups, iam:ListInstanceProfiles, iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles, iam:ListSAMLProviders, iot:DescribeFleetMetric, iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags, mobiletargeting:GetApp, mobiletargeting:GetCampaigns, networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites, panorama:ListNodes, rds:DescribeDBProxyEndpoints, redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig, sagemaker:DescribeImage, sagemaker:DescribeImageVersion, sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

更改	描述	日期
AWS_ConfigRole – 添加 appflow:DescribeFlow, appflow:ListFlows, appflow:ListTagsForResource, apprunner:DescribeService, apprunner:ListServices, apprunner:ListTagsForResource, appstream:DescribeApplications, appstream:DescribeFleets, cloudformation:ListTypes, cloudfront:GetResponseHeadersPolicy, cloudfront:ListDistributions, cloudwatch:ListTagsForResource, codeartifact:DescribeRepository, codeartifact:GetRepositoryPermissionsPolicy, codeartifact:ListTagsForResource, codecommit:GetRepository, codecommit:GetRepositoryTriggers, codecommit:ListRepositories, codecommit:ListTagsForResource, devicefarm:GetInstanceProfile, devicefarm:ListInstanceProfiles, devicefarm:ListProjects, ec2:DescribeTrafficMirrorFilters, evidently:GetProject, evidently:ListProjects, evidently:ListTagsForResource, forecast:DescribeDataset, forecast:ListDatasets, forecast:ListTagsForResource, groundsta	该政策现在支持亚马逊、亚马逊 AppStream 2.0、亚马逊、亚马逊 AppFlow、亚马逊、、、 AWS App Runner、亚马逊弹性计算云 (Amazon EC2) CloudFront CloudWatch AWS CodeArtifact AWS CodeCommit、Amazon Evicently AWS Device Farm、Amazon Forecast、、(IAM)、、A CloudWatch mazon MemoryDB for Redis AWS IoT、Amazon Pinpoint、、、亚马逊关系 AWS Panorama数据库服务 (Amazon RDS) 的额外权限、 AWS Network Manager 亚马逊 Redshift 和亚马逊。 AWS CloudFormation AWS Ground Station AWS Identity and Access Management SageMaker	2023 年 3 月 30 日

更改	描述	日期
tion:GetConfig，groundstation:ListConfigs，groundstation:ListTagsForResource, iam:GetInstanceProfile, iam:GetSAMLProvider, iam:GetServerCertificate，iam:ListAccessKeys，iam:ListGroups，iam:ListInstanceProfiles，iam:ListMFADevices, iam:ListMFADeviceTags, iam:ListRoles，iam:ListSAMLProviders，iot:DescribeFleetMetric，iot:ListFleetMetrics, memorydb:DescribeUsers, memorydb:ListTags，mobiletargeting:GetApp，mobiletargeting:GetCampaigns，networkmanager:GetDevices, networkmanager:GetLinks, networkmanager:GetSites，panorama:ListNodes，rds:DescribeDBProxyEndpoints，redshift:DescribeScheduledActions, sagemaker:DescribeAppImageConfig，sagemaker:DescribeImage，sagemaker:DescribeImageVersion，sagemaker:ListAppImageConfigs, sagemaker:ListImages, and sagemaker:ListImageVersions		

更改	描述	日期
AWSConfigRulesExecutionRole— AWS Config 开始跟踪此 AWS 托管策略的更改	此策略允许 AWS Lambda 函数访问定期发送到 Amazon S3 的 AWS Config AWS Config API 和配置快照。评估 AWS 自定义 Lambda 规则的配置更改的函数需要此访问权限。	2023 年 3 月 7 日
AWSConfigRoleForOrganizations— AWS Config 开始跟踪此 AWS 托管策略的更改	此策略允许调 AWS Config 用只读 AWS Organizations API。	2023 年 3 月 7 日
AWSConfigRemediationServiceRolePolicy— AWS Config 开始跟踪此 AWS 托管策略的更改	此政策 AWS Config 允许代表您修复`NON_COMPLIANT` 资源。	2023 年 3 月 7 日
AWSConfigServiceRolePolicy – 添加 auditmanager:GetAccountStatus	此策略现在授予返回 AWS Audit Manager中的账户注册状态的权限。	2023 年 3 月 3 日
AWS_ConfigRole – 添加 auditmanager:GetAccountStatus	此策略现在授予返回 AWS Audit Manager中的账户注册状态的权限。	2023 年 3 月 3 日
AWSConfigMultiAccountSetupPolicy— AWS Config 开始跟踪此 AWS 托管策略的更改	此策略 AWS Config 允许使用调用 AWS 服务并在整个组织中部署 AWS Config 资源 AWS Organizations。	2023 年 2 月 27 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 airflow:ListTagsForResource，iot:ListCustomMetrics，iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs，appstream:ListTagsForResource， codeguru-reviewer:DescribeRepositoryAssociation，codeguru-reviewer:ListRepositoryAssociations，healthlake:ListFHIRDatastores，healthlake:DescribeFHIRDatastore，healthlake:ListTagsForResource, kinesisvideo:DescribeStream，kinesisvideo:ListStreams， kinesisvideo:ListTagsForStream，kinesisvideo:DescribeSignalingChannel，kinesisvideo:ListTagsForResource，kinesisvideo:ListSignalingChannels，route53-recovery-control-config:DescribeCluster，route53-recovery-control-config:DescribeRoutingControl， route53-recovery-control-config:DescribeSafetyRule， route53-recovery-control-config:ListClusters，route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules，devicefarm:GetTestGridProject，devicefarm:L	该政策现在支持Apache Airflow、Amazon AppStream 2.0、 AWS IoT Amazon CodeGuru Reviewer、Amazon Kinesis Video Streams AWS HealthLake、亚马逊 Route 53 应用程序恢复控制器 AWS Device Farm、亚马逊弹性计算云 (Amazon EC2)、亚马逊 Pinpoint、AWS Identity and Access Management (IAM)、亚马逊和亚马逊日志的额外权限。GuardDuty CloudWatch	2023 年 2 月 1 日

更改	描述	日期
istTestGridProjects，ec2:DescribeCapacityReservationFleets，ec2:DescribeIpamPools， ec2:DescribeIpams，ec2:GetInstanceTypesFromInstanceRequirement，mobiletargeting:GetApplicationSettings，mobiletargeting:ListTagsForResource，ecr:BatchGetRepositoryScanningConfiguration, iam:ListServerCertificates, guardduty:ListPublishingDestinations，guardduty:DescribePublishingDestination，logs:GetLogDelivery, and logs:ListLogDeliveries		

更改	描述	日期
AWS_ConfigRole – 添加 airflow:ListTagsForResource，iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs，appstream:ListTagsForResource，codeguru-reviewer:DescribeRepositoryAssociation，codeguru-reviewer:ListRepositoryAssociations，healthlake:ListFHIRDatastores，healthlake:DescribeFHIRDatastore，healthlake:ListTagsForResource，kinesisvideo:DescribeStream, kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream，kinesisvideo:DescribeSignalingChannel，kinesisvideo:ListTagsForResource，kinesisvideo:ListSignalingChannels，route53-recovery-control-config:DescribeCluster，route53-recovery-control-config:DescribeRoutingControl, route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters，route53-recovery-control-config:ListRoutingControls，route53-recovery-control-config:ListSafetyRules，devicefarm:GetTestGridProject, devicefar	该政策现在支持Apache Airflow、Amazon AppStream 2.0、 AWS IoT Amazon CodeGuru Reviewer、Amazon Kinesis Video Streams AWS HealthLake、亚马逊 Route 53 应用程序恢复控制器 AWS Device Farm、亚马逊弹性计算云 (Amazon EC2)、亚马逊 Pinpoint、AWS Identity and Access Management (IAM)、亚马逊和亚马逊日志的额外权限。GuardDuty CloudWatch	2023 年 2 月 1 日

更改	描述	日期
m:ListTestGridProjects，ec2:DescribeCapacityReservationFleets，ec2:DescribeIpamPools，ec2:DescribeIpams， ec2:GetInstanceTypesFromInstanceRequirement， mobiletargeting:GetApplicationSettings，mobiletargeting:ListTagsForResource， ecr:BatchGetRepositoryScanningConfiguration， iam:ListServerCertificates， guardduty:ListPublishingDestinations，guardduty:DescribePublishingDestination， logs:GetLogDelivery, and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – 更新 config:DescribeConfigRules	作为安全最佳实践，此策略现在取消了对 `config:DescribeConfigRules` 的广泛资源级别权限。	2023 年 1 月 12 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrations, networkmanager:ListTagsFor	该政策现在支持亚马逊托管服务 Prometheus、、、、、、、、、、Amazon Route 53 应用程序恢复控制器 AWS Audit Manager AWS Device Farm、AWS Directory Service、亚马逊弹性计算云 AWS Database Migration Service (AWS DMS Amazon EC2)、、、Amaz AWS IoT on Lightsail AWS Glue、、、Amazon Route 53 应用程序恢复控制器 AWS Elemental MediaPackage AWS Network Manager AWS Resource Access Manager、QuickSight亚马逊简单存储服务 (Amazon S3) 和亚马逊 Timestream 的额外权限。	2022 年 12 月 15 日

更改	描述	日期
Resource，quicksight:DescribeDashboard，quicksight:DescribeDashboardPermissions，quicksight:DescribeTemplate，quicksight:DescribeTemplatePermissions， quicksight:ListDashboards， quicksight:ListTemplates， ram:ListResources，route53-recovery-control-config:DescribeControlPanel，route53-recovery-control-config:ListControlPanels，route53-recovery-control-config:ListTagsForResource，route53resolver:GetResolverQueryLogConfigAssociation，route53resolver:ListResolverQueryLogConfigAssociations， s3:GetAccessPointForObjectLambda，s3:GetAccessPointPolicyForObjectLambda，s3:GetAccessPointPolicyStatusForObjectLambda，s3:GetMultiRegionAccessPoint，s3:ListAccessPointsForObjectLambda，s3:ListMultiRegionAccessPoints， timestream:DescribeEndpoints，transfer:DescribeConnector，transfer:ListConnectors， and transfer:ListTagsForResource		

更改	描述	日期
AWS_ConfigRole – 添加 APS:DescribeRuleGroupsNamespace，APS:DescribeWorkspace，APS:ListWorkspaces，auditmanager:GetAssessment， auditmanager:ListAssessments，devicefarm:GetNetworkProfile，devicefarm:GetProject，devicefarm:ListNetworkProfiles，devicefarm:ListTagsForResource，dms:DescribeEndpoints，ds:ListTagsForResource，ec2:DescribeTags，ec2:DescribeTrafficMirrorSessions，ec2:DescribeTrafficMirrorTargets，ec2:GetIpamPoolAllocations， ec2:GetIpamPoolCidrs， glue:GetMLTransform， glue:GetMLTransforms，glue:ListMLTransforms，iot:DescribeScheduledAudit，iot:ListScheduledAudits，ivs:GetChannel，lightsail:GetRelationalDatabases，mediapackage-vod:DescribePackagingConfiguration，mediapackage-vod:ListPackagingConfigurations，networkmanager:DescribeGlobalNetworks， networkmanager:GetTransitGatewayRegistrations， networkmanager:ListTagsFor	该政策现在支持亚马逊托管服务 Prometheus、、、、、、、、、、Amazon Route 53 应用程序恢复控制器 AWS Audit Manager AWS Device Farm、AWS Directory Service、亚马逊弹性计算云 AWS Database Migration Service (AWS DMS Amazon EC2)、、、Amaz AWS IoT on Lightsail AWS Glue、、、Amazon Route 53 应用程序恢复控制器 AWS Elemental MediaPackage AWS Network Manager AWS Resource Access Manager、QuickSight亚马逊简单存储服务 (Amazon S3) 和亚马逊 Timestream 的额外权限。	2022 年 12 月 15 日

更改	描述	日期
Resource，quicksight:DescribeDashboard，quicksight:DescribeDashboardPermissions，quicksight:DescribeTemplate，quicksight:DescribeTemplatePermissions， quicksight:ListDashboards， quicksight:ListTemplates， ram:ListResources，route53-recovery-control-config:DescribeControlPanel，route53-recovery-control-config:ListControlPanels，route53-recovery-control-config:ListTagsForResource，route53resolver:GetResolverQueryLogConfigAssociation，route53resolver:ListResolverQueryLogConfigAssociations， s3:GetAccessPointForObjectLambda，s3:GetAccessPointPolicyForObjectLambda，s3:GetAccessPointPolicyStatusForObjectLambda，s3:GetMultiRegionAccessPoint，s3:ListAccessPointsForObjectLambda，s3:ListMultiRegionAccessPoints， timestream:DescribeEndpoints，transfer:DescribeConnector，transfer:ListConnectors， and transfer:ListTagsForResource		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 cloudformation:ListStackResources and cloudformation:ListStacks	现在，此策略允许返回指定 AWS CloudFormation 堆栈中所有资源的描述并返回状态与指定StackStatusFilter堆栈的摘要信息。	2022 年 11 月 7 日
AWS_ConfigRole – 添加 cloudformation:ListStackResources and cloudformation:ListStacks	现在，此策略允许返回指定 AWS CloudFormation 堆栈中所有资源的描述并返回状态与指定StackStatusFilter堆栈的摘要信息。	2022 年 11 月 7 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 acm-pca:GetCertificateAuthorityCsr，acm-pca:ListCertificateAuthorities，acm-pca:ListTags， airflow:GetEnvironment， airflow:ListEnvironments， amplifyuibuilder:ListThemes ，appconfig:ListConfigurationProfiles，appconfig:ListDeployments, appconfig:ListDeploymentStrategies，appconfig:ListEnvironments，appconfig:ListHostedConfigurationVersions，cassandra:Select， cloudwatch:DescribeAnomalyDetectors，cloudwatch:GetDashboard，cloudwatch:ListDashboards, connect:DescribePhoneNumber， connect:ListPhoneNumbers， connect:ListPhoneNumbersV2，connect:SearchAvailablePhoneNumbers， databrew:DescribeDataset， databrew:DescribeJob， databrew:DescribeProject， databrew:DescribeRecipe， databrew:DescribeRuleset， databrew:DescribeSchedule， databrew:ListDatasets，databrew:ListJobs，databrew:ListProjects, databrew:ListRecipes，databrew:ListRecipeVersi	该政策现在支持以下方面的额外权限：Apache Airflow AWS Certificate Manager、、、亚马逊密钥空间、亚马逊、Amazon Connect AWS Amplify、 AWS AppConfig亚马逊弹性计算云 (A CloudWatch mazon EC2) AWS Glue DataBrew、亚马逊 Elastic Kubernetes Service（亚马逊 EKS）、亚马逊、、亚马逊 Fraud Detector、Amazon F AWS Fault Injection Service raud Detector、亚马逊 fsX、EventBridge亚马逊、亚马逊定位 GameLift服务、、Amazon Lex、Amazon Lightsail 、Amazon Pinpoint、、、、、亚马逊、亚马逊关系数据库服务（亚马逊 RDS）、 AWS IoT AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight亚马逊 AWS RoboMaker Rekognition AWS Resource Groups、、、Amazon Route 53、亚马逊简单存储服务 AWS Cloud Map(Amazon S3)、以及。 AWS Security Token Service	2022 年 10 月 19 日

更改	描述	日期
ons，databrew:ListRulesets， databrew:ListSchedules， ec2:DescribeRouteTables ，eks:DescribeAddon， eks:DescribeIdentityProvid erConfig, eks:ListAddons，eks :ListIdentityProviderConfigs， events:DescribeConnection ，events:ListApiDestinations ，events:ListConnections，fis :GetExperimentTemplate，fis: ListExperimentTemplates， frauddetector:GetRules， fsx:DescribeBackups，fsx:D escribeSnapshots，fsx:Descri beStorageVirtualMachines，ga melift:DescribeMatchmakingR uleSets，gamelift:DescribeVp cPeeringConnections，geo:Lis tGeofenceCollections，geo:Li stPlaceIndexes，geo:ListRout eCalculators，geo:ListTracke rs，iot:DescribeAccountAudit Configuration，iot:DescribeA uthorizer，iot:DescribeDomai nConfiguration，iot:Describe MitigationAction，iot:ListAu thorizers，iot:ListDomainCon figurations，iot:ListMitigat ionActions，iotsitewise:Desc ribeAssetModel，iotsitewise: DescribeDashboard, iotsitewi se:DescribeGateway，iotsitew ise:DescribePortal，iotsitew ise:DescribeProject，iotsite		

更改	描述	日期
wise:ListAssetModels，iotsitewise:ListDashboards，iotsitewise:ListGateways，iotsitewise:ListPortals，iotsitewise:ListProjectAssets，iotsitewise:ListProjects，iotsitewise:ListTagsForResource，iotwireless:GetServiceProfile，iotwireless:GetWirelessDevice，iotwireless:GetWirelessGatewayTaskDefinition，iotwireless:ListServiceProfiles，iotwireless:ListTagsForResource，iotwireless:ListWirelessDevices，iotwireless:ListWirelessGatewayTaskDefinitions，lex:DescribeBotVersion，lex:ListBotVersions，lightsail:GetContainerServices，lightsail:GetDistributions，lightsail:GetRelationalDatabase，lightsail:GetRelationalDatabaseParameters，mobiletargeting:GetApps，mobiletargeting:GetCampaign，mobiletargeting:GetSegment，mobiletargeting:GetSegments，opsworks:DescribeInstances，opsworks:DescribeTimeBasedAutoScaling，opsworks:DescribeVolumes，panorama:DescribeApplicationInstance，panorama:DescribeApplicationInstanceDetails，panorama:DescribePackage		

更改	描述	日期
, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

更改	描述	日期
AWS_ConfigRole – 添加 acm-pca:GetCertificateAuthorityCsr，acm-pca:ListCertificateAuthorities，acm-pca:ListTags，airflow:GetEnvironment，airflow:ListEnvironments，amplifyuibuilder:ListThemes，appconfig:ListConfigurationProfiles，appconfig:ListDeployments, appconfig:ListDeploymentStrategies，appconfig:ListEnvironments，appconfig:ListHostedConfigurationVersions，cassandra:Select， cloudwatch:DescribeAnomalyDetectors，cloudwatch:GetDashboard，cloudwatch:ListDashboards, connect:DescribePhoneNumber， connect:ListPhoneNumbers， connect:ListPhoneNumbersV2，connect:SearchAvailablePhoneNumbers， databrew:DescribeDataset， databrew:DescribeJob， databrew:DescribeProject， databrew:DescribeRecipe， databrew:DescribeRuleset， databrew:DescribeSchedule， databrew:ListDatasets，databrew:ListJobs，databrew:ListProjects, databrew:ListRecipes，databrew:ListRecipeVersions，databrew:ListRulesets，	该政策现在支持以下方面的额外权限：Apache Airflow AWS Certificate Manager、、、亚马逊密钥空间、亚马逊、Amazon Connect AWS Amplify、 AWS AppConfig亚马逊弹性计算云 (A CloudWatch mazon EC2) AWS Glue DataBrew、亚马逊 Elastic Kubernetes Service（亚马逊 EKS）、亚马逊、、亚马逊 Fraud Detector、Amazon F AWS Fault Injection Service raud Detector、亚马逊 fsX、EventBridge亚马逊、亚马逊定位 GameLift服务、、Amazon Lex、Amazon Lightsail、Amazon Pinpoint、、、、、亚马逊、亚马逊关系数据库服务（亚马逊 RDS）、 AWS IoT AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight亚马逊 AWS RoboMaker Rekognition AWS Resource Groups、、、Amazon Route 53、亚马逊简单存储服务 AWS Cloud Map(Amazon S3)、以及。 AWS Security Token Service	2022 年 10 月 19 日

更改	描述	日期
databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewise:DescribeProject, iotsitewise:ListAssetModels, iotsit		

更改	描述	日期
ewise:ListDashboards，iotsitewise:ListGateways，iotsitewise:ListPortals，iotsitewise:ListProjectAssets，iotsitewise:ListProjects，iotsitewise:ListTagsForResource，iotwireless:GetServiceProfile，iotwireless:GetWirelessDevice，iotwireless:GetWirelessGatewayTaskDefinition，iotwireless:ListServiceProfiles，iotwireless:ListTagsForResource，iotwireless:ListWirelessDevices，iotwireless:ListWirelessGatewayTaskDefinitions，lex:DescribeBotVersion，lex:ListBotVersions，lightsail:GetContainerServices，lightsail:GetDistributions，lightsail:GetRelationalDatabase，lightsail:GetRelationalDatabaseParameters，mobiletargeting:GetApps，mobiletargeting:GetCampaign，mobiletargeting:GetSegment，mobiletargeting:GetSegments，opsworks:DescribeInstances，opsworks:DescribeTimeBasedAutoScaling，opsworks:DescribeVolumes，panorama:DescribeApplicationInstance，panorama:DescribeApplicationInstanceDetails，panorama:DescribePackage，panorama:Describe		

更改	描述	日期
PackageVersion，panorama:ListApplicationInstances，panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions，rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors，resource-groups:GetGroup，resource-groups:GetGroupConfiguration，resource-groups:GetGroupQuery, resource-groups:GetTags，resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications，robomaker:ListSimulationApplications，route53resolver:GetResolverDnssecConfig，route53resolver:ListResolverDnssecConfigs，s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances，sts:GetCallerIdentity，synthetics:GetGroup, synthetics:ListAssociatedGroups，synthetics:ListGroupResources, and synthetics:ListGroups		
AWSConfigServiceRolePolicy – 添加 Glue::GetTable	现在，此策略授予在数据目录中检索指定 AWS Glue 表的表定义的权限。	2022 年 9 月 14 日

更改	描述	日期
AWS_ConfigRole – 添加 Glue::GetTable	现在，此策略授予在数据目录中检索指定 AWS Glue 表的表定义的权限。	2022 年 9 月 14 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirr	该政策现在支持亚马逊 AppFlow、亚马逊、亚马逊 R CloudWatch UM、Amazon Synth CloudWatch etics CloudWatch、Amazon Connect 客户档案、Amazon Connect 语音 ID、亚马逊 DevOps Guru、亚马逊弹性计算云 (Amazon EC2)、亚马逊 EC2 Auto Scaling、亚马逊 EMR、亚马逊、亚马逊、亚马逊架构、Amazon Fraud Detector、亚马逊 Fraud Detector、亚马逊 EMR、亚马逊 Fraud Detector、亚马逊 EMR EventBridge、亚马逊 EventBridge Fraud Detector、亚马逊、 Amazon FinSpace 亚马逊互动视频服务（亚马逊 IVS）Interactive Video Service GameLift、适用于 Apache Flink 的亚马逊托管服务、EC2 Image Builder、Amazon Lex、亚马逊 Lightsail、亚马逊定位服务、亚马逊 Lookout for Equipment、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、亚马逊 Nimble P StudioAmazon inpoint、 QuickSight亚马逊、亚马逊 Route 53 应用程序恢复 Amazon Route 53 Resolver 控制器、亚马逊简单存储服	2022 年 9 月 7 日

更改	描述	日期
orFilters，ec2:DescribeTrafficMirrorTargets，ec2:GetNetworkInsightsAccessScopeAnalysisFindings，ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio，elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint，events:DescribeEventBus，events:DescribeRule，events:ListArchives， events:ListEndpoints， events:ListEventBuses，events:ListRules，events:ListTagsForResource，events:ListTargetsByRule，finspace:GetEnvironment，finspace:ListEnvironments，frauddetector:GetDetectors，frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes，frauddetector:GetEventTypes，frauddetector:GetExternalModels，frauddetector:GetLabels, frauddetector:GetModels，frauddetector:GetOutcomes，frauddetector:GetVariables，frauddetector:ListTagsForResource，gamelift:DescribeAlias，gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity，game	务 (亚马逊 S3) SimpleDB、亚马逊简单电子邮件服务 (Amazon SES)、Amazon Timestream、、、、、、、、、、、、、、、、、、 AWS AppConfig AWS AppSync AWS Auto Scaling AWS Backup AWS Budgets AWS Cost Explorer AWS Cloud9 AWS Directory Service AWS DataSync AWS Elemental MediaPackage AWS Glue AWS IoT AWS IoT Analytics AWS IoT Events AWS IoT SiteWise AWS IoT TwinMaker、 AWS Lake Formation、 AWS License Manager AWS Resilience Hub、 AWS Signer、和 AWS Transfer Family。	

更改	描述	日期
lift:DescribeFleetLocationAttributes，gamelift:DescribeFleetLocationCapacity，gamelift:DescribeFleetPortSettings， gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues，gamelift:DescribeMatchmakingConfigurations，gamelift:DescribeMatchmakingRuleSets， gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript，gamelift:DescribeVpcPeeringAuthorizations，gamelift:ListAliases，gamelift:ListBuilds，gamelift:ListFleets，gamelift:ListGameServerGroups，gamelift:ListScripts，gamelift:ListTagsForResource, geo:ListMaps， glue:GetClassifier，glue:GetClassifiers，imagebuilder:GetContainerRecipe， imagebuilder:GetImage，imagebuilder:GetImagePipeline， imagebuilder:GetImageRecipe，imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines，imagebuilder:ListImageRecipes， imagebuilder:ListImages， iot:DescribeCertificate， iot:DescribeDimension，iot:DescribeRoleAlias，iot:Desc		

更改	描述	日期
ribeSecurityProfile，iot:Get Policy，iot:GetTopicRule，iot :GetTopicRuleDestination， iot:ListCertificates，iot:List Dimensions，iot:ListPolicies ，iot:ListRoleAliases，iot:Li stSecurityProfiles，iot:List SecurityProfilesForTarget，i ot:ListTagsForResource，iot: ListTargetsForSecurityProfi le，iot:ListTopicRuleDestina tions，iot:ListTopicRules，io t:ListV2LoggingLevels，iot:V alidateSecurityProfileBehav iors，iotanalytics:DescribeC hannel，iotanalytics:Describ eDataset, iotanalytics:Descr ibeDatastore，iotanalytics:D escribePipeline，iotanalytic s:ListChannels，iotanalytics :ListDatasets，iotanalytics: ListDatastores，iotanalytics :ListPipelines，iotanalytics :ListTagsForResource，ioteve nts:DescribeAlarmModel，iote vents:DescribeDetectorModel ，iotevents:DescribeInput，io tevents:ListAlarmModels，iot events:ListDetectorModels，i otevents:ListInputs，ioteven ts:ListTagsForResource，iots itewise:DescribeAccessPolic y，iotsitewise:DescribeAsset ，iotsitewise:ListAccessPoli cies，iotsitewise:ListAssets		

更改	描述	日期
, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwinmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:Ge		

更改	描述	日期
tInstance，lightsail:GetInstances，lightsail:GetKeyPair，lightsail:GetLoadBalancer，lightsail:GetLoadBalancers，lightsail:GetLoadBalancerTlsCertificates，lightsail:GetStaticIp，lightsail:GetStaticIps，lookoutequipment:DescribeInferenceScheduler，lookoutequipment:ListTagsForResource，lookoutmetrics:DescribeAlert，lookoutmetrics:DescribeAnomalyDetector，lookoutmetrics:ListAlerts，lookoutmetrics:ListAnomalyDetectors，lookoutmetrics:ListMetricSets，lookoutmetrics:ListTagsForResource，lookoutvision:DescribeProject，lookoutvision:ListProjects，managedblockchain:GetMember，managedblockchain:GetNetwork，managedblockchain:GetNode，managedblockchain:ListInvitations，managedblockchain:ListMembers，managedblockchain:ListNodes，mediapackage-vod:DescribePackagingGroup，mediapackage-vod:ListPackagingGroups，mediapackage-vod:ListTagsForResource，mobiletargeting:GetInAppTemplate，mobiletargeting:		

更改	描述	日期
ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies,		

更改	描述	日期
route53-recovery-readiness:GetCell，route53-recovery-readiness:GetReadinessCheck，route53-recovery-readiness:GetRecoveryGroup，route53-recovery-readiness:GetResourceSet，route53-recovery-readiness:ListCells，route53-recovery-readiness:ListReadinessChecks，route53-recovery-readiness:ListRecoveryGroups，route53-recovery-readiness:ListResourceSets，route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup，route53resolver:GetFirewallRuleGroupAssociation，route53resolver:GetResolverQueryLogConfig，route53resolver:ListFirewallDomainLists，route53resolver:ListFirewallDomains，route53resolver:ListFirewallRuleGroupAssociations，route53resolver:ListFirewallRuleGroups，route53resolver:ListFirewallRules，route53resolver:ListResolverQueryLogConfigs，rum:GetAppMonitor，rum:GetAppMonitorData，rum:ListAppMonitors，rum:ListTagsForResource，s3-outposts:GetAccessPoint，s3-outposts:GetAccessPo		

更改	描述	日期
intPolicy，s3-outposts:GetBucket，s3-outposts:GetBucketPolicy，s3-outposts:GetBucketTagging，s3-outposts:GetLifecycleConfiguration，s3-outposts:ListAccessPoints，s3-outposts:ListEndpoints，s3-outposts:ListRegionalBuckets，schemas:DescribeDiscoverer，schemas:DescribeRegistry，schemas:DescribeSchema，schemas:ListDiscoverers，schemas:ListRegistries，schemas:ListSchemas，sdb:GetAttributes，sdb:ListDomains，ses:ListEmailTemplates，ses:ListReceiptFilters，ses:ListReceiptRuleSets，ses:ListTemplates，signer:GetSigningProfile，signer:ListProfilePermissions，signer:ListSigningProfiles，synthetics:DescribeCanaries，synthetics:DescribeCanariesLastRun，synthetics:DescribeRuntimeVersions，synthetics:GetCanary，synthetics:GetCanaryRuns，synthetics:ListTagsForResource，timestream:DescribeDatabase，timestream:DescribeTable，timestream:ListDatabases，timestream:ListTables，timestream:ListTagsForResource，transfer:DescribeServer，transfer:DescribeUs		

更改	描述	日期
er, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

更改	描述	日期
AWS_ConfigRole – 添加 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTargets,	该政策现在支持亚马逊 AppFlow、亚马逊、亚马逊 R CloudWatch UM、Amazon Synth CloudWatch etics CloudWatch、Amazon Connect 客户档案、Amazon Connect 语音 ID、亚马逊 DevOps Guru、亚马逊弹性计算云 (Amazon EC2)、亚马逊 EC2 Auto Scaling、亚马逊 EMR、亚马逊、亚马逊、亚马逊架构、Amazon Fraud Detector、亚马逊 Fraud Detector、亚马逊 EMR、亚马逊 Fraud Detector、亚马逊 EMR EventBridge、亚马逊 EventBridge Fraud Detector、亚马逊、 Amazon FinSpace 亚马逊互动视频服务（亚马逊 IVS）Interactive Video Service GameLift、适用于 Apache Flink 的亚马逊托管服务、EC2 Image Builder、Amazon Lex、亚马逊 Lightsail、亚马逊定位服务、亚马逊 Lookout for Equipment、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、亚马逊 Nimble P StudioAmazon inpoint、 QuickSight亚马逊、亚马逊 Route 53 应用程序恢复 Amazon Route 53 Resolver 控制器、亚马逊简单存储服	2022 年 9 月 7 日

更改	描述	日期
ec2:GetNetworkInsightsAccessScopeAnalysisFindings, ec2:GetNetworkInsightsAccessScopeContent, elasticmapreduce:DescribeStudio, elasticmapreduce:GetStudioSessionMapping, elasticmapreduce:ListStudios, elasticmapreduce:ListStudioSessionMappings, events:DescribeEndpoint, events:DescribeEventBus, events:DescribeRule, events:ListArchives, events:ListEndpoints, events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion, frauddetector:GetEntityTypes, frauddetector:GetEventTypes, frauddetector:GetExternalModels, frauddetector:GetLabels, frauddetector:GetModels, frauddetector:GetOutcomes, frauddetector:GetVariables, frauddetector:ListTagsForResource, gamelift:DescribeAlias, gamelift:DescribeBuild, gamelift:DescribeFleetAttributes, gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocationAttributes, gamel	务 (亚马逊 S3) SimpleDB、亚马逊简单电子邮件服务 (Amazon SES)、Amazon Timestream、、、

更改	描述	日期
ift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination		

更改	描述	日期
, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorkspace, iottwi		

更改	描述	日期
nmaker:ListEntities, iottwinmaker:ListScenes, iottwinmaker:ListTagsForResource, iottwinmaker:ListWorkspaces, ivs:GetPlaybackKeyPair, ivs:GetRecordingConfiguration, ivs:GetStreamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, ivs:ListRecordingConfigurations, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplications, lakeformation:DescribeResource, lakeformation:GetDataLakeSettings, lakeformation:ListPermissions, lakeformation:ListResources, lex:DescribeBot, lex:DescribeBotAlias, lex:DescribeResourcePolicy, lex:ListBotAliases, lex:ListBotLocales, lex:ListBots, lex:ListTagsForResource, license-manager:GetGrant, license-manager:GetLicense, license-manager:ListDistributedGrants, license-manager:ListLicenses, license-manager:ListReceivedGrants, lightsail:GetAlarms, lightsail:GetBuckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lights		

更改	描述	日期
ail:GetLoadBalancer，lightsail:GetLoadBalancers，lightsail:GetLoadBalancerTlsCertificates，lightsail:GetStaticIp，lightsail:GetStaticIps， lookoutequipment:DescribeInferenceScheduler，lookoutequipment:ListTagsForResource，lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector，lookoutmetrics:ListAlerts，lookoutmetrics:ListAnomalyDetectors，lookoutmetrics:ListMetricSets，lookoutmetrics:ListTagsForResource，lookoutvision:DescribeProject，lookoutvision:ListProjects，managedblockchain:GetMember，managedblockchain:GetNetwork，managedblockchain:GetNode, managedblockchain:ListInvitations， managedblockchain:ListMembers，managedblockchain:ListNodes，mediapackage-vod:DescribePackagingGroup，mediapackage-vod:ListPackagingGroups，mediapackage-vod:ListTagsForResource，mobiletargeting:GetInAppTemplate，mobiletargeting:ListTemplates，mq:DescribeBroker，mq:ListBrokers， nimble:GetLaunchProfile,		

更改	描述	日期
nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetRead		

更改	描述	日期
inessCheck，route53-recovery-readiness:GetRecoveryGroup，route53-recovery-readiness:GetResourceSet，route53-recovery-readiness:ListCells，route53-recovery-readiness:ListReadinessChecks，route53-recovery-readiness:ListRecoveryGroups，route53-recovery-readiness:ListResourceSets，route53resolver:GetFirewallDomainList，route53resolver:GetFirewallRuleGroup，route53resolver:GetFirewallRuleGroupAssociation，route53resolver:GetResolverQueryLogConfig，route53resolver:ListFirewallDomainLists，route53resolver:ListFirewallDomains，route53resolver:ListFirewallRuleGroupAssociations，route53resolver:ListFirewallRuleGroups，route53resolver:ListFirewallRules，route53resolver:ListResolverQueryLogConfigs，rum:GetAppMonitor，rum:GetAppMonitorData，rum:ListAppMonitors，rum:ListTagsForResource，s3-outposts:GetAccessPoint，s3-outposts:GetAccessPointPolicy，s3-outposts:GetBucket，s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging，s3-outposts:GetL		

更改	描述	日期
ifecycleConfiguration，s3-outposts:ListAccessPoints，s3-outposts:ListEndpoints，s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer，schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers，schemas:ListRegistries, schemas:ListSchemas，sdb:GetAttributes，sdb:ListDomains，ses:ListEmailTemplates，ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates，signer:GetSigningProfile，signer:ListProfilePermissions，signer:ListSigningProfiles，synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun，synthetics:DescribeRuntimeVersions, synthetics:GetCanary，synthetics:GetCanaryRuns，synthetics:ListTagsForResource, timestream:DescribeDatabase，timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource，transfer:DescribeServer，transfer:DescribeUser, transfer:DescribeWorkflow，transfer:ListServers, transfer:ListUsers, transfer:		

更改	描述	日期
ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 airflow:ListTagsForResource, iot:ListCustomMetrics，iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs，appstream:ListTagsForResource, codeguru-reviewer:DescribeRepositoryAssociation, codeguru-reviewer:ListRepositoryAssociations, healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore，healthlake:ListTagsForResource, kinesisvideo:DescribeStream，kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream，kinesisvideo:DescribeSignalingChannel，kinesisvideo:ListTagsForResource，kinesisvideo:ListSignalingChannels，route53-recovery-control-config:DescribeCluster，route53-recovery-control-config:DescribeRoutingControl，route53-recovery-control-config:DescribeSafetyRule，route53-recovery-control-config:ListClusters，route53-recovery-control-config:ListRoutingControls, route53-recovery-control-config:ListSafetyRules，devicefarm:GetTestGridProject,	该政策现在支持Apache Airflow、Amazon AppStream 2.0、 AWS IoT Amazon CodeGuru Reviewer、Amazon Kinesis Video Streams AWS HealthLake、亚马逊 Route 53 应用程序恢复控制器 AWS Device Farm、亚马逊弹性计算云 (Amazon EC2)、亚马逊 Pinpoint、 AWS Identity and Access Management (IAM)、亚马逊和亚马逊日志的额外权限。GuardDuty CloudWatch	2023 年 2 月 1 日

更改	描述	日期
devicefarm:ListTestGridProjects，ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools，ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement, mobiletargeting:GetApplicationSettings，mobiletargeting:ListTagsForResource, ecr:BatchGetRepositoryScanningConfiguration，iam:ListServerCertificates, guardduty:ListPublishingDestinations, guardduty:DescribePublishingDestination, logs:GetLogDelivery, and logs:ListLogDeliveries		

更改	描述	日期
AWS_ConfigRole – 添加 airflow:ListTagsForResource, iot:ListCustomMetrics, iot:DescribeCustomMetric, appstream:DescribeDirectoryConfigs，appstream:ListTagsForResource，codeguru-reviewer:DescribeRepositoryAssociation，codeguru-reviewer:ListRepositoryAssociations，healthlake:ListFHIRDatastores, healthlake:DescribeFHIRDatastore，healthlake:ListTagsForResource, kinesisvideo:DescribeStream，kinesisvideo:ListStreams, kinesisvideo:ListTagsForStream，kinesisvideo:DescribeSignalingChannel，kinesisvideo:ListTagsForResource，kinesisvideo:ListSignalingChannels，route53-recovery-control-config:DescribeCluster, route53-recovery-control-config:DescribeRoutingControl，route53-recovery-control-config:DescribeSafetyRule, route53-recovery-control-config:ListClusters，route53-recovery-control-config:ListRoutingControls，route53-recovery-control-config:ListSafetyRules，devicefarm:GetTestGridProject, devicefar	该政策现在支持Apache Airflow、Amazon AppStream 2.0、 AWS IoT Amazon CodeGuru Reviewer、Amazon Kinesis Video Streams AWS HealthLake、亚马逊 Route 53 应用程序恢复控制器 AWS Device Farm、亚马逊弹性计算云 (Amazon EC2)、亚马逊 Pinpoint、AWS Identity and Access Management (IAM)、亚马逊和亚马逊日志的额外权限。GuardDuty CloudWatch	2023 年 2 月 1 日

更改	描述	日期
m:ListTestGridProjects，ec2:DescribeCapacityReservationFleets, ec2:DescribeIpamPools，ec2:DescribeIpams, ec2:GetInstanceTypesFromInstanceRequirement，mobiletargeting:GetApplicationSettings，mobiletargeting:ListTagsForResource，ecr:BatchGetRepositoryScanningConfiguration，iam:ListServerCertificates，guardduty:ListPublishingDestinations，guardduty:DescribePublishingDestination, logs:GetLogDelivery，and logs:ListLogDeliveries		
ConfigConformsServiceRolePolicy – 更新 config:DescribeConfigRules	作为安全最佳实践，此策略现在取消了对 `config:DescribeConfigRules` 的广泛资源级别权限。	2023 年 1 月 12 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace, APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile, AWS Transfer Family devicefarm:GetProject, devicefarm:ListNetworkProfiles, devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags, ec2:DescribeTrafficMirrorSessions, ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations, ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel, lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations, networkmanager:DescribeGlobalNetworks, networkmanager:GetTransitGatewayRegistrat	该政策现在支持亚马逊托管服务 Prometheus、、、、、、、、、、Amazon Route 53 应用程序恢复控制器 AWS Audit Manager AWS Device Farm、AWS Directory Service、亚马逊弹性计算云 AWS Database Migration Service (AWS DMS Amazon EC2)、、、Amaz AWS IoT on Lightsail AWS Glue、、、Amazon Route 53 应用程序恢复控制器 AWS Elemental MediaPackage AWS Network Manager AWS Resource Access Manager、QuickSight亚马逊简单存储服务 (Amazon S3) 和亚马逊 Timestream 的额外权限。	2022 年 12 月 15 日

更改	描述	日期
ions，networkmanager:ListTagsForResource，quicksight:DescribeDashboard，quicksight:DescribeDashboardPermissions，quicksight:DescribeTemplate，quicksight:DescribeTemplatePermissions，quicksight:ListDashboards, quicksight:ListTemplates，ram:ListResources，route53-recovery-control-config:DescribeControlPanel，route53-recovery-control-config:ListControlPanels，route53-recovery-control-config:ListTagsForResource，route53resolver:GetResolverQueryLogConfigAssociation，route53resolver:ListResolverQueryLogConfigAssociations，s3:GetAccessPointForObjectLambda，s3:GetAccessPointPolicyForObjectLambda，s3:GetAccessPointPolicyStatusForObjectLambda，s3:GetMultiRegionAccessPoint，s3:ListAccessPointsForObjectLambda，s3:ListMultiRegionAccessPoints, timestream:DescribeEndpoints，transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

更改	描述	日期
AWS_ConfigRole – 添加 APS:DescribeRuleGroupsNamespace, APS:DescribeWorkspace，APS:ListWorkspaces, auditmanager:GetAssessment, auditmanager:ListAssessments, devicefarm:GetNetworkProfile，devicefarm:GetProject, devicefarm:ListNetworkProfiles，devicefarm:ListTagsForResource, dms:DescribeEndpoints, ds:ListTagsForResource, ec2:DescribeTags，ec2:DescribeTrafficMirrorSessions，ec2:DescribeTrafficMirrorTargets, ec2:GetIpamPoolAllocations，ec2:GetIpamPoolCidrs, glue:GetMLTransform, glue:GetMLTransforms, glue:ListMLTransforms, iot:DescribeScheduledAudit, iot:ListScheduledAudits, ivs:GetChannel，lightsail:GetRelationalDatabases, mediapackage-vod:DescribePackagingConfiguration, mediapackage-vod:ListPackagingConfigurations，networkmanager:DescribeGlobalNetworks，networkmanager:GetTransitGatewayRegistrations，networkmanager:ListTa	该政策现在支持亚马逊托管服务 Prometheus、、、、、、、、、、Amazon Route 53 应用程序恢复控制器 AWS Audit Manager AWS Device Farm、AWS Directory Service、亚马逊弹性计算云 AWS Database Migration Service (AWS DMS Amazon EC2)、、、Amaz AWS IoT on Lightsail AWS Glue、、、Amazon Route 53 应用程序恢复控制器 AWS Elemental MediaPackage AWS Network Manager AWS Resource Access Manager、QuickSight亚马逊简单存储服务 (Amazon S3) 和亚马逊 Timestream 的额外权限。	2022 年 12 月 15 日

更改	描述	日期
gsForResource，quicksight:DescribeDashboard，quicksight:DescribeDashboardPermissions，quicksight:DescribeTemplate，quicksight:DescribeTemplatePermissions，quicksight:ListDashboards, quicksight:ListTemplates，ram:ListResources，route53-recovery-control-config:DescribeControlPanel，route53-recovery-control-config:ListControlPanels，route53-recovery-control-config:ListTagsForResource，route53resolver:GetResolverQueryLogConfigAssociation，route53resolver:ListResolverQueryLogConfigAssociations，s3:GetAccessPointForObjectLambda，s3:GetAccessPointPolicyForObjectLambda，s3:GetAccessPointPolicyStatusForObjectLambda，s3:GetMultiRegionAccessPoint，s3:ListAccessPointsForObjectLambda，s3:ListMultiRegionAccessPoints，timestream:DescribeEndpoints，transfer:DescribeConnector, transfer:ListConnectors, and transfer:ListTagsForResource		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 cloudformation:ListStackResources and cloudformation:ListStacks	现在，此策略允许返回指定 AWS CloudFormation 堆栈中所有资源的描述并返回状态与指定StackStatusFilter堆栈的摘要信息。	2022 年 11 月 7 日
AWS_ConfigRole – 添加 cloudformation:ListStackResources and cloudformation:ListStacks	现在，此策略允许返回指定 AWS CloudFormation 堆栈中所有资源的描述并返回状态与指定StackStatusFilter堆栈的摘要信息。	2022 年 11 月 7 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 acm-pca:GetCertificateAuthorityCsr，acm-pca:ListCertificateAuthorities, acm-pca:ListTags，airflow:GetEnvironment, airflow:ListEnvironments，amplifyuibuilder:ListThemes，appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments，appconfig:ListHostedConfigurationVersions, cassandra:Select，cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber，connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset，databrew:DescribeJob, databrew:DescribeProject，databrew:DescribeRecipe, databrew:DescribeRuleset，databrew:DescribeSchedule, databrew:ListDatasets，databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	该政策现在支持以下方面的额外权限：Apache Airflow AWS Certificate Manager、、、亚马逊密钥空间、亚马逊、Amazon Connect AWS Amplify、 AWS AppConfig亚马逊弹性计算云 (A CloudWatch mazon EC2) AWS Glue DataBrew、亚马逊 Elastic Kubernetes Service（亚马逊 EKS）、亚马逊、、亚马逊 Fraud Detector、Amazon F AWS Fault Injection Service raud Detector、亚马逊 fsX、EventBridge亚马逊、亚马逊定位 GameLift服务、、Amazon Lex、Amazon Lightsail、Amazon Pinpoint、、、、、亚马逊、亚马逊关系数据库服务（亚马逊 RDS）、 AWS IoT AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight亚马逊 AWS RoboMaker Rekognition AWS Resource Groups、、、Amazon Route 53、亚马逊简单存储服务 AWS Cloud Map(Amazon S3)、以及。 AWS Security Token Service	2022 年 10 月 19 日

更改	描述	日期
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

更改	描述	日期
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

更改	描述	日期
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

更改	描述	日期
AWS_ConfigRole – 添加 acm-pca:GetCertificateAuthorityCsr，acm-pca:ListCertificateAuthorities, acm-pca:ListTags，airflow:GetEnvironment, airflow:ListEnvironments，amplifyuibuilder:ListThemes，appconfig:ListConfigurationProfiles, appconfig:ListDeployments, appconfig:ListDeploymentStrategies, appconfig:ListEnvironments，appconfig:ListHostedConfigurationVersions, cassandra:Select，cloudwatch:DescribeAnomalyDetectors, cloudwatch:GetDashboard, cloudwatch:ListDashboards, connect:DescribePhoneNumber，connect:ListPhoneNumbers, connect:ListPhoneNumbersV2, connect:SearchAvailablePhoneNumbers, databrew:DescribeDataset，databrew:DescribeJob, databrew:DescribeProject，databrew:DescribeRecipe, databrew:DescribeRuleset，databrew:DescribeSchedule, databrew:ListDatasets，databrew:ListJobs, databrew:ListProjects, databrew:ListRecipes, databrew:ListRecipeVers	该政策现在支持以下方面的额外权限：Apache Airflow AWS Certificate Manager、、、亚马逊密钥空间、亚马逊、Amazon Connect AWS Amplify、 AWS AppConfig亚马逊弹性计算云 (A CloudWatch mazon EC2) AWS Glue DataBrew、亚马逊 Elastic Kubernetes Service（亚马逊 EKS）、亚马逊、、亚马逊 Fraud Detector、Amazon F AWS Fault Injection Service raud Detector、亚马逊 fsX、EventBridge亚马逊、亚马逊定位 GameLift服务、、Amazon Lex、Amazon Lightsail、Amazon Pinpoint、、、、、亚马逊、亚马逊关系数据库服务（亚马逊 RDS）、 AWS IoT AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight亚马逊 AWS RoboMaker Rekognition AWS Resource Groups、、、Amazon Route 53、亚马逊简单存储服务 AWS Cloud Map(Amazon S3)、以及。 AWS Security Token Service	2022 年 10 月 19 日

更改	描述	日期
ions, databrew:ListRulesets, databrew:ListSchedules, ec2:DescribeRouteTables, eks:DescribeAddon, eks:DescribeIdentityProviderConfig, eks:ListAddons, eks:ListIdentityProviderConfigs, events:DescribeConnection, events:ListApiDestinations, events:ListConnections, fis:GetExperimentTemplate, fis:ListExperimentTemplates, frauddetector:GetRules, fsx:DescribeBackups, fsx:DescribeSnapshots, fsx:DescribeStorageVirtualMachines, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeVpcPeeringConnections, geo:ListGeofenceCollections, geo:ListPlaceIndexes, geo:ListRouteCalculators, geo:ListTrackers, iot:DescribeAccountAuditConfiguration, iot:DescribeAuthorizer, iot:DescribeDomainConfiguration, iot:DescribeMitigationAction, iot:ListAuthorizers, iot:ListDomainConfigurations, iot:ListMitigationActions, iotsitewise:DescribeAssetModel, iotsitewise:DescribeDashboard, iotsitewise:DescribeGateway, iotsitewise:DescribePortal, iotsitewi		

更改	描述	日期
se:DescribeProject, iotsite wise:ListAssetModels, iotsitewi se:ListDashboards, iotsitew ise:ListGateways, iotsitewi se:ListPortals, iotsitewise :ListProjectAssets, iotsitewi se:ListProjects, iotsitewis e:ListTagsForResource, iotwireless:GetServiceProfi le, iotwireless:GetWireless Device, iotwireless:GetWire lessGatewayTaskDefinition, iotwireless:ListServiceProf iles, iotwireless:ListTagsF orResource, iotwireless:Lis tWirelessDevices, iotwirele ss:ListWirelessGatewayTaskD efinitions, lex:DescribeBot Version, lex:ListBotVersions, lightsail:GetContainerServices, lightsail:GetDistributions, lightsail:GetRelationalDat abase, lightsail:GetRelatio nalDatabaseParameters, mobiletargeting:GetApps, mobiletargeting:GetCampaign , mobiletargeting:GetSegmen t, mobiletargeting:Ge tSegments, opsworks:Describ eInstances, opsworks:Descri beTimeBasedAutoScaling, opsworks:DescribeVolumes, panorama:DescribeApplication Instance, panorama:Describe ApplicationInstanceDetails,		

更改	描述	日期
panorama:DescribePackage, panorama:DescribePackageVersion, panorama:ListApplicationInstances, panorama:ListPackages, quicksight:ListDataSources, ram:ListResourceSharePermissions, rds:DescribeDBProxies, rds:DescribeGlobalClusters, rekognition:ListStreamProcessors, resource-groups:GetGroup, resource-groups:GetGroupConfiguration, resource-groups:GetGroupQuery, resource-groups:GetTags, resource-groups:ListGroupResources, resource-groups:ListGroups, robomaker:ListRobotApplications, robomaker:ListSimulationApplications, route53resolver:GetResolverDnssecConfig, route53resolver:ListResolverDnssecConfigs, s3:ListStorageLensConfigurations, schemas:GetResourcePolicy, servicediscovery:ListInstances, sts:GetCallerIdentity, synthetics:GetGroup, synthetics:ListAssociatedGroups, synthetics:ListGroupResources, and synthetics:ListGroups		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 Glue::GetTable	现在，此策略授予在数据目录中检索指定 AWS Glue 表的表定义的权限。	2022 年 9 月 14 日
AWS_ConfigRole – 添加 Glue::GetTable	现在，此策略授予在数据目录中检索指定 AWS Glue 表的表定义的权限。	2022 年 9 月 14 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 appconfig:ListApplications，appflow:DescribeConnectorProfiles, appsync:GetApiCache，autoscaling-plans:DescribeScalingPlanResources，autoscaling-plans:DescribeScalingPlans，autoscaling-plans:GetScalingPlanResourceForecastData，autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction，budgets:DescribeBudgetActionsForAccount，budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships，cloud9:DescribeEnvironments, cloud9:ListEnvironments，cloud9:ListTagsForResource, cloudwatch:GetMetricStream，cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows，devops-guru:GetResourceCollection, ds:DescribeDirectories，ec2:DescribeTrafficMirrorFilte	该政策现在支持亚马逊 AppFlow、亚马逊、亚马逊 R CloudWatch UM、Amazon Synth CloudWatch etics CloudWatch、Amazon Connect 客户档案、Amazon Connect 语音 ID、亚马逊 DevOps Guru、亚马逊弹性计算云 (Amazon EC2)、亚马逊 EC2 Auto Scaling、亚马逊 EMR、亚马逊、亚马逊、亚马逊架构、Amazon Fraud Detector、亚马逊 Fraud Detector、亚马逊 EMR、亚马逊 Fraud Detector、亚马逊 EMR EventBridge、亚马逊 EventBridge Fraud Detector、亚马逊、 Amazon FinSpace 亚马逊互动视频服务（亚马逊 IVS）Interactive Video Service GameLift、适用于 Apache Flink 的亚马逊托管服务、EC2 Image Builder、Amazon Lex、亚马逊 Lightsail、亚马逊定位服务、亚马逊 Lookout for Equipment、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、亚马逊 Nimble P StudioAmazon inpoint、 QuickSight亚马逊、亚马逊 Route 53 应用程序恢复 Amazon Route 53 Resolver 控制器、亚马逊简单存储服	2022 年 9 月 7 日

更改	描述	日期
rs，ec2:DescribeTrafficMirrorTargets，ec2:GetNetworkInsightsAccessScopeAnalysisFindings，ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio，elasticmapreduce:GetStudioSessionMapping，elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings，events:DescribeEndpoint, events:DescribeEventBus，events:DescribeRule, events:ListArchives, events:ListEndpoints，events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule, finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes, frauddetector:GetEventTypes，frauddetector:GetExternalModels, frauddetector:GetLabels，frauddetector:GetModels, frauddetector:GetOutcomes，frauddetector:GetVariables, frauddetector:ListTagsForResource，gamelift:DescribeAlias, gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity,	务 (亚马逊 S3) SimpleDB、亚马逊简单电子邮件服务 (Amazon SES)、Amazon Timestream、、、

更改	描述	日期
gamelift:DescribeFleetLocationAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias,		

更改	描述	日期
iot:DescribeSecurityProfile, iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolic		

更改	描述	日期
ies, iotsitewise:ListAssets, iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu		

更改	描述	日期
ckets, lightsail:GetCertificates, lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:		

更改	描述	日期
GetInAppTemplate, mobiletargeting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings,		

更改	描述	日期
resiliencehub:ListResiliencyPolicies, route53-recovery-readiness:GetCell, route53-recovery-readiness:GetReadinessCheck, route53-recovery-readiness:GetRecoveryGroup, route53-recovery-readiness:GetResourceSet, route53-recovery-readiness:ListCells, route53-recovery-readiness:ListReadinessChecks, route53-recovery-readiness:ListRecoveryGroups, route53-recovery-readiness:ListResourceSets, route53resolver:GetFirewallDomainList, route53resolver:GetFirewallRuleGroup, route53resolver:GetFirewallRuleGroupAssociation, route53resolver:GetResolverQueryLogConfig, route53resolver:ListFirewallDomainLists, route53resolver:ListFirewallDomains, route53resolver:ListFirewallRuleGroupAssociations, route53resolver:ListFirewallRuleGroups, route53resolver:ListFirewallRules, route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor, rum:GetAppMonitorData, rum:ListAppMonitors, rum:ListTagsForResource, s3-outposts:GetAccessPoint,		

更改	描述	日期
s3-outposts:GetAccessPoint Policy, s3-outposts:GetBuc ket, s3-outposts:GetBucketP olicy, s3-outposts:GetBuc ketTagging, s3-outposts:Get LifecycleConfiguration, s3- outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuc kets, schemas:DescribeDi scoverer, schemas:DescribeR egistry, schemas:DescribeSc hema, schemas:ListDiscovere rs, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListD omains, ses:ListEmailTempla tes, ses:ListReceiptFilters, ses:ListReceiptRuleSe ts, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissio ns, signer:ListSigningProfiles, synthetics:DescribeCanaries , synthetics:DescribeCanari esLastRun, synthetics:Descr ibeRuntimeVersions, synthetic s:GetCanary, synthetics:Get CanaryRuns, synthetic s:ListTagsForResource, time stream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, time stream:ListTagsForResource,		

更改	描述	日期
transfer:DescribeServer，transfer:DescribeUser, transfer:DescribeWorkflow，transfer:ListServers, transfer:ListUsers，transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		

更改	描述	日期
AWS_ConfigRole – 添加 appconfig:ListApplications, appflow:DescribeConnectorProfiles, appsync:GetApiCache, autoscaling-plans:DescribeScalingPlanResources, autoscaling-plans:DescribeScalingPlans, autoscaling-plans:GetScalingPlanResourceForecastData, autoscaling:DescribeWarmPool, backup:DescribeFramework, backup:DescribeReportPlan, backup:ListFrameworks, backup:ListReportPlans, budgets:DescribeBudgetAction, budgets:DescribeBudgetActionsForAccount, budgets:DescribeBudgetActionsForBudget, budgets:ViewBudget, ce:GetAnomalyMonitors, ce:GetAnomalySubscriptions, cloud9:DescribeEnvironmentMemberships, cloud9:DescribeEnvironments, cloud9:ListEnvironments, cloud9:ListTagsForResource, cloudwatch:GetMetricStream, cloudwatch:ListMetricStreams, datasync:DescribeLocationFsxWindows, devops-guru:GetResourceCollection, ds:DescribeDirectories, ec2:DescribeTrafficMirrorTarge	该政策现在支持亚马逊 AppFlow、亚马逊、亚马逊 R CloudWatch UM、Amazon Synth CloudWatch etics CloudWatch、Amazon Connect 客户档案、Amazon Connect 语音 ID、亚马逊 DevOps Guru、亚马逊弹性计算云 (Amazon EC2)、亚马逊 EC2 Auto Scaling、亚马逊 EMR、亚马逊、亚马逊、亚马逊架构、Amazon Fraud Detector、亚马逊 Fraud Detector、亚马逊 EMR、亚马逊 Fraud Detector、亚马逊 EMR EventBridge、亚马逊 EventBridge Fraud Detector、亚马逊、 Amazon FinSpace 亚马逊互动视频服务（亚马逊 IVS）Interactive Video Service GameLift、适用于 Apache Flink 的亚马逊托管服务、EC2 Image Builder、Amazon Lex、亚马逊 Lightsail、亚马逊定位服务、亚马逊 Lookout for Equipment、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、亚马逊 Nimble P StudioAmazon inpoint、 QuickSight亚马逊、亚马逊 Route 53 应用程序恢复 Amazon Route 53 Resolver 控制器、亚马逊简单存储服	2022 年 9 月 7 日

更改	描述	日期
ts，ec2:GetNetworkInsightsAccessScopeAnalysisFindings， ec2:GetNetworkInsightsAccessScopeContent，elasticmapreduce:DescribeStudio， elasticmapreduce:GetStudioSessionMapping，elasticmapreduce:ListStudios，elasticmapreduce:ListStudioSessionMappings，events:DescribeEndpoint, events:DescribeEventBus，events:DescribeRule, events:ListArchives, events:ListEndpoints，events:ListEventBuses, events:ListRules, events:ListTagsForResource, events:ListTargetsByRule， finspace:GetEnvironment, finspace:ListEnvironments, frauddetector:GetDetectors, frauddetector:GetDetectorVersion，frauddetector:GetEntityTypes, frauddetector:GetEventTypes，frauddetector:GetExternalModels, frauddetector:GetLabels，frauddetector:GetModels, frauddetector:GetOutcomes，frauddetector:GetVariables, frauddetector:ListTagsForResource，gamelift:DescribeAlias, gamelift:DescribeBuild，gamelift:DescribeFleetAttributes，gamelift:DescribeFleetCapacity, gamelift:DescribeFleetLocat	务 (亚马逊 S3) SimpleDB、亚马逊简单电子邮件服务 (Amazon SES)、Amazon Timestream、、、

更改	描述	日期
ionAttributes, gamelift:DescribeFleetLocationCapacity, gamelift:DescribeFleetPortSettings, gamelift:DescribeGameServerGroup, gamelift:DescribeGameSessionQueues, gamelift:DescribeMatchmakingConfigurations, gamelift:DescribeMatchmakingRuleSets, gamelift:DescribeRuntimeConfiguration, gamelift:DescribeScript, gamelift:DescribeVpcPeeringAuthorizations, gamelift:ListAliases, gamelift:ListBuilds, gamelift:ListFleets, gamelift:ListGameServerGroups, gamelift:ListScripts, gamelift:ListTagsForResource, geo:ListMaps, glue:GetClassifier, glue:GetClassifiers, imagebuilder:GetContainerRecipe, imagebuilder:GetImage, imagebuilder:GetImagePipeline, imagebuilder:GetImageRecipe, imagebuilder:ListContainerRecipes, imagebuilder:ListImageBuildVersions, imagebuilder:ListImagePipelines, imagebuilder:ListImageRecipes, imagebuilder:ListImages, iot:DescribeCertificate, iot:DescribeDimension, iot:DescribeRoleAlias, iot:DescribeSecurityProfile,		

更改	描述	日期
iot:GetPolicy, iot:GetTopicRule, iot:GetTopicRuleDestination, iot:ListCertificates, iot:ListDimensions, iot:ListPolicies, iot:ListRoleAliases, iot:ListSecurityProfiles, iot:ListSecurityProfilesForTarget, iot:ListTagsForResource, iot:ListTargetsForSecurityProfile, iot:ListTopicRuleDestinations, iot:ListTopicRules, iot:ListV2LoggingLevels, iot:ValidateSecurityProfileBehaviors, iotanalytics:DescribeChannel, iotanalytics:DescribeDataset, iotanalytics:DescribeDatastore, iotanalytics:DescribePipeline, iotanalytics:ListChannels, iotanalytics:ListDatasets, iotanalytics:ListDatastores, iotanalytics:ListPipelines, iotanalytics:ListTagsForResource, iotevents:DescribeAlarmModel, iotevents:DescribeDetectorModel, iotevents:DescribeInput, iotevents:ListAlarmModels, iotevents:ListDetectorModels, iotevents:ListInputs, iotevents:ListTagsForResource, iotsitewise:DescribeAccessPolicy, iotsitewise:DescribeAsset, iotsitewise:ListAccessPolicies, iotsitewise:ListAssets,		

更改	描述	日期
iottwinmaker:GetEntity, iottwinmaker:GetScene, iottwinmaker:GetWorksp ace, iottwinmaker:ListE ntities, iottwinmaker:ListS cenes, iottwinmaker:ListT agsForResource, iottwinmake r:ListWorkspaces, ivs:GetPl aybackKeyPair, ivs:GetRecor dingConfiguration, ivs:GetSt reamKey, ivs:ListChannels, ivs:ListPlaybackKeyPairs, i vs:ListRecordingConfigurati ons, ivs:ListStreamKeys, ivs:ListTagsForResource, kinesisanalytics:ListApplic ations, lakeformation:Descr ibeResource, lakeformation: GetDataLakeSettings, lakefo rmation:ListPermissions, lakeformation:ListResources , lex:DescribeBot, lex:Descr ibeBotAlias, lex:DescribeRe sourcePolicy, lex:ListB otAliases, lex:ListBotLocal es, lex:ListBots, lex:ListT agsForResource, license-manager:GetGrant, license-m anager:GetLicense, license-manager:ListDistributedGran ts, license-manager:ListLic enses, license-manager:List ReceivedGrants, lightsail :GetAlarms, lightsail:GetBu ckets, lightsail:GetCertificates,		

更改	描述	日期
lightsail:GetDisk, lightsail:GetDisks, lightsail:GetInstance, lightsail:GetInstances, lightsail:GetKeyPair, lightsail:GetLoadBalancer, lightsail:GetLoadBalancers, lightsail:GetLoadBalancerTlsCertificates, lightsail:GetStaticIp, lightsail:GetStaticIps, lookoutequipment:DescribeInferenceScheduler, lookoutequipment:ListTagsForResource, lookoutmetrics:DescribeAlert, lookoutmetrics:DescribeAnomalyDetector, lookoutmetrics:ListAlerts, lookoutmetrics:ListAnomalyDetectors, lookoutmetrics:ListMetricSets, lookoutmetrics:ListTagsForResource, lookoutvision:DescribeProject, lookoutvision:ListProjects, managedblockchain:GetMember, managedblockchain:GetNetwork, managedblockchain:GetNode, managedblockchain:ListInvitations, managedblockchain:ListMembers, managedblockchain:ListNodes, mediapackage-vod:DescribePackagingGroup, mediapackage-vod:ListPackagingGroups, mediapackage-vod:ListTagsForResource, mobiletargeting:GetInAppTemplate, mobiletar		

更改	描述	日期
geting:ListTemplates, mq:DescribeBroker, mq:ListBrokers, nimble:GetLaunchProfile, nimble:GetLaunchProfileDetails, nimble:GetStreamingImage, nimble:GetStudio, nimble:GetStudioComponent, nimble:ListLaunchProfiles, nimble:ListStreamingImages, nimble:ListStudioComponents, nimble:ListStudios, profile:GetDomain, profile:GetIntegration, profile:GetProfileObjectType, profile:ListDomains, profile:ListIntegrations, profile:ListProfileObjectTypes, profile:ListTagsForResource, quicksight:DescribeAnalysis, quicksight:DescribeAnalysisPermissions, quicksight:DescribeDataSet, quicksight:DescribeDataSetPermissions, quicksight:DescribeTheme, quicksight:DescribeThemePermissions, quicksight:ListAnalyses, quicksight:ListDataSets, quicksight:ListThemes, resiliencehub:DescribeApp, resiliencehub:DescribeAppVersionTemplate, resiliencehub:DescribeResiliencyPolicy, resiliencehub:ListApps, resiliencehub:ListAppVersionResourceMappings, resiliencehub:ListResiliencyP		

更改	描述	日期
olicies，route53-recovery-readiness:GetCell，route53-recovery-readiness:GetReadinessCheck，route53-recovery-readiness:GetRecoveryGroup，route53-recovery-readiness:GetResourceSet，route53-recovery-readiness:ListCells，route53-recovery-readiness:ListReadinessChecks，route53-recovery-readiness:ListRecoveryGroups，route53-recovery-readiness:ListResourceSets，route53resolver:GetFirewallDomainList，route53resolver:GetFirewallRuleGroup，route53resolver:GetFirewallRuleGroupAssociation，route53resolver:GetResolverQueryLogConfig，route53resolver:ListFirewallDomainLists，route53resolver:ListFirewallDomains，route53resolver:ListFirewallRuleGroupAssociations，route53resolver:ListFirewallRuleGroups，route53resolver:ListFirewallRules，route53resolver:ListResolverQueryLogConfigs, rum:GetAppMonitor，rum:GetAppMonitorData，rum:ListAppMonitors，rum:ListTagsForResource, s3-outposts:GetAccessPoint，s3-outposts:GetAccessPoint		

更改	描述	日期
Policy, s3-outposts:GetBucket, s3-outposts:GetBucketPolicy, s3-outposts:GetBucketTagging, s3-outposts:GetLifecycleConfiguration, s3-outposts:ListAccessPoints, s3-outposts:ListEndpoints, s3-outposts:ListRegionalBuckets, schemas:DescribeDiscoverer, schemas:DescribeRegistry, schemas:DescribeSchema, schemas:ListDiscoverers, schemas:ListRegistries, schemas:ListSchemas, sdb:GetAttributes, sdb:ListDomains, ses:ListEmailTemplates, ses:ListReceiptFilters, ses:ListReceiptRuleSets, ses:ListTemplates, signer:GetSigningProfile, signer:ListProfilePermissions, signer:ListSigningProfiles, synthetics:DescribeCanaries, synthetics:DescribeCanariesLastRun, synthetics:DescribeRuntimeVersions, synthetics:GetCanary, synthetics:GetCanaryRuns, synthetics:ListTagsForResource, timestream:DescribeDatabase, timestream:DescribeTable, timestream:ListDatabases, timestream:ListTables, timestream:ListTagsForResource, transfer:DescribeServer, tr		

更改	描述	日期
ansfer:DescribeUser, transfer:DescribeWorkflow, transfer:ListServers, transfer:ListUsers, transfer:ListWorkflows, voiceid:DescribeDomain, and voiceid:ListTagsForResource		
AWSConfigServiceRolePolicy – 添加 datasync:ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists	此策略现在允许返回中 AWS DataSync 代理人、 DataSync 来源和目标位置以及 DataSync 任务的列表 AWS 账户；列出与中一个或多个指定命名空间关联的 AWS Cloud Map 命名空间和服务的摘要信息 AWS 账户；以及列出中所有可用的 Amazon Simple Email Service (Amazon SES) 联系人列表。AWS 账户	2022 年 8 月 22 日
AWS_ConfigRole – 添加 datasync:ListAgents, datasync:ListLocations, datasync:ListTasks, servicediscovery:ListNamespaces, servicediscovery:ListServices, and ses:ListContactLists	此策略现在允许返回中 AWS DataSync 代理人、 DataSync 来源和目标位置以及 DataSync 任务的列表 AWS 账户；列出与中一个或多个指定命名空间关联的 AWS Cloud Map 命名空间和服务的摘要信息 AWS 账户；以及列出中所有可用的 Amazon Simple Email Service (Amazon SES) 联系人列表。AWS 账户	2022 年 8 月 22 日
ConfigConformsServiceRolePolicy – 添加 cloudwatch:PutMetricData	该政策现在授予向 Amazon 发布指标数据点的权限 CloudWatch。	2022 年 7 月 25 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor:ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocatio	该政策现在支持亚马逊弹性容器服务 (Amazon ECS)、亚马逊、亚马逊、亚马逊、亚马逊 FsX、适用于 A ElastiCache pache Flink 的亚马逊托管服务、亚马逊定位服务、适用于 Apache Kafka 的亚马逊托管流媒体、亚马逊、亚马逊 Rekognition、 QuickSight亚马逊简单存储服务 (Amazon S3) 的额外权限) AWS RoboMaker、亚马逊简单电子邮件服务 (Amazon SES)、、、、、、、、、、、、（IAM 身份中心）、EC2 Image Builder 和 E AWS Amplify lastic Load Balancing。 EventBridge AWS AppConfig AWS AppSync AWS Billing Conductor AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center	2022 年 7 月 15 日

更改	描述	日期
nObjectStorage, datasync:DescribeLocationS3, datasync:DescribeLocationSmb, datasync:DescribeTask, datasync:ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVers		

更改	描述	日期
ions, imagebuilder: ListComponents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

更改	描述	日期
sso:GetInlinePolicyForPermissionSet		

更改	描述	日期
AWS_ConfigRole – 添加 amplifyuibuilder:ExportThemes, amplifyuibuilder:GetTheme, appconfig:GetApplication, appconfig:GetApplication, appconfig:GetConfigurationProfile, appconfig:GetConfigurationProfile, appconfig:GetDeployment, appconfig:GetDeploymentStrategy, appconfig:GetEnvironment, appconfig:GetHostedConfigurationVersion, appconfig:ListTagsForResource, appsync:GetGraphqlApi, appsync:ListGraphqlApis, billingconductor: ListPricingRulesAssociatedToPricingPlan, billingconductor:ListAccountAssociations, billingconductor:ListBillingGroups, billingconductor:ListCustomLineItems, billingconductor:ListPricingPlans, billingconductor:ListPricingRules, billingconductor:ListTagsForResource, datasync:DescribeAgent, datasync:DescribeLocationEfs, datasync:DescribeLocationFsxLustre, datasync:DescribeLocationHdfs, datasync:DescribeLocationNfs, datasync:DescribeLocationObjectStorage, datasync:De	该政策现在支持亚马逊弹性容器服务 (Amazon ECS)、亚马逊、亚马逊、亚马逊、亚马逊 FsX、适用于 A ElastiCache pache Flink 的亚马逊托管服务、亚马逊定位服务、适用于 Apache Kafka 的亚马逊托管流媒体、亚马逊、亚马逊 Rekognition、 QuickSight亚马逊简单存储服务 (Amazon S3) 的额外权限) AWS RoboMaker、亚马逊简单电子邮件服务 (Amazon SES)、、、、、、、、、、、、（IAM 身份中心）、EC2 Image Builder 和 E AWS Amplify lastic Load Balancing。 EventBridge AWS AppConfig AWS AppSync AWS Billing Conductor AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center	2022 年 7 月 15 日

更改	描述	日期
scribeLocationS3, datasync: DescribeLocationSmb, datasync:DescribeTask, datasync: ListTagsForResource, ecr:DescribePullThroughCacheRules, ecr:DescribeRegistry, ecr:GetRegistryPolicy, elasticache:DescribeCacheParameters, elasticloadbalancing:DescribeListenerCertificates, elasticloadbalancing:DescribeTargetGroupAttributes, elasticloadbalancing:DescribeTargetGroups, elasticloadbalancing:DescribeTargetHealth, events:DescribeApiDestination, events:DescribeArchive, fms:GetNotificationChannel, fms:GetPolicy, fms:ListPolicies, fms:ListTagsForResource, fsx:DescribeVolumes, geo:DescribeGeofenceCollection, geo:DescribeMap, geo:DescribePlaceIndex, geo:DescribeRouteCalculator, geo:DescribeTracker, geo:ListTrackerConsumers, glue:BatchGetJobs, glue:BatchGetWorkflows, glue:GetCrawler, glue:GetCrawlers, glue:GetJob, glue:GetJobs, glue:GetWorkflow, imagebuilder: GetComponent, imagebuilder: ListComponentBuildVersions, imagebuilder: ListCompo		

更改	描述	日期
nents, imagebuilder:GetDistributionConfiguration, imagebuilder:GetInfrastructureConfiguration, imagebuilder:ListDistributionConfigurations, imagebuilder:ListInfrastructureConfigurations, kafka:DescribeClusterV2, kafka:ListClustersV2, kinesisanalytics:DescribeApplication, kinesisanalytics:ListTagsForResource, quicksight:DescribeDataSource, quicksight:DescribeDataSourcePermissions, quicksight:ListTagsForResource, rekognition:DescribeStreamProcessor, rekognition:ListTagsForResource, robomaker:DescribeRobotApplication, robomaker:DescribeSimulationApplication, s3:GetStorageLensConfiguration, s3:GetStorageLensConfigurationTagging, servicediscovery:GetInstance, servicediscovery:GetNamespace, servicediscovery:GetService, servicediscovery:ListTagsForResource, ses:DescribeReceiptRule, ses:DescribeReceiptRuleSet, ses:GetContactList, ses:GetEmailTemplate, ses:GetTemplate, and		

更改	描述	日期
sso:GetInlinePolicyForPermissionSet		

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	此政策现在授予以下权限：获取指定的 Amazon Athena 数据目录 AWS 账户、在中列出 Athena 数据目录以及列出与 Athena 工作组或数据目录资源关联的标签；获取 Amazon Detective 行为图列表并列出侦探行为图的标签；获取给定开发终端节点名称列表的资源元数据列表，获取有关指定开发的信息端点，获取所有开发端点，检索 AWS Glue 指定的安全性 AWS Glue AWS Glue AWS 账户 AWS Glue 配置，获取所有 AWS Glue 安全配置，获取与 AWS Glue 资源关联的标签列表，获取有关具有指定名称 AWS Glue 的工作组的信息，检索 AWS 账户中所有 AWS Glue 爬虫资源的名称，获取中所有 AWS Glue `DevEndpoint` 资源的名称，列出中所有 AWS Glue 作业资源的名称 AWS 账户，获取 AWS Glue 成员账户的详细信息，列出账户中创建 AWS Glue 的工作流名称，以及列出账户中可用 AWS Glue 的工作组； AWS 账户检索有关 Amazon GuardDuty 筛选器的详细信息、检索 GuardDuty IPSe GuardDuty ThreatIntel t、检索集合、检索 GuardDuty 成员账户、获取 GuardDuty筛	2022 年 5 月 31 日

更改	描述	日期
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	选器列表、获取 GuardDuty 服务的 IP 集、检索GuardDuty 服务的标签以及获取服务的信息；获取 Amazon Macie 账户的当前状态和配置设置；检索AWS RAM() 资源共享的资源和委托人关联 AWS Resource Access Manager 并检索 AWS RAM 有关资源共享的详细信息； ThreatIntelSets GuardDuty 获取有关亚马逊简单电子邮件服务 (Amazon SES) 现有配置集的信息，获取与 Amazon SES 配置集关联的事件目标列表，并列出与 Amazon SES 账户关联的所有配置集；要获取身份中心目录属性列表，请获取权限集的详细信息，获取附加到指定 IAM 身份中心权限集的 IAM 托管策略，获取，为 IAM 身份中心实例设置的权限，以及为 IAM 身份中心获取标签 AWS IAM Identity Center 资源。	

更改	描述	日期
AWS_ConfigRole – 添加 athena:GetDataCatalog, athena:ListDataCatalogs, athena:ListTagsForResource, detective:ListGraphs, detective:ListTagsForResource, glue:BatchGetDevEndpoints, glue:GetDevEndpoint, glue:GetDevEndpoints, glue:GetSecurityConfiguration, glue:GetSecurityConfigurations, glue:GetTags glue:GetWorkGroup, glue:ListCrawlers, glue:ListDevEndpoints, glue:ListJobs, glue:ListMembers, glue:ListWorkflows, glue:ListWorkGroups, guardduty:GetFilter, guardduty:GetIPSet, guardduty:GetThreatIntelSet, guardduty:GetMembers, guardduty:ListFilters, guardduty:ListIPSets, guardduty:ListTagsForResource, guardduty:ListThreatIntelSets, macie:GetMacieSession, ram:GetResourceShareAssociations, ram:GetResourceShares, ses:GetConfigurationSet, ses:GetConfigurationSetEventDestinations, ses:ListConfigurationSets, sso:DescribeInstanceAccessControlAttributeConfiguration, sso:De	此政策现在授予以下权限：获取指定的 Amazon Athena 数据目录 AWS 账户、在中列出 Athena 数据目录以及列出与 Athena 工作组或数据目录资源关联的标签；获取 Amazon Detective 行为图列表并列出侦探行为图的标签；获取给定开发终端节点名称列表的资源元数据列表，获取有关指定开发的信息端点，获取所有开发端点，检索 AWS Glue 指定的安全性 AWS Glue AWS Glue AWS 账户 AWS Glue 配置，获取所有 AWS Glue 安全配置，获取与 AWS Glue 资源关联的标签列表，获取有关具有指定名称 AWS Glue 的工作组的信息，检索 AWS 账户中所有 AWS Glue 爬虫资源的名称，获取中所有 AWS Glue `DevEndpoint` 资源的名称，列出中所有 AWS Glue 作业资源的名称 AWS 账户，获取 AWS Glue 成员账户的详细信息，列出账户中创建 AWS Glue 的工作流名称，以及列出账户中可用 AWS Glue 的工作组； AWS 账户检索有关 Amazon GuardDuty 筛选器的详细信息、检索 GuardDuty IPSe GuardDuty ThreatIntel t、检索集合、检索 GuardDuty 成员账户、获取 GuardDuty筛	2022 年 5 月 31 日

更改	描述	日期
scribePermissionSet, sso:ListManagedPoliciesInPermissionSet, sso:ListPermissionSets, and sso:ListTagsForResource	选器列表、获取 GuardDuty 服务的 IP 集、检索GuardDuty 服务的标签以及获取服务的信息；获取 Amazon Macie 账户的当前状态和配置设置；检索AWS RAM() 资源共享的资源和委托人关联 AWS Resource Access Manager 并检索 AWS RAM 有关资源共享的详细信息； ThreatIntelSets GuardDuty 获取有关亚马逊简单电子邮件服务 (Amazon SES) 现有配置集的信息，获取与 Amazon SES 配置集关联的事件目标列表，并列出与 Amazon SES 账户关联的所有配置集；要获取身份中心目录属性列表，请获取权限集的详细信息，获取附加到指定 IAM 身份中心权限集的 IAM 托管策略，获取，为 IAM 身份中心实例设置的权限，以及为 IAM 身份中心获取标签 AWS IAM Identity Center 资源。	

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	此策略现在授予以下权限：获取有关所有或指定 AWS CloudTrail 事件数据存储 (EDS) 的信息、获取有关全部或指定 AWS CloudFormation 资源的信息、获取 DynamoDB 加速器 (DAX) 参数组或子网组的列表、获取 AWS Database Migration Service 有关当前正在访问的区域中您的账户的AWS DMS() 复制任务的信息，以及获取指定类型的所有策略的列表。 AWS Organizations	2022 年 4 月 7 日
AWS_ConfigRole – 添加 cloudformation:GetResource, cloudformation:ListResources, cloudtrail:GetEventDataStore, cloudtrail:ListEventDataStores, dax:DescribeParameterGroups, dax:DescribeParameters, dax:DescribeSubnetGroups, DMS:DescribeReplicationTasks, and organizations:ListPolicies	此策略现在授予以下权限：获取有关所有或指定 AWS CloudTrail 事件数据存储 (EDS) 的信息、获取有关全部或指定 AWS CloudFormation 资源的信息、获取 DynamoDB 加速器 (DAX) 参数组或子网组的列表、获取 AWS Database Migration Service 有关当前正在访问的区域中您的账户的AWS DMS() 复制任务的信息，以及获取指定类型的所有策略的列表。 AWS Organizations	2022 年 4 月 7 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 backup-gateway:ListTagsForResource, backup-gateway:ListVirtualMachines, batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags, dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings, ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions, ec2:DescribeFleets, ec2:DescribeNetworkAcls, ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests, ec2:DescribeVolumeAttribute, ec2:DescribeVolumes, eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource, guardduty:ListOrganizationAdminAccounts, kms:ListAliases, opsworks:DescribeLayers, opsworks:DescribeStacks, opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterPara	该策略现在支持、、DynamoDB 加速器 AWS Backup AWS Batch、亚马逊 DynamoDB、 AWS Database Migration Service亚马逊弹性计算云 (Amazon EC2)、亚马逊 Elastic Kubernetes Service、亚马逊 FSx、亚马逊、、、、、亚马逊关系数据库服务、V2 和亚马逊的额外权限。 GuardDuty AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces	2022 年 3 月 14 日

更改	描述	日期
meters, states:DescribeActivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		

更改	描述	日期
AWS_ConfigRole – 添加 backup-gateway:ListTagsForResource，backup-gateway:ListVirtualMachines，batch:DescribeComputeEnvironments, batch:DescribeJobQueues, batch:ListTagsForResource, dax:ListTags，dms:DescribeCertificates, dynamodb:DescribeGlobalTable, dynamodb:DescribeGlobalTableSettings，ec2:DescribeClientVpnAuthorizationRules, ec2:DescribeClientVpnEndpoints, ec2:DescribeDhcpOptions，ec2:DescribeFleets, ec2:DescribeNetworkAcls，ec2:DescribePlacementGroups, ec2:DescribeSpotFleetRequests，ec2:DescribeVolumeAttribute, ec2:DescribeVolumes，eks:DescribeFargateProfile, eks:ListFargateProfiles, eks:ListTagsForResource, fsx:ListTagsForResource，guardduty:ListOrganizationAdminAccounts, kms:ListAliases，opsworks:DescribeLayers, opsworks:DescribeStacks，opsworks:ListTags, rds:DescribeDBClusterParameterGroups, rds:DescribeDBClusterParameters, states:DescribeAct	该策略现在支持、、DynamoDB 加速器 AWS Backup AWS Batch、亚马逊 DynamoDB、 AWS Database Migration Service亚马逊弹性计算云 (Amazon EC2)、亚马逊 Elastic Kubernetes Service、亚马逊 FSx、亚马逊、、、、、亚马逊关系数据库服务、V2 和亚马逊的额外权限。 GuardDuty AWS Key Management Service AWS OpsWorks AWS WAF WorkSpaces	2022 年 3 月 14 日

更改	描述	日期
ivity, states:ListActivities, wafv2:GetRuleGroup, wafv2:ListRuleGroups, wafv2:ListTagsForResource, workspaces:DescribeConnectionAliases, workspaces:DescribeTags, and workspaces:DescribeWorkspaces		
AWSConfigServiceRolePolicy – 添加 elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	现在，该策略允许获取有关 Elastic Beanstalk 环境的详细信息以及指定 Elastic Beanstalk 配置集的设置描述、获取或 Elasticsearch 版本的地图、描述数据库 OpenSearch 的可用的 Amazon RDS 选项组以及获取有关部署配置的信息。 CodeDeploy 现在，该策略还授予以下权限：检索附加到的指定备用联系人 AWS 账户、检索有关 AWS Organizations 策略的信息、检索 Amazon ECR 存储库策略、检索有关存档 AWS Config 规则的信息、检索 Amazon ECS 任务定义系列列表、列出指定子 OU 或账户的根或上级组织单位 (OU)，以及列出附加到指定目标根目录、组织单位或账户的策略。	2022 年 2 月 10 日

更改	描述	日期
AWS_ConfigRole – 添加 elasticbeanstalk:DescribeEnvironments, elasticbeanstalk:DescribeConfigurationSettings, account:GetAlternateContact, organizations:DescribePolicy, organizations:ListParents, organizations:ListPoliciesForTarget, es:GetCompatibleElasticsearchVersions, rds:DescribeOptionGroups, rds:DescribeOptionGroups, es:GetCompatibleVersions, codedeploy:GetDeploymentConfig, ecr-public:GetRepositoryPolicy, access-analyzer:GetArchiveRule, and ecs:ListTaskDefinitionFamilies	现在，该策略允许获取有关 Elastic Beanstalk 环境的详细信息以及指定 Elastic Beanstalk 配置集的设置描述、获取或 Elasticsearch 版本的地图、描述数据库 OpenSearch 的可用的 Amazon RDS 选项组以及获取有关部署配置的信息。 CodeDeploy 现在，该策略还授予以下权限：检索附加到的指定备用联系人 AWS 账户、检索有关 AWS Organizations 策略的信息、检索 Amazon ECR 存储库策略、检索有关存档 AWS Config 规则的信息、检索 Amazon ECS 任务定义系列列表、列出指定子 OU 或账户的根或上级组织单位 (OU)，以及列出附加到指定目标根目录、组织单位或账户的策略。	2022 年 2 月 10 日
AWSConfigServiceRolePolicy – 添加 logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	此策略现在授予创建 Amazon CloudWatch 日志组和流以及向已创建的日志流写入日志的权限。	2021 年 12 月 15 日
AWS_ConfigRole – 添加 logs:CreateLogStream, logs:CreateLogGroup, and logs:PutLogEvent	此策略现在授予创建 Amazon CloudWatch 日志组和流以及向已创建的日志流写入日志的权限。	2021 年 12 月 15 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	该策略现在授予获取有关亚马逊 OpenSearch 服务（OpenSearch 服务）域/域的详细信息以及获取特定亚马逊关系数据库服务 (Amazon RDS) 数据库参数组的详细参数列表的权限。该政策还允许获取有关 Ama ElastiCache zon 快照的详细信息。	2021 年 9 月 8 日
AWS_ConfigRole – 添加 es:DescribeDomain, es:DescribeDomains, rds:DescribeDBParameters, and, elasticache:DescribeSnapshots	该策略现在授予获取有关亚马逊 OpenSearch 服务（OpenSearch 服务）域/域的详细信息以及获取特定亚马逊关系数据库服务 (Amazon RDS) 数据库参数组的详细参数列表的权限。该政策还允许获取有关 Ama ElastiCache zon 快照的详细信息。	2021 年 9 月 8 日

更改	描述	日期
AWSConfigServiceRolePolicy— 添加logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine AWS 资源类型以及其他权限	此策略现在授予列出日志组的标签，列出状态机的标签，以及列出所有状态机的权限。此策略现在授予获取有关状态机的详细信息的权限。该政策现在还支持亚马逊 EC2 Systems Manager (SSM)、亚马逊弹性容器注册表、亚马逊 FSx、Amazon Data Firehose、适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK）、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Route 53、亚马逊、SageMaker亚马逊简单通知服务、、和。 AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	2021 年 7 月 28 日

更改	描述	日期
AWS_ConfigRole— 添加 logs:ListTagsLogGroup, states:ListTagsForResource, states:ListStateMachines, states:DescribeStateMachine，以及 AWS 资源类型的其他权限	此策略现在授予列出日志组的标签，列出状态机的标签，以及列出所有状态机的权限。此策略现在授予获取有关状态机的详细信息的权限。该政策现在还支持亚马逊 EC2 Systems Manager (SSM)、亚马逊弹性容器注册表、亚马逊 FSx、Amazon Data Firehose、适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK）、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Route 53、亚马逊、SageMaker亚马逊简单通知服务、、和。 AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway	2021 年 7 月 28 日

更改	描述	日期
AWSConfigServiceRolePolicy— 为 AWS 资源类型添加ssm:DescribeDocumentPermission权限和其他权限	此策略现在授予查看有关 IAM Access Analyzer 的 AWS Systems Manager 文档和信息的权限。该政策现在支持亚马逊 Kinesis、亚马逊、亚马逊 EMR、 ElastiCache亚马逊 Route 53 和 AWS Network Firewall亚马逊关系数据库服务 (Amazon RDS) 的其他 AWS 资源类型。这些权限更改 AWS Config 允许调用支持这些资源类型所需的只读 API。该策略现在还支持筛选 Lambda - inside-vpc 托管规则的 Lambda AWS Config @Edge 函数。	2021 年 6 月 8 日
AWS_ConfigRole— 为 AWS 资源类型添加ssm:DescribeDocumentPermission权限和其他权限	此策略现在授予查看有关 IAM Access Analyzer 的 AWS Systems Manager 文档和信息的权限。该政策现在支持亚马逊 Kinesis、亚马逊、亚马逊 EMR、 ElastiCache亚马逊 Route 53 和 AWS Network Firewall亚马逊关系数据库服务 (Amazon RDS) 的其他 AWS 资源类型。这些权限更改 AWS Config 允许调用支持这些资源类型所需的只读 API。该策略现在还支持筛选 Lambda - inside-vpc 托管规则的 Lambda AWS Config @Edge 函数。	2021 年 6 月 8 日

更改	描述	日期
AWSConfigServiceRolePolicy – 添加 apigateway:GET 权限，以对 API Gateway 进行只读 GET 调用，添加 s3:GetAccessPointPolicy 权限和 s3:GetAccessPointPolicyStatus 权限，以调用 Amazon S3 只读 API	现在，此策略授予 AWS Config 允许对 API Gateway 进行只读 GET 调用的权限，以支持 API 网关的 AWS Config 规则。该策略还增加了 AWS Config 允许调用亚马逊简单存储服务 (Amazon S3) 只读 API 的权限，这是支持`AWS::S3::AccessPoint` 新资源类型所必需的。	2021 年 5 月 10 日
AWS_ConfigRole — 添加apigateway:GET对 API Gateway 进行只读 GET 调用的s3:GetAccessPointPolicy权限以及调用 Amazon S3 只读 API 的s3:GetAccessPointPolicyStatus权限和权限	现在，此策略授予的权限 AWS Config 允许对 API Gateway 进行只读 GET 调用， AWS Config 以支持 API 网关。该策略还增加了 AWS Config 允许调用亚马逊简单存储服务 (Amazon S3) 只读 API 的权限，这是支持`AWS::S3::AccessPoint` 新资源类型所必需的。	2021 年 5 月 10 日

更改	描述	日期
AWSConfigServiceRolePolicy— 为 AWS 资源类型添加ssm:ListDocuments权限和其他权限	此策略现在授予查看有关 AWS Systems Manager 指定文档信息的权限 该政策现在还支持亚马逊弹性文件系统 AWS Backup、亚马逊、亚马逊简单存储服务 (Amazon S3) ElastiCache、亚马逊弹性计算云 (Amazon EC2)、Amazon Kinesis、亚马逊和亚马逊 Route 53 的其他 AWS 资源类型。 SageMaker AWS Database Migration Service这些权限更改 AWS Config 允许调用支持这些资源类型所需的只读 API。	2021 年 4 月 1 日
AWS_ConfigRole— 为 AWS 资源类型添加ssm:ListDocuments权限和其他权限	此策略现在授予查看有关 AWS Systems Manager 指定文档信息的权限 该政策现在还支持亚马逊弹性文件系统 AWS Backup、亚马逊、亚马逊简单存储服务 (Amazon S3) ElastiCache、亚马逊弹性计算云 (Amazon EC2)、Amazon Kinesis、亚马逊和亚马逊 Route 53 的其他 AWS 资源类型。 SageMaker AWS Database Migration Service这些权限更改 AWS Config 允许调用支持这些资源类型所需的只读 API。	2021 年 4 月 1 日
`AWSConfigRole` 已弃用	`AWSConfigRole` 已弃用。替换策略是 `AWS_ConfigRole` 。	2021 年 4 月 1 日

更改	描述	日期
AWS Config 开始跟踪更改	AWS Config 开始跟踪其 AWS 托管策略的更改。	2021 年 4 月 1 日

分配给的 IAM 角色的权限 AWS Config

IAM 角色允许您定义一组权限。 AWS Config 担任您分配给它的角色来写入您的 S3 存储桶、发布到您的 SNS 主题以及发出`Describe`或 `List` API 请求以获取 AWS 资源的配置详细信息。有关 IAM 角色的更多信息，请参阅《IAM 用户指南》中的 IAM 角色。

当您使用 AWS Config 控制台创建或更新 IAM 角色时， AWS Config 会自动为您附加所需的权限。有关更多信息，请参阅 使用控制 AWS Config 台进行设置。

目录

- 创建 IAM 角色策略
  - 将 IAM 信任策略添加到您的角色
  - 用于 S3 存储桶的 IAM 角色策略
  - KMS 密钥的 IAM 角色策略
  - 用于 Amazon SNS 主题的 IAM 角色策略
  - 用于获取配置详细信息的 IAM 角色策略
- 管理 S3 存储桶记录的权限

创建 IAM 角色策略

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

如果您使用 AWS CLI 进行设置 AWS Config 或更新现有 IAM 角色，则必须手动更新策略以允许 AWS Config 访问您的 S3 存储桶、发布到您的 SNS 主题并获取有关您的资源的配置详细信息。

将 IAM 信任策略添加到您的角色

您可以创建一个 IAM 信任策略，该策略 AWS Config 允许代入角色并使用它来跟踪您的资源。有关信任策略的更多信息，请参阅《IAM 用户指南》中的角色术语和概念。

以下是 AWS Config 角色的信任策略示例：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

您可以使用上述 IAM 角色信任关系中的 `AWS:SourceAccount` 条件来限制 Config 服务主体，仅在代表特定账户执行操作时与 AWS IAM 角色进行交互。

AWS Config 还支持这样的`AWS:SourceArn`条件，即限制 Config 服务委托人只能在代表拥有账户执行操作时担任 IAM 角色。使用 AWS Config 服务主体时，该`AWS:SourceArn`属性将始终设置`sourceRegion`为`arn:aws:config:sourceRegion:sourceAccountID:*`配置记录器的区域`sourceAccountID`，以及包含配置记录器的帐户的 ID。有关 AWS Config 配置记录器的更多信息，请参阅管理配置记录器。例如，添加以下条件限制 Config 服务主体只能代表账户 `123456789012` 中 `us-east-1` 区域中的配置记录器代入 IAM 角色：`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`。

用于 S3 存储桶的 IAM 角色策略

以下示例策略授予访问您的 S3 存储桶的 AWS Config 权限：

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

```
      ],
      "Resource":[
        "arn:aws:s3:::myBucketName/prefix/AWSLogs/myAccountID/*"
      ],
      "Condition":{
        "StringLike":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:GetBucketAcl"
      ],
      "Resource":"arn:aws:s3:::myBucketName"
    }
  ]
}
```

KMS 密钥的 IAM 角色策略

以下示例策略授予对新对象使用基于 KMS 的加密以进行 S3 存储桶交付的 AWS Config 权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN"
        }
    ]
}
```

用于 Amazon SNS 主题的 IAM 角色策略

以下示例策略授予访问您的 SNS 主题的 AWS Config 权限：

```
{
```

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

如果您的 SNS 主题已加密，要了解更多设置说明，请参阅《Amazon Simple Notification Service 开发人员指南》中的配置 AWS KMS 权限。

用于获取配置详细信息的 IAM 角色策略

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

使用 AWS 托管策略 AWS_ConfigRole 并将其附加到您分配的 IAM 角色。 AWS Config AWS 每次 AWS Config 添加对 AWS 资源类型的支持时都会更新此策略，这意味着只要角色附加了此托管策略，它 AWS Config 就会继续拥有获取配置详细信息所需的权限。

如果您使用控制台创建或更新角色，请为您 AWS Config 附加 AWS_ConfigRole。

如果您使用 AWS CLI，请使用**attach-role-policy**命令并指定 AWS_ConfigRole 的 Amazon 资源名称 (ARN)：

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

管理 S3 存储桶记录的权限

AWS Config 在创建、更新或删除 S3 存储桶时记录和发送通知。

建议您通过 `AWS_ConfigRole` 托管策略使用 `AWSServiceRoleForConfig`（请参阅对 AWS Config 使用服务相关角色）或自定义 IAM 角色。有关配置记录的最佳实践的更多信息，请参阅 AWS Config 最佳实践。

如果您需要管理存储桶记录的对象级权限，请确保在 S3 存储桶策略中提供`config.amazonaws.com`（ AWS Config 服务主体名称）对`AWS_ConfigRole`托管策略中所有 S3 相关权限的访问权限。有关更多信息，请参阅 Amazon S3 存储桶的权限。

更新分配给的 IAM 角色 AWS Config

您可以 AWS Config 随时更新担任的 IAM 角色。在更新 IAM 角色之前，请确保您已经创建了一个新的角色来取代旧角色。您必须将策略附加到新角色，以 AWS Config 授予记录配置并将其传送到您的交付渠道的权限。此外，请确保复制您的新 IAM 角色的 Amazon 资源名称 (ARN)。您在更新 IAM 角色时需要使用该名称。有关创建 IAM 角色并将所需策略附加到 IAM 角色的信息，请参阅创建 IAM 角色。

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

更新 IAM 角色

您可以使用 AWS Management Console 或更新您的 IAM 角色 AWS CLI。

To update the IAM role (Console)

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

1. 登录 AWS Management Console 并打开 AWS Config 控制台，网址为 https://console.aws.amazon.com/config/。
2. 在导航窗格中，选择设置。
3. 在 “设置” 页面上选择 “编辑”。
4. 在数据治理部分中，为 AWS Config以下角色选择 IAM 角色：
   - 使用现有的 AWS Config 服务相关角色- AWS Config 创建具有所需权限的角色。
   - 从您的账户中选择一个角色-对于现有角色，请在您的账户中选择一个 IAM 角色。
5. 选择保存。

To update the IAM role (AWS CLI)

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

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

AWS Config 传送渠道的 Amazon S3 存储桶的权限

> **Important**
>
> 本页介绍的是为 AWS Config 配送渠道设置 Amazon S3 存储桶。此页面与 AWS Config 配置记录器可以记录的`AWS::S3::Bucket`资源类型无关。有关 AWS Config 配送渠道的更多信息，请参阅管理交付渠道。

默认情况下，所有 Amazon S3 存储桶和对象都是私有的。只有创建存储桶的 AWS 账户 资源所有者才能访问该存储桶。但是，资源所有者可以选择将访问权限授予其他资源和用户。要授予访问权限，其中一种方法是编写访问策略。

如果自动为您 AWS Config 创建 Amazon S3 存储桶（例如，如果您使用 AWS Config 控制台设置交付渠道），则这些权限将自动添加到 Amazon S3 存储桶。但是，如果您指定现有 Amazon S3 存储桶，则您必须确保该 S3 存储桶具有相应权限。

> **Note**
>
> 对象不继承其存储桶的权限。例如，如果您创建了一个存储桶并授予一个用户写入权限，则将无法访问此用户的对象，除非此用户显式授予您访问权限。

目录

- 使用 IAM 角色时 Amazon S3 存储桶的必需权限
- 使用服务相关角色时 Amazon S3 Bucket 存储桶的必需权限
- 授予 AWS Config 对 Amazon S3 存储桶的访问权限

使用 IAM 角色时 Amazon S3 存储桶的必需权限

AWS Config 将配置信息（历史文件和快照）发送到您账户中的 Amazon S3 存储桶时，它将使用您在设置时分配的 IAM 角色 AWS Config。当 AWS Config 向其他账户中的 Amazon S3 存储桶发送配置信

息时，它会首先尝试使用 IAM 角色，但如果该存储桶的访问策略未向此 IAM 角色授予 `WRITE` 访问权限，那么此次尝试将会失败。在这种情况下，再次 AWS Config 发送信息，这次是作为 AWS Config 服务主体发送。在成功交付之前，访问策略必须授予对`config.amazonaws.com`主体名称的`WRITE`访问权限。 AWS Config 然后是它传送到 S3 存储桶的对象的所有者。您必须将下面第 6 步中提到的一个访问策略附加到另一账户中的 S3 存储桶，以向 AWS Config 授予访问 Amazon S3 存储桶的权限。

在 AWS Config 可以将日志传送到您的 Amazon S3 存储桶之前，请 AWS Config 检查该存储桶是否存在以及该存储桶位于哪个 AWS 区域。 AWS Config 尝试调用 Amazon S3 HeadBucketAPI 来检查存储桶是否存在并获取存储桶区域。如果在执行位置检查时未提供定位存储桶的权限，则会在 AWS CloudTrail 日志中看到`AccessDenied`错误。不过，如果您未提供存储桶定位权限，日志会成功传输到您的 Amazon S3 存储桶。

> **Note**
>
> 要允许 Amazon S3 `HeadBucket` API 的权限，请按照以下第 6 步所述提供以 Sid `AWSConfigBucketExistenceCheck` 身份执行 `s3:ListBucket` 操作的权限。

使用服务相关角色时 Amazon S3 Bucket 存储桶的必需权限

AWS Config 服务相关角色无权将对象放入 Amazon S3 存储桶。因此，如果您 AWS Config 使用服务相关角色进行设置，则会改为 AWS Config 将配置项目作为 AWS Config 服务主体发送。您需要将下文步骤 6 中提及的访问策略附加到您自己的账户或其他账户中的 Amazon S3 存储桶，才能授予对 Amazon S3 存储桶的 AWS Config 访问权限。

授予 AWS Config 对 Amazon S3 存储桶的访问权限

按照以下步骤向您自己的账户或其他账户中的 Amazon S3 存储桶添加访问策略。访问策略 AWS Config 允许向 Amazon S3 存储桶发送配置信息。

1. AWS Management Console 使用拥有 S3 存储桶的账户登录。
2. 打开 Amazon S3 控制台，网址为：https://console.aws.amazon.com/s3/。
3. 选择 AWS Config 要用于传送配置项目的存储桶，然后选择 Propert ie s。
4. 选择权限。
5. 选择 Edit Bucket Policy。
6. 将以下策略复制到 Bucket Policy Editor 窗口中：

> **Important**
>
> 作为允许 AWS Config 访问 Amazon S3 存储桶时的最佳安全实践，我们强烈建议您在存储桶策略中使用`AWS:SourceAccount`条件来限制访问权限。如果现有的存储桶策略未遵循此最佳安全实践，强烈建议您编辑该存储桶策略以纳入此保护。这样可以确保 AWS Config 仅代表预期用户授予访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSConfigBucketPermissionsCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketExistenceCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::targetBucketName",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    },
    {
      "Sid": "AWSConfigBucketDelivery",
```

```
      "Effect": "Allow",
      "Principal": {
        "Service": "config.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::targetBucketName/[optional] prefix/
AWSLogs/sourceAccountID/Config/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "AWS:SourceAccount": "sourceAccountID"
        }
      }
    }
  ]
}
```

> **Note**
>
> 向您的 IAM 角色而不是 AWS Config 服务委托人名称 (SPN) 授予权限时，请确保您的 IAM 角色拥有跨账户存储桶的`PutObjectACL`权限，以免出现权限不足错误。请参阅位于用于 S3 存储桶的 IAM 角色策略的 IAM 角色策略示例。

7. 替换存储桶策略中的以下值：
   - *## BucketName* — AWS Config 将向其传送配置项目的 Amazon S3 存储桶的名称。
   - *[##] prefix* – Amazon S3 对象键的可选附加内容，可帮助在存储桶中创建类似文件夹的组织结构。
   - *SourceAccountId* — AWS Config 将向目标存储桶传送配置项目的账户的 ID。
8. 选择 Save，然后选择 Close。

您可以使用上述 Amazon S3 存储桶策略中的 `AWS:SourceAccount` 条件来限制 Config 服务主体，仅在代表特定账户执行操作时与 Amazon S3 存储桶进行交互。如果您计划在同一组织的多个账户 AWS Config 中设置配置项目以将配置项目传送到单个 Amazon S3 存储桶，我们建议您使用 IAM 角色代替服务相关角色，以便您可以使用 AWS Organizations 条件密钥，例如`AWS:PrincipalOrgID`。有关管理要与使用的 IAM 角色的访问权限的更多信息 AWS Config，请参阅分配给的 IAM 角色的权限 AWS Config。有关管理访问权限的更多信息 AWS Organizations，请参阅管理 AWS 组织的访问权限。

AWS Config 还支持这样的`AWS:SourceArn`条件，即限制 Config 服务委托人仅在代表特定 AWS Config 交付渠道执行操作时与 Amazon S3 存储桶进行交互。使用 AWS Config 服务主体时，该`AWS:SourceArn`属性将始终设置为交付渠道`arn:aws:config:sourceRegion:sourceAccountID:*`所在`sourceRegion`区域，并且`sourceAccountID`是包含配送渠道的账户的 ID。有关 AWS Config 配送渠道的更多信息，请参阅管理交付渠道。例如，添加以下条件以限制 Config 服务主体仅代表账户 `123456789012` 中 `us-east-1` 区域中的传输通道与您的 Amazon S3 存储桶进行交互：`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`。

AWS Config 交付渠道 KMS 密钥的权限

如果您想为 S3 存储桶的 AWS KMS 密钥创建策略，允许您对由 AWS Config S3 存储桶交付的对象使用基于 KMS 的加密，请使用本主题中的信息。

目录

- 使用 IAM 角色（S3 存储桶传输）时 KMS 密钥的必需权限
- 使用服务相关角色时 AWS KMS 密钥所需的权限（S3 存储桶交付）
- 授予对 AWS KMS 密钥的 AWS Config 访问权限

使用 IAM 角色（S3 存储桶传输）时 KMS 密钥的必需权限

如果您 AWS Config 使用 IAM 角色进行设置，则可以将以下权限策略附加到 KMS 密钥：

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Effect": "Allow",
            "Resource": "*myKMSKeyARN*",
            "Principal": {
                "AWS": [
                    "account-id1",
                    "account-id2",
```

```
                    "account-id3"
                ]
            }
        }
    ]
}
```

> **Note**
>
> 如果 IAM 角色、Amazon S3 存储桶策略或 AWS KMS 密钥未提供对 AWS Config的适当访问权限 AWS Config，则尝试向 Amazon S3 存储桶发送配置信息将失败。在这种情况下，再次 AWS Config 发送信息，这次是作为 AWS Config 服务主体发送。在这种情况下，您必须将下文提到的权限策略附加到 AWS KMS 密钥，以授予在向 Amazon S3 存储桶传送信息时使用该密钥的 AWS Config 权限。

使用服务相关角色时 AWS KMS 密钥所需的权限（S3 存储桶交付）

AWS Config 服务相关角色无权访问 AWS KMS 密钥。因此，如果您 AWS Config 使用服务相关角色进行设置，则 AWS Config 将改为以 AWS Config 服务主体身份发送信息。您需要在 AWS KMS 密钥上附加访问策略（如下所述），以授予在向 Amazon S3 存储桶传送信息时使用该 AWS KMS 密钥的 AWS Config 权限。

授予对 AWS KMS 密钥的 AWS Config 访问权限

此策略 AWS Config 允许在向 Amazon S3 存储桶传送信息时使用 AWS KMS 密钥

```
{
    "Id": "Policy_ID",
    "Statement": [
        {
            "Sid": "AWSConfigKMSPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "myKMSKeyARN",
```

```
            "Condition": {
                "StringEquals": {
                    "AWS:SourceAccount": "sourceAccountID"
                }
            }
        }
    ]
}
```

替换密钥策略中的以下值：

- *mykmsKeyarn* — 用于加密将向其传送配置项目 AWS KMS 的 Amazon S3 存储桶 AWS Config 中数据的密钥的 ARN。
- *sourceAccountID* – AWS Config 将向其传送配置项的账户的 ID。

您可以使用上述 AWS KMS 密钥策略中的`AWS:SourceAccount`条件来限制 Config 服务主体仅在代表特定账户执行操作时与 AWS KMS 密钥交互。

AWS Config 还支持这样的`AWS:SourceArn`条件，即限制 Config 服务委托人仅在代表特定 AWS Config 交付渠道执行操作时与 Amazon S3 存储桶进行交互。使用 AWS Config 服务主体时，该`AWS:SourceArn`属性将始终设置为交付渠道`arn:aws:config:sourceRegion:sourceAccountID:*`所在`sourceRegion`区域，并且`sourceAccountID`是包含配送渠道的账户的 ID。有关 AWS Config 配送渠道的更多信息，请参阅管理交付渠道。例如，添加以下条件以限制 Config 服务主体仅代表账户 `123456789012` 中 `us-east-1` 区域中的传输通道与您的 Amazon S3 存储桶进行交互：`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`。

Amazon SNS 主题的权限

本主题介绍如何配置 AWS Config 以交付由其他账户拥有的 Amazon SNS 主题。 AWS Config 必须具有向 Amazon SNS 主题发送通知所需的权限。对于同账户设置，当 AWS Config 控制台创建 Amazon SNS 主题或您从自己的账户中选择一个 Amazon SNS 主题时 AWS Config ，请确保 Amazon SNS 主题包含所需的权限并遵循安全最佳实践。

> **Note**
>
> AWS Config 目前仅支持在同一地区和跨账户进行访问。用于补救 AWS Systems Manager (SSM) 文档或录音机交付渠道的 SNS 主题不能跨区域。

目录

- 使用 IAM 角色时 Amazon SNS 主题的必需权限
- 使用服务相关角色时 Amazon SNS 主题的必需权限
- 授予 AWS Config 对 Amazon SNS 主题的访问权限。
- Amazon SNS 主题故障排除

使用 IAM 角色时 Amazon SNS 主题的必需权限

您可以将权限策略附加到不同账户拥有的 Amazon SNS 主题。如果要使用另一个账户中的 Amazon SNS 主题，请确保将以下策略附加到现有 Amazon SNS 主题。

```
{
  "Id": "Policy_ID",
  "Statement": [
    {
      "Sid": "AWSConfigSNSPolicy",
      "Action": [
        "sns:Publish"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
      "Principal": {
        "AWS": [
          "account-id1",
          "account-id2",
          "account-id3"
        ]
      }
    }
  ]
}
```

对于 `Resource` 键，*`account-id`* 为主题所有者的 AWS 账号。对于*`## id1### id 2 ### id 3# ###### AWS ## ### A mazon SNS ##`*的。您可以用适当的值替换 *`region`* 和 *`myTopic`*。

向 Amazon SNS 主题 AWS Config 发送通知时，它会首先尝试使用 IAM 角色，但是如果该角色或 AWS 账户 没有向该主题发布的权限，则尝试会失败。在这种情况下，将再次 AWS Config 发送通知，这次是以 AWS Config 服务主体名称 (SPN) 的形式发送。发布成功之前，主题的访问策略必须授予 `sns:Publish` 对 `config.amazonaws.com` 主体名称的访问权限。如果 IAM 角色无权向 Amazon

SNS 主题发布内容，则必须按下一节中所述，在 Amazon SNS 主题中附加访问策略，以授予 AWS Config 访问该主题的权限。

使用服务相关角色时 Amazon SNS 主题的必需权限

AWS Config 服务相关角色无权访问 Amazon SNS 主题。因此，如果您 AWS Config 使用服务相关角色 (SLR) 进行设置，则 AWS Config 将改为以 AWS Config 服务主体身份发送信息。您需要在 Amazon SNS 主题中附加访问策略（如下所述），才能授予向亚马逊 SNS 主题发送信息的 AWS Config 权限。

对于同账户设置，当 Amazon SNS 主题和 SLR 位于同一账户中，并且 Amazon SNS 策略授予 SLR“`sns:Publish`”权限时，您无需使用 AWS Config SPN。以下权限策略和安全最佳实践建议适用于跨账户设置。

授予 AWS Config 对 Amazon SNS 主题的访问权限。

此政策 AWS Config 允许向 Amazon SNS 主题发送通知。要授予从其他账户 AWS Config 访问 Amazon SNS 主题的权限，您需要附加以下权限策略。

> **Note**
>
> 作为安全最佳实践，强烈建议通过限制对`AWS:SourceAccount`条件中列出的账户的访问来确保 AWS Config 仅代表预期用户访问资源。

```
{
"Id": "Policy_ID",
"Statement": [
  {
    "Sid": "AWSConfigSNSPolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "config.amazonaws.com"
    },
    "Action": "sns:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic",
        "Condition" : {
        "StringEquals": {
          "AWS:SourceAccount": [
            "account-id1",
            "account-id2",
```

```
            "account-id3"
          ]
        }
      }
    }
  ]
}
```

对于 `Resource` 键，*`account-id`* 为主题所有者的 AWS 账号。对于*`## id1### id 2 ### id 3# ###### AWS ## ### A mazon SNS ##`*的。您可以用适当的值替换 *`region`* 和 *`myTopic`*。

在代表特定账户执行操作时，您可以使用之前的 Amazon SNS 主题政策中的`AWS:SourceAccount`条件来限制 AWS Config 服务主体名称 (SPN) 只能与 Amazon SNS 主题进行交互。

AWS Config 还支持将 AWS Config 服务主体名称 (SPN) 限制为仅在代表特定 AWS Config 交付渠道执行操作时与 S3 存储桶交互的`AWS:SourceArn`条件。使用 AWS Config 服务主体名称 (SPN) 时，该`AWS:SourceArn`属性将始终设置为交付渠道的区域`arn:aws:config:sourceRegion:sourceAccountID:*`在哪里`sourceRegion`，并且`sourceAccountID`是包含配送渠道的账户的 ID。有关 AWS Config 交付渠道的更多信息，请参阅管理交付渠道。例如，添加以下条件以限制 AWS Config 服务主体名称 (SPN) 仅代表账户中`us-east-1`该区域的交付渠道与您的 S3 存储桶进行交互`123456789012`：`"ArnLike": {"AWS:SourceArn": "arn:aws:config:us-east-1:123456789012:*"}`。

Amazon SNS 主题故障排除

AWS Config 必须拥有向 Amazon SNS 主题发送通知的权限。如果 Amazon SNS 主题无法收到通知，请验证所担任 AWS Config 的 IAM 角色是否具有所需的`sns:Publish`权限。

对 AWS Config 身份和访问进行故障排除

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

主题

- 我无权在以下位置执行操作 AWS Config
- 我无权执行 iam：PassRole
- 我想允许我以外的人 AWS 账户 访问我的 AWS Config 资源

我无权在以下位置执行操作 AWS Config

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

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

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

在此情况下，Mateo 的策略必须更新以允许其使用 `config:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 AWS Config。

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

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

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

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

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 AWS Config 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解是否 AWS Config 支持这些功能，请参阅如何 AWS Config 与 IAM 配合使用。

- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过联合身份验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅 IA M 用户指南中的跨账户资源访问。

将服务相关角色用于 AWS Config

AWS Config 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的 IAM 角色的独特类型。 AWS Config服务相关角色由服务预定义 AWS Config ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置变得 AWS Config 更加容易，因为您不必手动添加必要的权限。 AWS Config 定义其服务相关角色的权限，除非另有定义，否则 AWS Config 只能担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 IAM 实体。

有关支持服务相关角色的其它服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务相关角色文档。

的服务相关角色权限 AWS Config

AWS Config 使用名为的服务相关角色 AWSServiceRoleForConfig— AWS Config 使用此服务相关角色代表您调用其他 AWS 服务。

AWSServiceRoleForConfig服务相关角色信任`config.amazonaws.com`服务来代替该角色。

该`AWSServiceRoleForConfig`角色的权限策略包含 AWS Config 资源的只读和只写权限，以及其他支持的服务中资源的只读权限。 AWS Config 要查看托管策略 AWSServiceRoleForConfig，请参阅AWS 托管策略 AWS Config。有关更多信息，请参阅 支持的资源类型。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

要将服务相关角色与配合使用 AWS Config，您必须在 Amazon S3 存储桶和 Amazon SNS 主题上配置权限。有关更多信息，请参阅 使用服务相关角色时 Amazon S3 Bucket 存储桶的必需权限、使用服务

相关角色时 AWS KMS 密钥所需的权限（S3 存储桶交付） 和 使用服务相关角色时 Amazon SNS 主题的必需权限。

为创建服务相关角色 AWS Config

在 IAM CLI 或 IAM API 中，用 `config.amazonaws.com` 服务名称创建一个服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。如果您删除了此服务相关角色，可以使用同样的过程再次创建角色。

编辑的服务相关角色 AWS Config

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

删除的服务相关角色 AWS Config

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

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

删除使用的 AWS Config 资源 AWSServiceRoleForConfig

确保您没有使用服务相关角色的 `ConfigurationRecorders`。您可以使用 AWS Config 控制台停止配置记录器。要停止记录，请选择 Recording is on (记录已打开) 下的 Turn off (关闭)。

您可以删除`ConfigurationRecorder`使用的 AWS Config API。要删除，请使用 `delete-configuration-recorder` 命令。

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

使用 IAM 手动删除服务相关角色

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

中的事件响应 AWS Config

AWS非常重视安全性。作为 AWS 云责任共担模式的一部分， AWS 管理满足大多数安全敏感组织要求的数据中心、网络和软件架构。 AWS 负责与 AWS Config 服务本身有关的任何事件响应。此外，作为 AWS 客户，您也有责任维护云端的安全。这意味着您可以从自己有权访问的 AWS 工具和功能中控制您选择实施的安全性，并负责在责任共担模型中做出事件响应。

通过建立符合云端运行应用程序目标的安全基准，您可以检测出可以响应的偏差。由于安全事件响应可能是一个复杂的主题，因此我们鼓励您查看以下资源，以便更好地了解事件响应 (IR) 和您的选择对企业目标的影响：AWS 安全事件响应指南、AWS 安全最佳实践白皮书和AWS 云采用框架 (CAF) 的安全视角白皮书。

合规性验证 AWS Config

AWS Config 作为多个合规计划的一部分，第三方审计师对安全性和 AWS 合规性进行评估。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合AWS 规资源 — 此工作簿和指南集合可能适用于您的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

韧性在 AWS Config

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

中的基础设施安全 AWS Config

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

您可以使用 AWS 已发布的 API 调用 AWS Config 通过网络进行访问。客户端必须支持以下内容：

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

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

配置和脆弱性分析

对于 AWS Config， AWS 处理基本的安全任务，例如客户机操作系统 (OS) 和数据库修补、防火墙配置和灾难恢复。

防止跨服务混淆座席

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在中 AWS，跨服务模仿可能会导致混乱的副手问题。一个服务（呼叫服务）调用另一项服务（所谓的服务）时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有访问权限的方式对另一个客户的资源进行操作。为防止这种情况， AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议在资源策略中使用`aws:SourceArn`和`aws:SourceAccount`全局条件上下文密钥来限制为资源 AWS Config 提供其他服务的权限。如果您只希望将一个资源与跨服务访问相关联，请使用 `aws:SourceArn`。如果您想允许该账户中的任何资源与跨服务使用操作相关联，请使用 `aws:SourceAccount`。

防范混淆代理问题最有效的方法是使用 `aws:SourceArn` 全局条件上下文键和资源的完整 ARN。如果不知道资源的完整 ARN，或者正在指定多个资源，请针对 ARN 未知部分使用带有通配符字符 (*) 的 `aws:SourceArn` 全局上下文条件键。例如，`arn:aws:servicename:*:123456789012:*`。

如果 `aws:SourceArn` 值不包含账户 ID，例如 Amazon S3 存储桶 ARN，您必须使用两个全局条件上下文键来限制权限。

以下示例显示了如何使用中的`aws:SourceArn`和`aws:SourceAccount`全局条件上下文密钥 AWS Config 来防止出现混淆的副手问题：授予 AWS Config 对 Amazon S3 存储桶的访问权限。

的安全最佳实践 AWS Config

AWS Config 提供了许多安全功能，供您在制定和实施自己的安全策略时考虑。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

- 利用标记 AWS Config，这样可以更轻松地管理、搜索和筛选资源。

- 确认您的配送渠道已正确设置，确认后，请确认 AWS Config 是否正确录制。

有关更多信息，请参阅 AWS Config 最佳实践博客。

登录和监控 AWS Config

AWS Config 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在中执行的操作的记录 AWS Config。监控是维护 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS Config

主题

- 使用记录 AWS Config API 调用 AWS CloudTrail
- 监控

使用记录 AWS Config API 调用 AWS CloudTrail

CloudTrail 将所有 API 调用捕获 AWS Config 为事件。捕获的调用包括来自 AWS Config 控制台的调用和对 AWS Config API 操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括的事件 AWS Config。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向哪个请求发出 AWS Config、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

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

主题

- AWS Config 中的信息 CloudTrail
- 了解 AWS Config 日志文件条目
- 示例日志文件

AWS Config 中的信息 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当活动发生在中时 AWS Config，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

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

- 创建跟踪概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail日志文件

所有 AWS Config 操作均由《API 参考》记录 CloudTrail 并记录在《AWS Config API 参考》中。例如，调用 DeliverConfigSnapshot、DeleteDeliveryChannel 和 Ch DescribeDeliveryan nels 操作会在 CloudTrail 日志文件中生成条目。

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

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅CloudTrail 用户身份元素。

了解 AWS Config 日志文件条目

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

示例日志文件

有关 CloudTrail 日志条目的示例，请参阅以下主题。

DeleteDeliveryChannel

以下是 Chan DeleteDeliverynel 操作的示例 CloudTrail 日志文件。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:32:57Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeleteDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-internal/3",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": null,
      "requestID": "207d695a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "5dcff7a9-e414-411a-a43e-88d122a0ad4a",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DeliverConfigSnapshot

以下是DeliverConfig快照操作的示例 CloudTrail 日志文件。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
```

```
      },
      "eventTime": "2014-12-11T00:58:53Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DeliverConfigSnapshot",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "10.24.34.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannelName": "default"
      },
      "responseElements": {
        "configSnapshotId": "58d50f10-212d-4fa4-842e-97c614da67ce"
      },
      "requestID": "e0248561-80d0-11e4-9f1c-7739d36a3df2",
      "eventID": "3e88076c-eae1-4aa6-8990-86fe52aedbd8",
      "eventType": "AwsApiCall",
      recipientAccountId": "111111111111"
    }
```

DescribeConfigurationRecorderStatus

以下是该DescribeConfigurationRecorderStatus操作的 CloudTrail 日志文件示例。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:44Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorderStatus",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "8442f25d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "a675b36b-455f-4e18-a4bc-d3e01749d3f1",
      "eventType": "AwsApiCall",
```

```
      "recipientAccountId": "222222222222"
    }
```

DescribeConfigurationRecorders

以下是 “DescribeConfiguration录制器” 操作的示例 CloudTrail 日志文件。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:34:52Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeConfigurationRecorders",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6566b55c-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6259a9ad-889e-423b-beeb-6e1eec84a8b5",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

DescribeDeliveryChannels

以下是 Chann CloudTrail els 操作的DescribeDelivery日志文件示例。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
```

```
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:02Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "DescribeDeliveryChannels",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "6b6aee3f-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "3e15ebc5-bf39-4d2a-8b64-9392807985f1",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

GetResourceConfigHistory

以下是该GetResourceConfigHistory操作的 CloudTrail 日志文件示例。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAABCDEFGHIJKLNMOPQ:Config-API-Test",
        "arn": "arn:aws:sts::111111111111:assumed-role/JaneDoe/Config-API-Test",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-12-11T00:58:42Z"
          },
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDAABCDEFGHIJKLNMOPQ",
            "arn": "arn:aws:iam::111111111111:role/JaneDoe",
            "accountId": "111111111111",
            "userName": "JaneDoe"
          }
        }
      },
      "eventTime": "2014-12-11T00:58:42Z",
      "eventSource": "config.amazonaws.com",
```

```
        "eventName": "GetResourceConfigHistory",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "10.24.34.0",
        "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
        "requestParameters": {
          "resourceId": "vpc-a12bc345",
          "resourceType": "AWS::EC2::VPC",
          "limit": 0,
          "laterTime": "Dec 11, 2014 12:58:42 AM",
          "earlierTime": "Dec 10, 2014 4:58:42 PM"
        },
        "responseElements": null,
        "requestID": "d9f3490d-80d0-11e4-9f1c-7739d36a3df2",
        "eventID": "ba9c1766-d28f-40e3-b4c6-3ffb87dd6166",
        "eventType": "AwsApiCall",
        "recipientAccountId": "111111111111"
        }
```

PutConfigurationRecorder

以下是 R PutConfigurationecorder 操作的示例 CloudTrail 日志文件。

```
{
        "eventVersion": "1.02",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "AIDACKCEVSQ6C2EXAMPLE",
          "arn": "arn:aws:iam::222222222222:user/JohnDoe",
          "accountId": "222222222222",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "userName": "JohnDoe"
        },
        "eventTime": "2014-12-11T18:35:23Z",
        "eventSource": "config.amazonaws.com",
        "eventName": "PutConfigurationRecorder",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
        "requestParameters": {
          "configurationRecorder": {
            "name": "default",
            "roleARN": "arn:aws:iam::222222222222:role/config-role-pdx"
          }
        },
```

```
      "responseElements": null,
      "requestID": "779f7917-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "c91f3daa-96e8-44ee-8ddd-146ac06565a7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

PutDeliveryChannel

以下是 Chan PutDeliverynel 操作的示例 CloudTrail 日志文件。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:33:08Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "PutDeliveryChannel",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "deliveryChannel": {
          "name": "default",
          "s3BucketName": "config-api-test-pdx",
          "snsTopicARN": "arn:aws:sns:us-west-2:222222222222:config-api-test-pdx"
        }
      },
      "responseElements": null,
      "requestID": "268b8d4d-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "b2db05f1-1c73-4e52-b238-db69c04e8dd4",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StartConfigurationRecorder

以下是 R StartConfigurationecorder 操作的示例 CloudTrail 日志文件。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:34Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StartConfigurationRecorder",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "7e03fa6a-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "55a5507f-f306-4896-afe3-196dc078a88d",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

StopConfigurationRecorder

以下是 R StopConfigurationecorder 操作的示例 CloudTrail 日志文件。

```
{
      "eventVersion": "1.02",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::222222222222:user/JohnDoe",
        "accountId": "222222222222",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "userName": "JohnDoe"
      },
      "eventTime": "2014-12-11T18:35:13Z",
      "eventSource": "config.amazonaws.com",
      "eventName": "StopConfigurationRecorder",
```

```
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.0",
      "userAgent": "aws-cli/1.2.11 Python/2.7.4 Linux/2.6.18-164.el5",
      "requestParameters": {
        "configurationRecorderName": "default"
      },
      "responseElements": null,
      "requestID": "716deea3-8164-11e4-ab4f-657c7ab282ab",
      "eventID": "6225a85d-1e49-41e9-bf43-3cfc5549e560",
      "eventType": "AwsApiCall",
      "recipientAccountId": "222222222222"
    }
```

监控

您可以使用其他 AWS 服务来监控 AWS Config 资源。

- 每次由于用户 API 活动而创建、更新或以其他方式修改支持的 AWS 资源时，您都可以使用亚马逊简单通知服务 (SNS) Simple Notification Service 向您发送通知。
- 您可以使用 Amazon EventBridge 来检测 AWS Config 事件状态的变化并做出反应。

主题

- 使用 Amazon SQS 监控 AWS 资源变化
- AWS Config 使用 Amazon 进行监控 EventBridge

使用 Amazon SQS 监控 AWS 资源变化

AWS Config 每次由于用户 API 活动而创建、更新或以其他方式修改支持的 AWS 资源时，都会使用亚马逊简单通知服务 (SNS) Simple Notification Service 向您发送通知。但是您可能只关注特定资源配置的更改。例如，您可能认为必须在有人修改了安全组配置时了解这一情况，但不需要在您的 Amazon EC2 实例标签每次更改时都得到通知。或者，您可能想要编写一个在指定资源被更新时执行指定操作的程序。例如，您可能想要在某个安全组的配置发生更改时启动特定工作流程。如果您想通过这些或其他方式以编程方式使用来自 AWS Config 的数据，请使用亚马逊简单队列服务队列作为 Amazon SNS 的通知终端节点。

> **Note**
>
> Amazon SNS 发出的通知的形式可以是电子邮件、发送到支持短信服务功能的手机和智能手机上的短信服务 (SMS) 消息、发送到移动设备应用程序上的通知消息，或者发送到一个或多个 HTTP 或 HTTPS 端点的通知消息。

您可以让一个 SQS 队列订阅多个主题，无论您为每个区域订阅一个主题，还是每个区域的每个账户都有一个主题。您必须用队列订阅您需要的 SNS 主题。(您可以用多个队列订阅一个 SNS 主题。) 有关更多信息，请参阅将 Amazon SNS 消息发送到 Amazon SQS 队列。

Amazon SQS 的权限

要将 Amazon SQS 与配合使用 AWS Config，您必须配置一项策略，向您的账户授予执行所有 SQS 队列允许的操作的权限。以下示例策略授予账户 111122223333 和 444455556666 权限，允许其在名为 arn:aws:sqs:us-east-2:444455556666:queue1. 的队列每次发生配置更改时发送相关消息。

```
{
  "Version": "2012-10-17",
  "Id": "Queue1_Policy_UUID",
  "Statement":
    {
       "Sid":"Queue1_SendMessage",
       "Effect": "Allow",
       "Principal": {
            "AWS": ["111122223333","444455556666"]
         },
        "Action": "sqs:SendMessage",
        "Resource": "arn:aws:sqs:us-east-2:444455556666:queue1"
     }
}
```

您还必须创建一项策略，授予 SNS 主题和订阅该主题的 SQS 队列之间的连接权限。以下是一个策略示例，它允许使用亚马逊资源名称 (ARN) 的 SNS 主题 arn: aws: sns: us-east-2:111122223333: test-topic 对名为 arn: aws: sqs: us-east-2:111122223333: 的队列执行任何操作。test-topic-queue

> **Note**
>
> SNS 主题和 SQS 队列的账户必须处于同一区域中。

```
{
  "Version": "2012-10-17",
  "Id": "SNStoSQS",
  "Statement":
    {
      "Sid":"rule1",
      "Effect": "Allow",
      "Principal": {
        "Service": "sns.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:us-east-2:111122223333:test-topic-queue",
      "Condition" : {
        "StringEquals" : {
          "aws:SourceArn":"arn:aws:sns:us-east-2:111122223333:test-topic"
        }
      }
    }
}
```

每项策略中的规定可以只针对一个队列而不是多个队列。有关 Amazon SQS 策略受到的其他限制的信息，请参阅 Amazon SQS 策略的特别信息。

AWS Config 使用 Amazon 进行监控 EventBridge

Amazon EventBridge 提供了描述 AWS 资源变化的近乎实时的系统事件流。使用 Amazon EventBridge 来检测 AWS Config 事件状态的变化并做出反应。

您可以创建一个规则，只要状态发生变换或者在变换到一个或多个感兴趣的状态时，就运行该规则。然后，当事件与您在规则中指定的值相匹配时，Amazon 会根据您创建的规则 EventBridge 调用一个或多个目标操作。根据事件类型，您可能想要发送通知、捕获事件信息、采取纠正措施、启动事件或采取其他操作。

但是 AWS Config，在为创建事件规则之前，应执行以下操作：

- 熟悉中的事件、规则和目标。 EventBridge有关更多信息，请参阅什么是亚马逊 EventBridge？
- 有关如何开始使用 EventBridge 和设置规则的更多信息，请参阅 Amazon 入门 EventBridge。
- 创建将在您的事件规则中使用的目标。

主题

- Amazon EventBridge 格式为 AWS Config
- 为以下各项创建亚马逊 EventBridge 规则 AWS Config

Amazon EventBridge 格式为 AWS Config

EventBridge 的事件 AWS Config 采用以下格式：

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "event type",
   "source": "aws.config",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [
      resources
   ],
   "detail": {
      specific message type
   }
}
```

为以下各项创建亚马逊 EventBridge 规则 AWS Config

使用以下步骤创建触发事件的 EventBridge 规则。 AWS Config尽最大努力发出事件。

1. 在导航窗格中，选择规则。
2. 选择创建规则。
3. 为规则输入名称和描述。

   规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。
4. 对于规则类型，选择具有事件模式的规则。
5. 对于事件来源，选择AWS 事件或 EventBridge 合作伙伴事件。
6. （可选）对于示例事件类型，选择 AWS 事件。
7. （可选）对于示例事件，选择用于触发此规则的事件类型：

- 选择 AWS API 调用 CloudTrail方式，根据对此服务进行的 API 调用制定规则。有关创建此类规则的更多信息，请参阅教程：为 AWS CloudTrail API 调用创建 Amazon EventBridge 规则。
- 选择 Config Configuration Item Change 以在您账户中的资源发生更改时获取通知。

  如这些支持文章中所述，在创建或删除资源时，您可以使用 EventBridge 接收自定义电子邮件通知。在我的 using AWS Config 服务中创建资源时，如何接收自定义电子邮件通知？ AWS 账户 以及当我的 AWS 账户 使用 AWS Config 服务中的资源被删除时，如何才能收到自定义电子邮件通知？ 。
- 选择 Config Rules Compliance Change 以在对您的规则进行合规性检查失败时获取通知。

  如本支持文章所述，当资源不合规时，您可以使用 EventBridge 接收自定义电子邮件通知，当资源不合规时，如何使用通知我？ AWS AWS Config。
- 选择 Config Rules Re-evaluation Status 以获取重新评估状态通知。
- 选择 Config Configuration Snapshot Delivery Status 以获取配置快照传输状态通知。
- 选择 Config Configuration History Delivery Status 以获取配置历史记录传输状态通知。

8. 对于创建方法，选择使用模式表单。
9. 对于事件源，选择AWS 服务。
10. 对于 AWS 服务，请选择 Config。
11. 对于事件类型，选择用于触发此规则的事件类型：
    - 选择 “所有事件” 以制定适用于所有 AWS 服务的规则。如果您选择此选项，则不能选择特定的消息类型、规则名称、资源类型或资源 ID。
    - 选择 AWS API 调用 CloudTrail方式，根据对此服务进行的 API 调用制定规则。有关创建此类规则的更多信息，请参阅教程：为 AWS CloudTrail API 调用创建 Amazon EventBridge 规则。
    - 选择 Config Configuration Item Change 以在您账户中的资源发生更改时获取通知。

      如这些支持文章中所述，在创建或删除资源时，您可以使用 EventBridge 接收自定义电子邮件通知。在我的 using AWS Config 服务中创建资源时，如何接收自定义电子邮件通知？ AWS 账户 以及当我的 AWS 账户 使用 AWS Config 服务中的资源被删除时，如何才能收到自定义电子邮件通知？ 。
    - 选择 Config Rules Compliance Change 以在对您的规则进行合规性检查失败时获取通知。

      如本支持文章所述，当资源不合规时，您可以使用 EventBridge 接收自定义电子邮件通知，当资源不合规时，如何使用通知我？ AWS AWS Config。
    - 选择 Config Rules Re-evaluation Status 以获取重新评估状态通知。
    - 选择 Config Configuration Snapshot Delivery Status 以获取配置快照传输状态通知。

- 选择 Config Configuration History Delivery Status 以获取配置历史记录传输状态通知。

12选择 Any message type 以接收任何类型的通知。选择 Specific message type(s) 以接收以下类型的通知：

- 如果您愿意 ConfigurationItemChangeNotification，则在 AWS Config 评估的资源的配置发生变化时，您会收到消息。
- 如果选择 “ComplianceChange通知”，则当 AWS Config 评估的资源的合规性类型发生变化时，您会收到消息。
- 如果您愿意 ConfigRulesEvaluationStarted，则在 AWS Config 开始针对指定资源评估您的规则时，您会收到消息。
- 如果您愿意 ConfigurationSnapshotDeliveryCompleted，则在 AWS Config 成功将配置快照传送到您的 Amazon S3 存储桶时，您会收到消息。
- 如果您愿意 ConfigurationSnapshotDeliveryFailed，则在 AWS Config 无法将配置快照传送到您的 Amazon S3 存储桶时，您会收到消息。
- 如果您愿意 ConfigurationSnapshotDeliveryStarted，则在 AWS Config 开始将配置快照传送到您的 Amazon S3 存储桶时会收到消息。
- 如果您愿意 ConfigurationHistoryDeliveryCompleted，则在 AWS Config 成功将配置历史记录传送到您的 Amazon S3 存储桶时，您会收到消息。

13如果您从 “事件类型” 下拉列表中选择了特定的事件类型，请选择 “任何资源类型”，以制定适用于所有 AWS Config 支持的资源类型的规则。

或者，选择 Specific resource type(s) (特定资源类型)，然后键入 AWS Config 支持的资源类型（例如，`AWS::EC2::Instance`）。

14如果您从事件类型下拉列表中选择了某个特定事件类型，请选择任何资源 ID，以包括 AWS Config 支持的任何资源 ID。

或者，选择 Specific resource ID(s) (特定资源 ID)，然后键入 AWS Config 支持的资源 ID（例如，`i-04606de676e635647`）。

15如果您从事件类型下拉列表中选择了某个特定事件类型，请选择任何规则名称，以包括 AWS Config 支持的任何规则。

或者，选择 Specific rule name(s) (特定规则名称)，然后键入 AWS Config 支持的规则（例如，required-tags）。

16对于选择目标，选择您准备为此规则使用的目标类型，然后配置该类型所需的任何其他选项。

17显示的字段因您选择的服务而异。根据需要输入此目标类型的特定信息。

18对于许多目标类型， EventBridge 需要向目标发送事件的权限。在这些情况下， EventBridge 可以创建规则运行所需的 IAM 角色。

- 若要自动创建 IAM 角色，请选择 Create a new role for this specific resource (为此特定资源创建新角色)。
- 要使用您之前创建的 IAM 角色，请选择 Use existing role (使用现有角色)。

19.（可选）选择 Add target (添加目标)，以便为此规则添加另一个目标。

20.（可选）为规则输入一个或多个标签。有关更多信息，请参阅 Amazon EventBridge 标签。

21.审查您的规则设置以确保其符合事件监控要求。

22选择创建以确认您的选择。

AWS Config 与接口 Amazon VPC 终端节点一起使用

如果您使用亚马逊虚拟私有云（Amazon VPC）托管 AWS 资源，则可以在您的 VPC 和之间建立私有连接 AWS Config。您可以使用此连接从您的 VPC 上与 AWS Config 通信而不用访问公共 Internet。

Amazon VPC 是一项 AWS 服务，可用于在您定义的虚拟网络中启动 AWS 资源。借助 VPC，您可以控制您的网络设置，如 IP 地址范围、子网、路由表和网络网关。Interface VPC 终端节点由 AWS PrivateLink一种 AWS 技术提供支持，该技术使用带有私有 IP 地址的弹性网络接口实现 AWS 服务之间的私密通信。要将您的 VPC 连接到 AWS Config，您需要为定义接口 VPC 终端节点 AWS Config。这种类型的终端节点使您能够将 VPC 连接到 AWS 服务。该端点 AWS Config 无需互联网网关、网络地址转换 (NAT) 实例或 VPN 连接即可提供可靠、可扩展的连接。有关更多信息，请参阅 Amazon VPC 用户指南中的什么是 Amazon VPC。

以下步骤适用于 Amazon VPC 的用户。有关更多信息，请参阅 Amazon VPC 用户指南中的入门。

为创建 VPC 终端节点 AWS Config

要开始在您的 VPC 中使用 AWS Config ，请为创建一个接口 VPC 终端节点 AWS Config。您无需更改的设置 AWS Config。 AWS Config 使用其他 AWS 服务的公共端点调用其他服务。有关更多信息，请参阅 Amazon VPC 用户指南中的创建接口终端节点。

常见问题

看不到我最新的配置更改

我可以立即查看我的配置更改吗？

AWS Config 通常会在检测到更改后立即或按您指定的频率记录对资源的配置更改。但是，这是尽力而为，有时可能需要更长的时间。如果问题在一段时间后仍然存在，请联系AWS Support并提供亚马逊CloudWatch支持的 AWS Config 指标。有关这些指标的信息，请参阅AWS Config 使用情况和成功指标。

中的间接关系 AWS Config

主题

- 什么是资源关系？
- 什么是与资源的直接关系和间接关系？
- AWS Config 支持哪些间接关系？
- 由于直接关系和间接关系，配置项是如何创建的？
- 由于间接关系而生成的配置项有哪些？
- 如何检索与间接关系相关的配置数据？

什么是资源关系？

在中 AWS，资源是指可管理的实体，例如亚马逊弹性计算云 (Amazon EC2) 实例、 AWS CloudFormation 堆栈或 Amazon S3 存储桶。 AWS Config 是一项跟踪和监视资源的服务，每当检测到对录制的资源类型进行更改时，或者按照您设置的录制频率创建配置项目 (CI)。例如，当设置 AWS Config 为跟踪 Amazon EC2 实例时，它会在每次创建、更新或删除实例时创建一个配置项目。创建的每个配置项目 AWS Config 都有多个字段，包括`accountId`、`arn`（Amazon 资源名称）`awsRegionconfiguration`、`tags`、和`relationships`。CI 的关系字段可以 AWS Config 显示资源是如何相互关联的。例如，关系可能表示 ID 为 `vol-123ab45d` 的 Amazon EBS 卷已附加到 ID 为 `i-a1b2c3d4` 且与安全组 `sg-ef678hk` 关联的 Amazon EC2 实例。

什么是与资源的直接关系和间接关系？

AWS Config 从配置字段中推导出大多数资源类型的关系，这些关系称为 “直接” 关系。直接关系是一个资源 (A) 和另一个资源 (B) 之间的单向连接 (A→B)，通常从资源 (A) 的描述 API 响应中获得。过去，对于 AWS Config 最初支持的某些资源类型，它还会从其他资源的配置中捕获关系，从而创建双向的 “间接” 关系（B→A）。例如，Amazon EC2 实例与其安全组之间的关系是直接关系，因为安全组包含在 Amazon EC2 实例的描述 API 响应中。另一方面，安全组和 Amazon EC2 实例之间的关系是间接关系，因为描述安全组不会返回与其关联的实例的任何信息。因此，当检测到资源配置更改时， AWS Config 不仅会为该资源创建 CI，还会为任何相关资源（包括具有间接关系的资源）生成 CI。例如，当 AWS Config 检测到 Amazon EC2 实例中的更改时，它会为该实例创建一个 CI，为与该实例关联的安全组创建一个 CI。

AWS Config 支持哪些间接关系？

中支持以下间接资源关系 AWS Config。

资源类型	与此资源类型间接相关		
AWS::EC2::RouteTable	AWS::EC2::Instance，AWS::EC2::NetworkInterface，AWS::EC2::Subnet，AWS::EC2::VPNGateway，AWS::EC2::VPC		
AWS::EC2::EIP	AWS::EC2::Instance，AWS::EC2::NetworkInterface		
AWS::EC2::Instance	AWS::EC2::Security		

资源类型	与此资源类型间接相关		
	Group ，AWS::EC2::Subnet ，AWS::EC2::VPC		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup ，AWS::EC2::Subnet ，AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet ，AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway ，AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

由于直接关系和间接关系，配置项是如何创建的？

对于资源之间的直接关系 (A→B)，对资源 B 的任何配置更改也将启动资源 A 的配置项 (CI)。同样，对于间接关系 (B→A)，当资源 A 发生配置更改时，将为资源 B 生成一个新的 CI。例如，Amazon EC2 实例与安全组是直接关系，因此对安全组的任何配置更改都将为安全组生成一个 CI，并为 EC2 实例生成一个 CI。同样，安全组与 Amazon EC2 实例是间接关系，因此对 EC2 实例的任何配置更改都将为 Amazon EC2 实例生成一个 CI，并为安全组生成一个 CI。

由于间接关系而生成的配置项有哪些？

以下是由于间接资源关系而生成的其他配置项 (CI)。

以下资源类型的配置更改	将为以下资源类型生成 CI		
`AWS::EC2::RouteTable`	`AWS::EC2::Instance` 、`AWS::EC2::NetworkInterface` 、`AWS::EC2::Subnet` 、`AWS::EC2::VPNGateway` 和 `AWS::EC2::VPC`		
`AWS::EC2::EIP`	`AWS::EC2::Instance` ，`AWS::EC2::NetworkInterface`		
`AWS::EC2::Instance`	`AWS::EC2::SecurityGroup` ，`AWS::EC2::Subnet` ，`AWS::EC2::VPC`		

以下资源类型的配置更改	将为以下资源类型生成 CI		
AWS::EC2::NetworkInterface	AWS::EC2::SecurityGroup , AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::NetworkACL	AWS::EC2::Subnet , AWS::EC2::VPC		
AWS::EC2::VPNConnection	AWS::EC2::VPNGateway ,AWS::EC2::CustomerGateway		
AWS::EC2::InternetGateway	AWS::EC2::VPC		
AWS::EC2::SecurityGroup	AWS::EC2::VPC		
AWS::EC2::Subnet	AWS::EC2::VPC		
AWS::EC2::VPNGateway	AWS::EC2::VPC		

如何检索与间接关系相关的配置数据？

您可以在 AWS Config 高级查询中运行结构化查询语言 (SQL) 查询，以检索与间接资源关系相关的配置数据。例如，如果您想检索与安全组相关的 Amazon EC2 实例列表，请使用以下查询：

```
SELECT
```

```
    resourceId,
    resourceType
    WHERE
    resourceType ='AWS::EC2::Instance'
    AND
    relationships.resourceId = 'sg-234213'
```

AWS Config 使用 AWS SDK 的代码示例

以下代码示例说明如何 AWS Config 使用 AWS 软件开发套件 (SDK)。

操作是大型程序的代码摘录，必须在上下文中运行。您可以通过操作了解如何调用单个服务函数，还可以通过函数相关场景和跨服务示例的上下文查看操作。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

代码示例

- AWS Config 使用 AWS SDK 的操作
  - DeleteConfigRule与 AWS SDK 或 CLI 配合使用
  - DescribeComplianceByConfigRule与 AWS SDK 或 CLI 配合使用
  - DescribeComplianceByResource与 AWS SDK 或 CLI 配合使用
  - DescribeConfigRuleEvaluationStatus与 AWS SDK 或 CLI 配合使用
  - DescribeConfigRules与 AWS SDK 或 CLI 配合使用
  - DescribeConfigurationRecorderStatus与 AWS SDK 或 CLI 配合使用
  - DescribeConfigurationRecorders与 AWS SDK 或 CLI 配合使用
  - DescribeDeliveryChannels与 AWS SDK 或 CLI 配合使用
  - GetComplianceDetailsByConfigRule与 AWS SDK 或 CLI 配合使用
  - GetComplianceDetailsByResource与 AWS SDK 或 CLI 配合使用
  - GetComplianceSummaryByConfigRule与 AWS SDK 或 CLI 配合使用
  - GetComplianceSummaryByResourceType与 AWS SDK 或 CLI 配合使用
  - PutConfigRule与 AWS SDK 或 CLI 配合使用
  - PutDeliveryChannel与 AWS SDK 或 CLI 配合使用

AWS Config 使用 AWS SDK 的操作

以下代码示例演示了如何使用 AWS 软件开发工具包执行单个 AWS Config 操作。这些摘录调用 AWS Config API，是大型程序的代码摘录，这些程序必须在上下文中运行。每个示例都包含一个指向的链接 GitHub，您可以在其中找到有关设置和运行代码的说明。

以下示例仅包括最常用的操作。有关完整列表，请参阅 AWS Config API 参考。

示例

- DeleteConfigRule与 AWS SDK 或 CLI 配合使用
- DescribeComplianceByConfigRule与 AWS SDK 或 CLI 配合使用
- DescribeComplianceByResource与 AWS SDK 或 CLI 配合使用
- DescribeConfigRuleEvaluationStatus与 AWS SDK 或 CLI 配合使用
- DescribeConfigRules与 AWS SDK 或 CLI 配合使用
- DescribeConfigurationRecorderStatus与 AWS SDK 或 CLI 配合使用
- DescribeConfigurationRecorders与 AWS SDK 或 CLI 配合使用
- DescribeDeliveryChannels与 AWS SDK 或 CLI 配合使用
- GetComplianceDetailsByConfigRule与 AWS SDK 或 CLI 配合使用
- GetComplianceDetailsByResource与 AWS SDK 或 CLI 配合使用
- GetComplianceSummaryByConfigRule与 AWS SDK 或 CLI 配合使用
- GetComplianceSummaryByResourceType与 AWS SDK 或 CLI 配合使用
- PutConfigRule与 AWS SDK 或 CLI 配合使用
- PutDeliveryChannel与 AWS SDK 或 CLI 配合使用

`DeleteConfigRule`与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DeleteConfigRule`。

CLI

AWS CLI

删除 C AWS onfig 规则

以下命令删除名为的 AWS Config 规则`MyConfigRule`：

```
aws configservice delete-config-rule --config-rule-name MyConfigRule
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考DeleteConfigRule中的。

Python

SDK for Python (Boto3)

> **Note**
>
> 还有更多相关信息 GitHub。在 AWS 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client


    def delete_config_rule(self, rule_name):
        """
        Delete the specified rule.

        :param rule_name: The name of the rule to delete.
        """
        try:
            self.config_client.delete_config_rule(ConfigRuleName=rule_name)
            logger.info("Deleted rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't delete rule %s.", rule_name)
            raise
```

- 有关 API 的详细信息，请参阅适用DeleteConfigRule于 Python 的AWS SDK (Boto3) API 参考。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeComplianceByConfigRule`与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DescribeComplianceByConfigRule`。

CLI

AWS CLI

获取您的 AWS Config 规则的合规性信息

以下命令返回一个或多个 AWS 资源违反的每个 AWS Config 规则的合规性信息：

```
aws configservice describe-compliance-by-config-rule --compliance-types
 NON_COMPLIANT
```

在输出中，每个`CappedCount`属性的值都表示有多少资源不符合相关规则。例如，以下输出表明 3 个资源不符合名为的规则`InstanceTypesAreT2micro`。

输出：

```
{
    "ComplianceByConfigRules": [
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
            "ConfigRuleName": "InstanceTypesAreT2micro"
        },
        {
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            },
```

```
            "ConfigRuleName": "RequiredTagsForVolumes"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考DescribeComplianceByConfigRule中的。

PowerShell

用于 PowerShell

示例 1：此示例检索规则的合规性详细信息，该规则当前没有评估结果 ebs-optimized-instance，因此它返回 INSUFKIENT_DATA

```
(Get-CFGComplianceByConfigRule -ConfigRuleName ebs-optimized-instance).Compliance
```

输出：

```
ComplianceContributorCount ComplianceType
-------------------------- --------------
                           INSUFFICIENT_DATA
```

示例 2：此示例返回规则 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK 的不合规资源数量。

```
(Get-CFGComplianceByConfigRule -ConfigRuleName
 ALB_HTTP_TO_HTTPS_REDIRECTION_CHECK -ComplianceType
 NON_COMPLIANT).Compliance.ComplianceContributorCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       2
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考DescribeComplianceByConfigRule中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

DescribeComplianceByResource与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 DescribeComplianceByResource。

CLI

AWS CLI

获取 AWS 资源的合规性信息

以下命令返回由 AWS Config 记录且违反一条或多条规则的每个 EC2 实例的合规性信息：

```
aws configservice describe-compliance-by-resource --resource-type
 AWS::EC2::Instance --compliance-types NON_COMPLIANT
```

在输出中，每个CappedCount属性的值都表示该资源违反了多少规则。例如，以下输出表明该实例i-1a2b3c4d违反了 2 条规则。

输出：

```
{
    "ComplianceByResources": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-1a2b3c4d",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 2,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
        },
        {
            "ResourceType": "AWS::EC2::Instance",
            "ResourceId": "i-2a2b3c4d ",
            "Compliance": {
                "ComplianceContributorCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceType": "NON_COMPLIANT"
            }
```

```
        }
    ]
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考DescribeComplianceByResource中的。

PowerShell

用于 PowerShell

示例 1：此示例检查**AWS::SSM::ManagedInstanceInventory**资源类型的 “合规” 合规性类型。

```
Get-CFGComplianceByResource -ComplianceType COMPLIANT -ResourceType
 AWS::SSM::ManagedInstanceInventory
```

输出：

```
Compliance                            ResourceId          ResourceType
----------                            ----------          ------------
Amazon.ConfigService.Model.Compliance i-0123bcf4b567890e3
 AWS::SSM::ManagedInstanceInventory
Amazon.ConfigService.Model.Compliance i-0a1234f6f5d6b78f7
 AWS::SSM::ManagedInstanceInventory
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考DescribeComplianceByResource中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

DescribeConfigRuleEvaluationStatus与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DescribeConfigRuleEvaluationStatus`。

CLI

AWS CLI

获取 AWS Config 规则的状态信息

以下命令返回名为的 AWS Config 规则的状态信息`MyConfigRule`：

```
aws configservice describe-config-rule-evaluation-status --config-rule-names
 MyConfigRule
```

输出：

```
{
    "ConfigRulesEvaluationStatus": [
        {
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "FirstActivatedTime": 1450311703.844,
            "ConfigRuleId": "config-rule-abcdef",
            "LastSuccessfulInvocationTime": 1450314643.156,
            "ConfigRuleName": "MyConfigRule"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考DescribeConfigRuleEvaluationStatus中的。

PowerShell

用于 PowerShell

示例 1：此示例返回给定配置规则的状态信息。

```
Get-CFGConfigRuleEvaluationStatus -ConfigRuleName root-account-mfa-enabled, vpc-
flow-logs-enabled
```

输出：

```
ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-kvq1wk
ConfigRuleId                 : config-rule-kvq1wk
ConfigRuleName               : root-account-mfa-enabled
FirstActivatedTime           : 8/27/2019 8:05:17 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
```

```
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 8:12:03 AM
LastSuccessfulInvocationTime : 12/13/2019 8:12:03 AM

ConfigRuleArn                : arn:aws:config:eu-west-1:123456789012:config-rule/
config-rule-z1s23b
ConfigRuleId                 : config-rule-z1s23b
ConfigRuleName               : vpc-flow-logs-enabled
FirstActivatedTime           : 8/14/2019 6:23:44 AM
FirstEvaluationStarted       : True
LastErrorCode                :
LastErrorMessage             :
LastFailedEvaluationTime     : 1/1/0001 12:00:00 AM
LastFailedInvocationTime     : 1/1/0001 12:00:00 AM
LastSuccessfulEvaluationTime : 12/13/2019 7:12:01 AM
LastSuccessfulInvocationTime : 12/13/2019 7:12:01 AM
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考DescribeConfigRuleEvaluationStatus中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeConfigRules`与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DescribeConfigRules`。

CLI

AWS CLI

获取 AWS Config 规则的详细信息

以下命令返回名为的 AWS Config 规则的详细信息`InstanceTypesAreT2micro`：

```
aws configservice describe-config-rules --config-rule-names
 InstanceTypesAreT2micro
```

输出：

```
{
```

```
    "ConfigRules": [
        {
            "ConfigRuleState": "ACTIVE",
            "Description": "Evaluates whether EC2 instances are the t2.micro
 type.",
            "ConfigRuleName": "InstanceTypesAreT2micro",
            "ConfigRuleArn": "arn:aws:config:us-east-1:123456789012:config-rule/
config-rule-abcdef",
            "Source": {
                "Owner": "CUSTOM_LAMBDA",
                "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
                "SourceDetails": [
                    {
                        "EventSource": "aws.config",
                        "MessageType": "ConfigurationItemChangeNotification"
                    }
                ]
            },
            "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}",
            "Scope": {
                "ComplianceResourceTypes": [
                    "AWS::EC2::Instance"
                ]
            },
            "ConfigRuleId": "config-rule-abcdef"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考DescribeConfigRules中的。

PowerShell

用于 PowerShell

示例 1：此示例列出了账户的配置规则以及选定的属性。

```
Get-CFGConfigRule | Select-Object ConfigRuleName, ConfigRuleId, ConfigRuleArn,
 ConfigRuleState
```

输出：

```
ConfigRuleName                                      ConfigRuleId
 ConfigRuleArn
 ConfigRuleState
--------------                                      ------------
 -------------
 ---------------
ALB_REDIRECTION_CHECK                               config-rule-12iyn3
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-12iyn3
 ACTIVE
access-keys-rotated                                 config-rule-aospfr
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-aospfr
 ACTIVE
autoscaling-group-elb-healthcheck-required          config-rule-cn1f2x
 arn:aws:config-service:eu-west-1:123456789012:config-rule/config-rule-cn1f2x
 ACTIVE
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考DescribeConfigRules中的。

Python

SDK for Python (Boto3)

> **Note**
>
> 还有更多相关信息 GitHub。在 AWS 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
        """
        self.config_client = config_client
```

```
    def describe_config_rule(self, rule_name):
        """
        Gets data for the specified rule.

        :param rule_name: The name of the rule to retrieve.
        :return: The rule data.
        """
        try:
            response = self.config_client.describe_config_rules(
                ConfigRuleNames=[rule_name]
            )
            rule = response["ConfigRules"]
            logger.info("Got data for rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't get data for rule %s.", rule_name)
            raise
        else:
            return rule
```

- 有关 API 的详细信息，请参阅适用DescribeConfigRules于 Python 的AWS SDK (Boto3) API 参考。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeConfigurationRecorderStatus`与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DescribeConfigurationRecorderStatus`。

CLI

AWS CLI

获取配置记录器的状态信息

以下命令返回默认配置记录器的状态：

```
aws configservice describe-configuration-recorder-status
```

输出：

```
{
    "ConfigurationRecordersStatus": [
        {
            "name": "default",
            "lastStatus": "SUCCESS",
            "recording": true,
            "lastStatusChangeTime": 1452193834.344,
            "lastStartTime": 1441039997.819,
            "lastStopTime": 1441039992.835
        }
    ]
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考DescribeConfigurationRecorderStatus中的。

PowerShell

用于 PowerShell

示例 1：此示例返回配置记录器的状态。

```
Get-CFGConfigurationRecorderStatus
```

输出：

```
LastErrorCode        :
LastErrorMessage     :
LastStartTime        : 10/11/2019 10:13:51 AM
LastStatus           : Success
LastStatusChangeTime : 12/31/2019 6:14:12 AM
LastStopTime         : 10/11/2019 10:13:46 AM
Name                 : default
Recording            : True
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考DescribeConfigurationRecorderStatus中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

DescribeConfigurationRecorders与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 DescribeConfigurationRecorders。

CLI

AWS CLI

获取有关配置记录器的详细信息

以下命令返回有关默认配置记录器的详细信息：

```
aws configservice describe-configuration-recorders
```

输出：

```
{
    "ConfigurationRecorders": [
        {
            "recordingGroup": {
                "allSupported": true,
                "resourceTypes": [],
                "includeGlobalResourceTypes": true
            },
            "roleARN": "arn:aws:iam::123456789012:role/config-ConfigRole-
A1B2C3D4E5F6",
            "name": "default"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考DescribeConfigurationRecorders中的。

PowerShell

用于 PowerShell

示例 1：此示例返回配置记录器的详细信息。

```
Get-CFGConfigurationRecorder | Format-List
```

输出：

```
Name           : default
RecordingGroup : Amazon.ConfigService.Model.RecordingGroup
RoleARN        : arn:aws:iam::123456789012:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考DescribeConfigurationRecorders中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeDeliveryChannels`与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DescribeDeliveryChannels`。

CLI

AWS CLI

获取有关配送渠道的详细信息

以下命令返回有关交付渠道的详细信息：

```
aws configservice describe-delivery-channels
```

输出：

```
{
    "DeliveryChannels": [
        {
            "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
            "name": "default",
            "s3BucketName": "config-bucket-123456789012"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考DescribeDeliveryChannels中的。

PowerShell

用于 PowerShell

示例 1：此示例检索该地区的配送渠道并显示详细信息。

```
Get-CFGDeliveryChannel -Region eu-west-1 | Select-Object Name, S3BucketName,
 S3KeyPrefix,
 @{N="DeliveryFrequency";E={$_.ConfigSnapshotDeliveryProperties.DeliveryFrequency}}
```

输出：

```
Name    S3BucketName               S3KeyPrefix DeliveryFrequency
----    ------------               ----------- -----------------
default config-bucket-NA my          TwentyFour_Hours
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考DescribeDeliveryChannels中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`GetComplianceDetailsByConfigRule`与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 `GetComplianceDetailsByConfigRule`。

CLI

AWS CLI

获取 AWS Config 规则的评估结果

以下命令返回所有不符合名为的 AWS Config 规则的资源的评估结果`InstanceTypesAreT2micro`：

```
aws configservice get-compliance-details-by-config-rule --config-rule-name
 InstanceTypesAreT2micro --compliance-types NON_COMPLIANT
```

输出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-2a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314645.18,
            "ConfigRuleInvokedTime": 1450314642.902,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-3a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.346,
            "ConfigRuleInvokedTime": 1450314643.124,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
```

```
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考GetComplianceDetailsByConfigRule中的。

PowerShell

用于 PowerShell

示例 1：此示例获取规则的评估结果 access-keys-rotated 并返回按合规类型分组的输出

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-keys-rotated | Group-
Object ComplianceType
```

输出：

```
Count Name                      Group
----- ----                      -----
    2 COMPLIANT                 {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult}
    5 NON_COMPLIANT             {Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationResult,
 Amazon.ConfigService.Model.EvaluationRes...
```

示例 2：此示例查询合规资源的规则 access-keys-rotated 的合规性详细信息。

```
Get-CFGComplianceDetailsByConfigRule -ConfigRuleName access-
keys-rotated -ComplianceType COMPLIANT | ForEach-Object
 {$_.EvaluationResultIdentifier.EvaluationResultQualifier}
```

输出：

```
ConfigRuleName      ResourceId            ResourceType
--------------      ----------            ------------
access-keys-rotated BCAB1CDJ2LITAPVEW3JAH AWS::IAM::User
access-keys-rotated BCAB1CDJ2LITL3EHREM4Q AWS::IAM::User
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考GetComplianceDetailsByConfigRule中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

GetComplianceDetailsByResource与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 GetComplianceDetailsByResource。

CLI

AWS CLI

获取 AWS 资源的评估结果

以下命令返回 EC2 实例i-1a2b3c4d不符合的每条规则的评估结果：

```
aws configservice get-compliance-details-by-resource --resource-type
 AWS::EC2::Instance --resource-id i-1a2b3c4d --compliance-types NON_COMPLIANT
```

输出：

```
{
    "EvaluationResults": [
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "InstanceTypesAreT2micro"
                }
            },
            "ResultRecordedTime": 1450314643.288,
            "ConfigRuleInvokedTime": 1450314643.034,
            "ComplianceType": "NON_COMPLIANT"
        },
        {
            "EvaluationResultIdentifier": {
                "OrderingTimestamp": 1450314635.065,
                "EvaluationResultQualifier": {
                    "ResourceType": "AWS::EC2::Instance",
                    "ResourceId": "i-1a2b3c4d",
                    "ConfigRuleName": "RequiredTagForEC2Instances"
```

```
                }
            },
            "ResultRecordedTime": 1450314645.261,
            "ConfigRuleInvokedTime": 1450314642.948,
            "ComplianceType": "NON_COMPLIANT"
        }
    ]
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考GetComplianceDetailsByResource中的。

PowerShell

用于 PowerShell

示例 1：此示例评估结果针对给定资源。

```
Get-CFGComplianceDetailsByResource -ResourceId ABCD5STJ4EFGHIVEW6JAH -
ResourceType 'AWS::IAM::User'
```

输出：

```
Annotation                 :
ComplianceType             : COMPLIANT
ConfigRuleInvokedTime      : 8/25/2019 11:34:56 PM
EvaluationResultIdentifier :
 Amazon.ConfigService.Model.EvaluationResultIdentifier
ResultRecordedTime         : 8/25/2019 11:34:56 PM
ResultToken                :
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考GetComplianceDetailsByResource中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`GetComplianceSummaryByConfigRule`与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 `GetComplianceSummaryByConfigRule`。

CLI

AWS CLI

获取您的 AWS Config 规则的合规性摘要

以下命令返回合规规则的数量和不合规的规则数量：

```
aws configservice get-compliance-summary-by-config-rule
```

在输出中，每个CappedCount属性的值表示有多少规则合规或不合规。

输出：

```
{
    "ComplianceSummary": {
        "NonCompliantResourceCount": {
            "CappedCount": 3,
            "CapExceeded": false
        },
        "ComplianceSummaryTimestamp": 1452204131.493,
        "CompliantResourceCount": {
            "CappedCount": 2,
            "CapExceeded": false
        }
    }
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考GetComplianceSummaryByConfigRule中的。

PowerShell

用于 PowerShell

示例 1：此示例返回不合规的 Config 规则的数量。

```
Get-CFGComplianceSummaryByConfigRule -Select
 ComplianceSummary.NonCompliantResourceCount
```

输出：

```
CapExceeded CappedCount
----------- -----------
False       9
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考GetComplianceSummaryByConfigRule中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

GetComplianceSummaryByResourceType与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 GetComplianceSummaryByResourceType。

CLI

AWS CLI

获取所有资源类型的合规性摘要

以下命令返回不合规的 AWS 资源数量和合规资源的数量：

```
aws configservice get-compliance-summary-by-resource-type
```

在输出中，每个CappedCount属性的值表示有多少资源合规或不合规。

输出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 16,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1453237464.543,
                "CompliantResourceCount": {
                    "CappedCount": 10,
                    "CapExceeded": false
                }
            }
```

```
        }
    ]
}
```

获取特定资源类型的合规性摘要

以下命令返回不合规的 EC2 实例的数量和合规的数量：

```
aws configservice get-compliance-summary-by-resource-type --resource-types
 AWS::EC2::Instance
```

在输出中，每个CappedCount属性的值表示有多少资源合规或不合规。

输出：

```
{
    "ComplianceSummariesByResourceType": [
        {
            "ResourceType": "AWS::EC2::Instance",
            "ComplianceSummary": {
                "NonCompliantResourceCount": {
                    "CappedCount": 3,
                    "CapExceeded": false
                },
                "ComplianceSummaryTimestamp": 1452204923.518,
                "CompliantResourceCount": {
                    "CappedCount": 7,
                    "CapExceeded": false
                }
            }
        }
    ]
}
```

- 有关 API 的详细信息，请参阅AWS CLI 命令参考GetComplianceSummaryByResourceType中的。

PowerShell

用于 PowerShell

示例 1：此示例返回合规或不合规资源的数量，并将输出转换为 json。

```
Get-CFGComplianceSummaryByResourceType -Select
 ComplianceSummariesByResourceType.ComplianceSummary | ConvertTo-Json
{
  "ComplianceSummaryTimestamp": "2019-12-14T06:14:49.778Z",
  "CompliantResourceCount": {
    "CapExceeded": false,
    "CappedCount": 2
  },
  "NonCompliantResourceCount": {
    "CapExceeded": true,
    "CappedCount": 100
  }
}
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考GetComplianceSummaryByResourceType中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`PutConfigRule`与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 `PutConfigRule`。

CLI

AWS CLI

添加 AWS 托管 Config 规则

以下命令提供用于添加 AWS 托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
RequiredTagsForEC2Instances.json
```

`RequiredTagsForEC2Instances.json` 是一个包含规则配置的 JSON 文件：

```
{
  "ConfigRuleName": "RequiredTagsForEC2Instances",
  "Description": "Checks whether the CostCenter and Owner tags are applied to EC2
 instances.",
```

```
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "AWS",
    "SourceIdentifier": "REQUIRED_TAGS"
  },
  "InputParameters": "{\"tag1Key\":\"CostCenter\",\"tag2Key\":\"Owner\"}"
}
```

对于该`ComplianceResourceTypes`属性，此 JSON 代码将范围限制为该`AWS::EC2::Instance`类型的资源，因此 AWS Config 将仅根据规则评估 EC2 实例。由于该规则是托管规则，因此 `Owner` 属性设置为 `AWS`，`SourceIdentifier` 属性设置为规则标识符 `REQUIRED_TAGS`。对于 `InputParameters` 属性，指定了规则所需的标签键 `CostCenter` 和 `Owner`。

如果命令成功， AWS Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules 命令并指定规则名称。

添加客户托管的 Config 规则

以下命令将提供用于添加客户托管 Config 规则的 JSON 代码：

```
aws configservice put-config-rule --config-rule file://
InstanceTypesAreT2micro.json
```

`InstanceTypesAreT2micro.json` 是一个包含规则配置的 JSON 文件：

```
{
  "ConfigRuleName": "InstanceTypesAreT2micro",
  "Description": "Evaluates whether EC2 instances are the t2.micro type.",
  "Scope": {
    "ComplianceResourceTypes": [
      "AWS::EC2::Instance"
    ]
  },
  "Source": {
    "Owner": "CUSTOM_LAMBDA",
    "SourceIdentifier": "arn:aws:lambda:us-
east-1:123456789012:function:InstanceTypeCheck",
```

```
    "SourceDetails": [
      {
        "EventSource": "aws.config",
        "MessageType": "ConfigurationItemChangeNotification"
      }
    ]
  },
  "InputParameters": "{\"desiredInstanceType\":\"t2.micro\"}"
}
```

对于该`ComplianceResourceTypes`属性，此 JSON 代码将范围限制为该`AWS::EC2::Instance`类型的资源，因此 AWS Config 将仅根据规则评估 EC2 实例。由于此规则是客户托管规则，因此该`Owner`属性设置为`CUSTOM_LAMBDA`，并且该`SourceIdentifier`属性设置为 Lambda 函数 AWS 的 ARN。`SourceDetails`对象为必填项。当 Confi AWS g 调用 AWS Lambda 函数来根据规则评估资源时，为该`InputParameters`属性指定的参数将传递给 Lambda 函数。

如果命令成功， AWS Config 将不返回任何输出。要验证规则配置，请运行 describe-config-rules 命令并指定规则名称。

- 有关 API 的详细信息，请参阅AWS CLI 命令参考PutConfigRule中的。

Python

SDK for Python (Boto3)

> **Note**
>
> 还有更多相关信息 GitHub。在 AWS 代码示例存储库中查找完整示例，了解如何进行设置和运行。

```
class ConfigWrapper:
    """
    Encapsulates AWS Config functions.
    """

    def __init__(self, config_client):
        """
        :param config_client: A Boto3 AWS Config client.
```

```
        """
        self.config_client = config_client


    def put_config_rule(self, rule_name):
        """
        Sets a configuration rule that prohibits making Amazon S3 buckets
publicly
        readable.

        :param rule_name: The name to give the rule.
        """
        try:
            self.config_client.put_config_rule(
                ConfigRule={
                    "ConfigRuleName": rule_name,
                    "Description": "S3 Public Read Prohibited Bucket Rule",
                    "Scope": {
                        "ComplianceResourceTypes": [
                            "AWS::S3::Bucket",
                        ],
                    },
                    "Source": {
                        "Owner": "AWS",
                        "SourceIdentifier": "S3_BUCKET_PUBLIC_READ_PROHIBITED",
                    },
                    "InputParameters": "{}",
                    "ConfigRuleState": "ACTIVE",
                }
            )
            logger.info("Created configuration rule %s.", rule_name)
        except ClientError:
            logger.exception("Couldn't create configuration rule %s.", rule_name)
            raise
```

- 有关 API 的详细信息，请参阅适用PutConfigRule于 Python 的AWS SDK (Boto3) API 参考。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

PutDeliveryChannel与 AWS SDK 或 CLI 配合使用

以下代码示例演示如何使用 PutDeliveryChannel。

CLI

AWS CLI

创建配送渠道

以下命令以 JSON 代码的形式提供传送渠道的设置：

```
aws configservice put-delivery-channel --delivery-channel file://
deliveryChannel.json
```

该deliveryChannel.json文件指定了配送渠道属性：

```
{
    "name": "default",
    "s3BucketName": "config-bucket-123456789012",
    "snsTopicARN": "arn:aws:sns:us-east-1:123456789012:config-topic",
    "configSnapshotDeliveryProperties": {
        "deliveryFrequency": "Twelve_Hours"
    }
}
```

此示例设置了以下属性：

name-配送渠道的名称。默认情况下， AWS Config 会default将名称分配给新的交付渠道。您无法使用命令更新传递渠道名称。put-delivery-channel有关更改名称的步骤，请参阅重命名配送渠道。 s3BucketName- AWS Config 向其发送配置快照和配置历史记录文件的 Amazon S3 存储桶的名称。如果您指定的存储桶属于另一个 AWS 账户，则该存储桶必须具有授予对 Config AWS 的访问权限的策略。有关更多信息，请参阅 Amazon S3 存储桶的权限。

snsTopicARN-Amazon SNS 主题的亚马逊资源名称 (ARN)， AWS Config 会向该主题发送有关配置变更的通知。如果您从其他账户选择主题，则该主题必须具有授予对 Config 的访问权限的策略。 AWS 有关更多信息，请参阅 Amazon SNS 主题的权限。

configSnapshotDeliveryProperties-包含deliveryFrequency属性，该属性设置 AWS Config 提供配置快照的频率以及它为定期 Config 规则调用评估的频率。

如果命令成功， AWS Config 将不返回任何输出。要验证您的配送渠道的设置，请运行 describe-delivery-channels 命令。

- 有关 API 的详细信息，请参阅AWS CLI 命令参考PutDeliveryChannel中的。

PowerShell

用于 PowerShell

示例 1：此示例更改了现有配送渠道的 deliveryFrequency 属性。

```
Write-CFGDeliveryChannel -ConfigSnapshotDeliveryProperties_DeliveryFrequency
 TwentyFour_Hours -DeliveryChannelName default -DeliveryChannel_S3BucketName
 config-bucket-NA -DeliveryChannel_S3KeyPrefix my
```

- 有关 API 的详细信息，请参阅 AWS Tools for PowerShell Cmdlet 参考PutDeliveryChannel中的。

有关 S AWS DK 开发者指南和代码示例的完整列表，请参阅AWS Config 与 AWS SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

文档历史记录

下表描述了文档的重要更改 AWS Config。要获得本文档的更新通知，您可以订阅 RSS 源。

- API 版本：2014-11-12
- 最新文档更新：2024 年 6 月 17 日

变更	说明	日期
安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在授予亚马逊弹性文件系统（亚马逊 EFS）、亚马逊 Redshift 和的额外权限。 适用于 SAP 的 AWS Systems Manager有关更多信息，请参阅适用于 AWS Config的AWS托管策略。	2024年6月17日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • cloudtrail-s3 bucket-bucket-禁止公共访问 • cloudtrail-s3 存储桶访问日志	2024 年 5 月 8 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则：i am-external-access-analyzer 启用	2024年5月2日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • 已启用 guardduty 恶意软件防护 • 已启用 guardduty-rds 保护	2024 年 4 月 26 日

	• 已启用 guardduty-s3 保护 • 已启用 inspector-lambda 标准扫描功能	
AWS Config 通过 Amazon 简化使用情况分析 CloudWatch	在此版本中，用于监控 AWS Config 数据使用情况的 Amazon CloudWatch 指标将仅显示可计费的使用量。这意味着，向控制台发送的 Amazon CloudWatch 指标中将不再显示不可计费的使用量。 AWS Config AWS Config 这使您可以使用 Amazon CloudWatch 指标验证 AWS Config 设置和使用情况，并将计费用量与相关费用关联起来。有关更多信息，请参阅AWS Config 使用情况和成功指标。	2024 年 4 月 26 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则：i am-server-证书到期-检查	2024 年 4 月 23 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • vpc-sg-port 限制检查 • cloudtrail-all-write-s3 数据事件检查 • cloudtrail-all-read-s3 数据事件检查	2024 年 4 月 17 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • 已启用 guardduty-eks 保护审计 • 启用 guardduty-eks 保护运行时 • 启用 guardduty-lambda 保护 • 已启用 inspector-ec2-scan • 支持 inspector-ecr-scan • 已启用 inspector-lambda 代码扫描功能 • redshift-不受限制的端口访问权限	2024 年 4 月 16 日
AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则：ef s-mount-target-public 可访问	2024 年 3 月 20 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • 已启用 dms-neptune-iam 授权 • 已启用 dms-mongo-db 身份验证 • 启用 dms-redis-tls • dax-tls-端点加密 • eks集群密钥已加密 • kinesis-firehose-delivery-stream 加密 • 已启用 mq-cloudwatch 审计日志 • 已启用 mq-cloudwatch 审计日志 • opensearch 主节点容错能力 • sagemaker 端点配置产品实例计数 • 组织内共享的服务目录 • 传输家庭服务器没有 FTP	2024 年 2 月 26 日

安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为Prometheus、亚马逊、Amazon Cognito、亚马逊、亚马逊 FSx、（IAM）CloudWatch、、、、Amazon Redshift Serverless、亚马逊和亚马逊 ElastiCache 简单通知服务 AWS Identity and Access Management (Amazon SNS) Simple AWS Glue Notification Serverless AWS Lambda、 AWS RAM亚马逊和 SageMaker亚马逊简单通知服务 (Amazon SNS) 授予了额外的权限。有关更多信息，请参阅适用于 AWS Config 的AWS 托管策略。	2024年2月22日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则：s 3-bucket-启用跨区域复制	2024 年 2 月 12 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新的、Amazon CloudWatch Evidently AWS Identity and Access Management (IAM) AWS AppConfig、适用于 Redis 的 Amazon MemoryDB (MemoryDB)、适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK）、亚马逊 Redshift 和资源类型的配置更改。 AWS Transfer Family 有关更多信息，请参阅支持的资源类型。	2024年2月6日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则：mac ie-auto-sensitive-data-discovery-check	2024 年 1 月 29 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新亚马逊、()、亚马逊 AppStream关系数据库服务 AWS Key Management Service (Amazon RDS AWS KMS)、Amazon Cognito、亚马逊弹性计算云 (Amazon EC2)、EC2 Image Builder、、、、亚马逊 AWS Ground Station AWS Mainframe Modernization、Amazon QuickSight Redshift 和资源类型的配置更改。 AWS Systems Manager 有关更多信息，请参阅支持的资源类型。	2024 年 1 月 3 日

根据每个账户每个区域的最大 AWS Config 规则数，服务限制会提高	在此版本中，每个账户 AWS Config 支持每个 AWS 区域的 1000 AWS Config 条规则。这一增长适用于所有已部署规则的总数，包括每个账户每个区域的 AWS Config 托管规则、 AWS Config 自定义规则、 AWS Config 一致性包、 AWS Security Hub 控件、 AWS Firewall Manager 策略和 AWS Backup 备份计划。有关更多信息，请参阅 Service Limits。	2023 年 12 月 19 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • s3-meets-restore-time-target • ebs-meets-restore-time-target • ec2-meets-restore-time-target • rds-meets-restore-time-target • efs-meets-restore-time-target • fsx-meets-restore-time-target • aurora-meets-restore-time-target • dynamodb-meets-restore-time-target	2023 年 12 月 19 日

安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为适用于 Prometheus 的亚马逊托管服务 AWS AppConfig、()、AWS DMS() IAM AWS Database Migration Service、适用于 Apache Kafka 的亚马逊托管流媒体（AWS Identity and Access Management亚马逊 MSK）、亚马逊 AWS Organizations日志和亚马逊简单存储服务 (Ama CloudWatch zon S3) 授予额外权限。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 12 月 5 日
预览版：适用于高级查询的自然语言查询处理器	在此版本中，您可以使用自然语言查询处理器进行高级查询，该处理器使用生成式人工智能（生成人工智能）功能，允许您用通俗易懂的英语提问并将其转换为 ready-to-use 查询格式。使用自然语言查询处理器，您可以对您的组织 AWS 账户 或整个 AWS 组织进行查询。有关更多信息，请参阅适用于高级查询的自然语言查询处理器。	2023 年 11 月 26 日

定期记录	在此版本中， AWS Config 支持定期录制。定期记录让您能够捕获固定时间段内资源的最新配置更改。现在，您可以将配置记录器的默认频率设置为“每日”，这样您将能够收到代表过去 24 小时内资源的最新状态的配置项 (CI)，前提是它与之前记录的 CI 不同。 AWS Config 控制台还引入了全新的录制策略体验，您还可以在其中覆盖特定资源类型的录制频率或将特定资源类型排除在录制范围之外。这有助于您的设置符合精细要求。 将添加以下数据类型： • RecordingMode • RecordingMode覆盖 将更新以下数据类型： • PutConfiguration录音机 • ConfigurationRecorder • BaseConfiguration物品 • ConfigurationItem 将更新开发人员指南中的以下页面： • 重新编码资源 AWS • 使用 AWS Config 控制台 AWS Config 进行设置 | 一键设置	2023 年 11 月 26 日

- 使用 AWS Config 控制台 AWS Config 进行设置 | 手动设置
- 使用 AWS CLI AWS Config 进行设置

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为亚马逊 Cognito、Amazon Connect、亚马逊 EMR、、、适用于 Redis 的 Amazon MemoryDB AWS Ground Station、、 AWS Mainframe Modernization亚马逊、亚马逊 AWS Organizations关系数据库服务（亚马逊 RDS）、QuickSight亚马逊 Redshift、Amazon Route 53 和授予额外权限。 AWS Service Catalog AWS Transfer Family 现在，AWSConfigServiceRolePolicy 策略和 AWS_ConfigRole 策略还为 AWSConfigServiceRolePolicyStatementID 、AWSConfigSLRLogStatementID 、AWSConfigSLRLogEventStatementID 、AWSConfigSLRApiGatewayStatementID 和 AWSConfigServiceRolePolicy 策略添加了安全标识符 (SID)。 有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 11 月 17 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • acm-pca-root-ca-disabled • dynamodb-table-deletion-protection-enabled • ec2-client-vpn-connection-log-enabled • eks-cluster-log-enabled • emr-block-public-access • fsx-windows-audit-log-configured • fsx-openzfs-copy-tags-enabled • fsx-lustre-copy-tags-to-backups • msk-enhanced-monitoring-enabled • mq-auto-minor-version-upgrade-enabled • neptune-cluster-multi-az-enabled • opensearch-update-check • s3-access-point-in-vpc-only • s3-access-point-public-access-blocks • s3-bucket-mfa-delete-enabled	2023 年 11 月 9 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新的 AWS Identity and Access Management (IAM)、()、、Amazon Connect AWS Network Manager、亚马逊弹性计算云 AWS Private Certificate Authority (Amazon EC2 AWS Private CA) AWS App Mesh、亚马逊弹性容器服务 (Amazon ECS)、、、适用于 Apache Kafka Streaming 的亚马逊托管流媒体 Kafka Connect（亚马逊 MSK Connect） AWS IoT和资源的配置更改类型。 AWS IoT TwinMaker AWS Lambda AWS 资源探索器 有关更多信息，请参阅支持的资源类型。	2023 年 11 月 3 日
AWS Config 支持新的一致性包	在此版本中， AWS Config 更新了以下一致性包：BNM RMiT 的运营最佳实践	2023 年 10 月 26 日

聚合器的合规性和清单控制面板	在此版本中，在控制台的聚合视图中 AWS Config 添加了合规性控制面板页面和库存 AWS Config 控制面板页面。 在合规性控制面板页面中，您可以查看带有小组件的自动控制面板，这些小组件总结了对聚合器中资源合规性的见解，例如按不合规资源列出的排名前 10 的资源类型，按不合规规则列出的排名前 10 的账户级别合规包等。 在清单控制面板页面中，您可以查看带有小组件的自动控制面板，这些小组件总结了对聚合器中资源配置数据的见解，例如按资源计数列出的排名前 10 的资源类型，按资源计数列出的排名前 10 的账户等。 有关图表的信息，请参阅合规性控制面板和清单控制面板。	2023 年 10 月 23 日

安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为、、Amazon Connect AWS Private CA、 AWS App Mesh亚马逊弹性容器服务 (Amazon ECS)、Amazon Evicently、Amazon Managed Grafana、 CloudWatch 亚马逊、Amazon Insp AWS IoT TwinMaker ector、、、、A GuardDuty mazon Kafka Managed Streaming（ AWS IoT亚马逊 MSK）、、、亚马逊托管流媒体（亚马逊 MSK）、、、和亚马逊授予额外权限。 AWS Lambda AWS Network Manager AWS Organizations SageMaker有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 10 月 4 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对适用于 Apache Kafka（亚马逊 MSK）、亚马逊 AWS IoT AWS IoT TwinMaker AWS IoT Wireless、亚马逊和 Amazon Inspector 的新、、、Amazon SageMaker、Amazon 和 Amazon Inspector 资源类型的 AWS CodeBuild亚马逊个性化亚马逊托管流媒体的配置更改。 AppStream有关更多信息，请参阅支持的资源类型。	2023 年 10 月 4 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • docdb-cluster-deletion-protection-enabled • docdb-cluster-audit-logging-enabled • docdb-cluster-snapshot-public-prohibited • mq-active-deployment-mode • mq-rabbit-deployment-mode • dms-auto-minor-version-upgrade-check • dms-replication-task-target db-logging • dms-replication-task-source db-logging • dms-endpoint-ssl-configured • custom-eventbus-policy-attached • global-endpoint-event-replication-enabled • route53-query-logging-enabled • rds-aurora-mysql-audit-logging-enabled • rds-cluster-auto-minor-version-upgrade-enable • appsync-authorization-check • netfw-deletion-protection-enabled • wafv2-rulegroup-logging-enabled	2023 年 9 月 21 日

	• msk-in-cluster-node-require-tls	
AWS Config 支持新的一致性包	在此版本中， AWS Config 更新了以下一致性包： • Amazon S3 操作最佳实践 • EC2 操作最佳实践	2023 年 9 月 8 日
安全 IAM 更新	该`AWSConfigServiceRolePolicy` 策略现在会移除 AWS Systems Manager （Systems Manager）的权限。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 9 月 6 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新的 Amazon P CodeGuru rofiler、、 AWS Elemental MediaConnect AWS Transfer Family、Prom AWS Batch etheus 的亚马逊托管服务、、和资源类型的配置更改。 AWS Cloud Map Amazon Route 53 Resolver 有关更多信息，请参阅支持的资源类型。	2023 年 9 月 6 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • athena-workgroup-encrypted-at-rest • neptune-cluster-iam-database-authentication • neptune-cluster-copy-tags-to-snapshot-enabled • neptune-cluster-cloudwatch-log-export-enabled • neptune-cluster-deletion-protection-enabled • neptune-cluster-snapshot-encrypted • neptune-cluster-backup-retention-check • neptune-cluster-encrypted • neptune-cluster-snapshot-public-prohibited • docdb-cluster-backup-retention-check • docdb-cluster-encrypted • rds-cluster-encrypted-at-rest	2023 年 8 月 10 日

AWS Config 支持新的资源类型	在这个版本中，你可以 AWS Config 用来记录对新的、亚马逊、、亚马逊 Athena AWS Amplify AppIntegrations AWS App Mesh、亚马逊弹性计算云 (Amazon EC2) CloudWatch 、亚马逊 Evicently、Amazon Forecast、、、、、、、、Amazon Man AWS IoT Greengrass Version 2 aged Streaming（亚马逊 MSK）AWS Elemental MediaTailor、亚马逊个性化、亚马逊 Pinpoint 的配置更改资源类型。AWS Ground Station AWS Elemental MediaConvert AWS Resilience Hub 有关更多信息，请参阅支持的资源类型。	2023 年 8 月 3 日

安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为亚马逊 AppStream 2.0、、亚马逊、、、Amazon Connect AWS App Mesh、、亚马逊 AWS CloudFormation、 AWS Identity and Access Management (IAM) CloudFront AWS CodeArtifact AWS CodeBuild、Amazon Inspector GuardDuty、、、、、Amazon Macie AWS IoT、、 AWS IoT TwinMaker、 AWS IoT Wireless、、Amazon Route 53、亚马逊简单存储服务 (Amazon S3) 的亚马逊托管流媒体授予额外权限 AWS Elemental MediaConnect AWS Network Manager AWS Organizations AWS 资源探索器、亚马逊简单通知服务 (Amazon SNS) Semple Notification Service 和亚马逊 EC2 系统 AWS Glue经理 (SSM)。有关更多信息，请参阅适用于 AWS Config的AWS托管策略。	2023 年 7 月 28 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对全新 Amazon Kinesis、亚马逊弹性计算云 (Amazon EC2)、亚马逊 Pinpoint、亚马逊简单存储服务 (亚马逊 S3)、亚马逊虚拟私有云 (亚马逊 VPC)、亚马逊 Kendra、Amazon C AWS AppConfig onnect AWS App Mesh、、、、、 AWS CloudFormation和 () 资源类型。 AWS App Runner AWS Database Migration Service AWS DMS有关更多信息，请参阅支持的资源类型。	2023 年 7 月 10 日
组织合规包的服务限制有所增加	在此版本中， AWS Config 支持所有合 AWS Config 规包中每个账户的每个区域 350 条规则，每个组织支持 350 AWS Config 条组织规则。有关更多信息，请参阅 Service Limits。	2023 年 6 月 13 日

安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为亚马逊托管工作流程、Amazon Connect、Prometheus 的亚马逊托管服务 AWS Amplify、Amazon Athena AWS App Mesh、、、、、、、、、Amazon DynamoDB、Amazon Elastic Compute Cloud（AWS Batch Amazon EC2）AWS CloudFormation AWS CloudTrail AWS CodeArtifact、Amazon Evisently CodeGuru AWS Directory Service、Amazon Forecast、、、、（IA AWS Ground Station M）授予额外权限，适用于 Apache Kafka 的亚马逊托管流媒体 Kafka（亚马逊 MSK） CloudWatch 、亚马逊 Lightsail AWS Organizations AWS IoT Greengrass、A AWS Identity and Access Management mazon Lightsail、Amazon Logs、 ， CloudWatch AWS Elemental MediaConnect AWS Elemental MediaTailor、亚马逊 Pinpoint、亚马逊虚拟私有云（亚马逊 VPC）、Amazon Personalize、亚马逊 QuickSight、、AWS Migration Hub Refactor	2023 年 6 月 13 日

Spaces亚马逊简单存储服务（亚马逊 S3）Simple Storage Service、亚马逊和。SageMaker AWS Transfer Family有关更多信息，请参阅适用于 AWS Config的AWS托管策略。

AWS Config 按资源类型记录排除项	在此版本中， AWS Config 您可以将特定类型的 AWS 资源排除在库存跟踪和合规性监控之外，同时仍可以跟踪中当前可用的所有其他受支持的资源类型 AWS Config，包括将来将要添加的资源类型。您可以使用此功能将注意力集中在受合规性和监管标准约束的关键资源上。 配置记录器和录制组的 API 更新向后兼容，这意味着它们可以与以前版本的 PutConfigurationRecorder API 一起使用。您可以继续以与以前完全相同的方式管理记录哪些资源类型，而无需使用更新后的或新的 API。 将添加以下数据类型： • RecordingStrategy • ExclusionByResourceTypes 将更新以下数据类型： • PutConfiguration录音机 • ConfigurationRecorder • RecordingGroup 将更新开发人员指南中的以下页面： • 选择所记录的资源	2023 年 6 月 9 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新亚马逊弹性容器服务 (Amazon ECS)、亚马逊密钥空间（适用于 Apache Cassandra）（亚马逊密钥空间）、、、、、、亚马逊 2.0、、、亚马逊弹性计算云 (Amazon EC2 AWS Amplify) AWS App Mesh AWS App Runner、Amazon Evisently AppStream 、AWS CodeArtifact Amazon Forecast、(IAM) Amazon 的配置更改 Pinpoint CloudWatch 、Amazon、Amazon Data Firehose 资源类型。AWS Signer AWS Identity and Access Management SageMaker AWS Transfer Family有关更多信息，请参阅支持的资源类型。	2023 年 6 月 5 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • cloudfront-s3-origin-access-control-enabled • custom-schema-registry-policy-attached • ec2-client-vpn-not-authorize-all • elasticache-supported-engine-version • macie-status-check • mq-automatic-minor-version-upgrade-enabled • mq-cloudwatch-audit-logging-enabled • netfw-logging-enabled • opensearch-encrypted-at-res • step-functions-state-machine-logging-enabled	2023 年 5 月 10 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新的、亚马逊弹性计算云 (Amazon EC2) Amazon Route 53 Resolver、无线、、、、、亚马逊、Redshift AWS IoT 、A AppFlow mazon Pinpoint AWS Network Manager AWS Device Farm AWS Ground Station、、、、EC2 Image Builder、Amazon AWS IoT、Amazon Runtime AWS Panorama、 CloudWatch Amazon AWS AppConfig SageMaker ECR 和资源类型的配置更改。 AWS Audit Manager 有关更多信息，请参阅支持的资源类型。	2023 年 5 月 5 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对的配置更改`AWS::NetworkFirewall::TLSInspectionConfiguration` 。有关更多信息，请参阅支持的资源类型。	2023 年 5 月 1 日

安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在授予亚马逊托管工作流程的额外权限，包括、、、亚马逊 AWS Amplify、 AWS App Mesh、 AWS App Runner亚马逊 Elastic Compute Cloud CloudFront AWS CodeArtifact、Amazon Kendra、Amazon Macie、亚马逊 Route 53、亚马逊 Pinpoint、、SageMaker Resilience Hub、亚马逊 AWS Migration Hub AWS 、Di AWS rectory Service 和。 AWS Transfer Family CloudWatch AWS WAF 有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 4 月 13 日

AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • elasticache-auto-minor-version-upgrade-check • elasticache-repl-grp-auto-failover-enabled • elasticache-repl-grp-encrypted-at-rest • elasticache-repl-grp-encrypted-in-transit • elasticache-repl-grp-redis-auth-enabled • elasticache-subnet-group-check • cloudfront-s3-origin-non-existent-bucket	2023 年 4 月 10 日
组织合规包的服务限制有所增加	在此版本中，所有组织一致性包 AWS Config 支持每个账户 350 AWS Config 条规则。有关更多信息，请参阅 Service Limits。	2023 年 4 月 3 日

AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • acm-certificate-rsa-check • appsync-associated-with-waf • appsync-logging-enabled • elasticache-rbac-auth-enabled • mq-no-public-access • netfw-multi-az-enabled • ses-malware-scanning-enabled • eks-cluster-logging-enabled • appsync-cache-encryption-at-rest	2023 年 4 月 3 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新亚马逊 AppStream 2.0、A AWS uto Scaling、Amazon Connect 亚马逊弹性计算云、亚马逊、、Kinesis 视频流 EventBridge HealthLake、Lookout for Vision AWS IoT TwinMaker、网络管理器、亚马逊 Pinpoint、亚马逊 Route 53 应用程序恢复控制器和资源类型的配置更改。 AWS RoboMaker 有关更多信息，请参阅支持的资源类型。	2023 年 4 月 3 日

安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为亚马逊、亚马逊 AppStream 2.0、、亚马逊、亚马逊 AppFlow、、亚马逊、、、 AWS App Runner、亚马逊弹性计算云 (Amazon EC2) CloudFront CloudWatch AWS CodeArtifact AWS CodeCommit、Amazon Evicently AWS Device Farm、Amazon Forecast、(IAM)、、、A CloudWatch mazon MemoryDB for Redis AWS IoT、Amazon Pinpoint、、亚马逊关系 AWS Panorama 数据库服务 (亚马逊) 授予额外权限 RDS)、 AWS Network Manager亚马逊 Redshift 和亚马逊。 AWS CloudFormation AWS Ground Station AWS Identity and Access Management SageMaker有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 3 月 30 日
安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` `AWS_ConfigRole` 策略和策略授予的额外权限 AWS Audit Manager。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 3 月 3 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新的、亚马逊、、、（亚马逊简单存储服务 (Amazon S3) AWS Elemental MediaPackage EventBridge AWS IoT、亚马逊弹性计算云 (Amazon EC2)、Amazon Lookout for Metrics、Amazon Lex、、、、Amazon Reviewer 和资源类型的配置更改。 AWS Budgets AWS Device Farm CodeGuru Amazon Route 53 Resolver AWS RoboMaker 有关更多信息，请参阅支持的资源类型。	2023 年 3 月 2 日
安全 IAM 更新	AWS Config 现在可以跟踪`AWSConfigMultiAccountSetupPolicy` 策略的更改。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 2 月 27 日
AWS Config 按地区可用性划分的资源覆盖率	在此版本中， AWS Config 为每种支持的资源类型提供了区域信息。有关哪些区域支持哪些资源类型的信息，请参阅按区域可用性列出的资源覆盖范围。	2023 年 2 月 20 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新的亚马逊互动视频服务 (Amazon IVS)、亚马逊简单存储服务 (Amazon AWS Glue S3)、亚马逊 Elastic Kubernetes 服务 (Amazon EKS)、亚马逊 AWS IoT关系数据库服务 (Amazon RDS) 和 Apache Flink 托管服务资源的配置更改类型。有关更多信息，请参阅支持的资源类型。	2023 年 2 月 7 日
安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为Apache Airflow、Amazon AppStream 2.0、Amazon CodeGuru Reviewer、 AWS IoT Amazon Kinesis Video Streams AWS HealthLake、亚马逊 Route 53 应用程序恢复控制器、亚马逊弹性计算云 (Amazon EC2) AWS Device Farm、亚马逊 Pinpoint、AWS Identity and Access Management (IAM)、亚马逊和亚马逊日志的托管工作流程授予额外权限。 GuardDuty CloudWatch 有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 2 月 1 日

安全 IAM 更新	作为安全最佳实践，`ConfigConformsServiceRolePolicy` 策略现在取消了对 `config:DescribeConfigRules` 的广泛资源级别权限。有关更多信息，请参阅适用于 AWS Config 的AWS 托管策略。	2023 年 1 月 12 日
安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为亚马逊托管服务 Prometheus AWS Audit Manager、、、、、、、、、、 AWS Device Farm Amazon Elastic Compute Cloud AWS Database Migration Service (Amazon EC2 AWS DMS) AWS Directory Service、、、、Amazon Lightsail、AWS Glue、、、 AWS IoT 亚马逊 Route 53 应用程序恢复控制器 AWS Elemental MediaPackage AWS Network Manager AWS Resource Access Manager、 QuickSight亚马逊简单存储服务 (Amazon S3) 和亚马逊 Timestream 授予额外权限。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2023 年 1 月 10 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新亚马逊 MQ、、、亚马逊 EventBridge 架构、 AWS AppConfig Amazon Fraud Detector、、、Amazon AWS IoT Analytics Lightsail AWS IoT、(AWS Elemental MediaPackage) MediaPackage、Amazon Route 53 应用程序恢复控制器和资源类型的配置更改。AWS Cloud9 AWS Resilience Hub AWS Transfer Family 有关更多信息，请参阅支持的资源类型。	2023 年 1 月 5 日
AWS Config 规则资源覆盖范围	在此版本中， AWS Config 显示更多 AWS Config 托管规则的资源类型覆盖范围。	2022 年 12 月 21 日
AWS Config 规则可发现性	在此版本中， AWS Config 支持 “按评估模式划分的 AWS Config 托管规则列表”、“按触发器类型划分的 AWS Config 托管规则列表” 和 “按区域可用性划分的 AWS Config 托管规则列表” 的页面。	2022 年 12 月 21 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 更新了以下一致性包： • K-ISMS 操作最佳实践 • NIST 800 171 操作最佳实践 • PCI DSS 3.2.1 操作最佳实践 • Esquema Nacional de Seguridad (ENS) High 操作最佳实践 • Esquema Nacional de Seguridad (ENS) Medium 操作最佳实践 • Esquema Nacional de Seguridad (ENS) Low 操作最佳实践 • NZISM 操作最佳实践 • NIST 800-53 rev 5 操作最佳实践	2022 年 12 月 19 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • api-gwv2-access-logs-enabled • api-gwv2-authorization-type-configured • cloudfront-security-policy-check • ec2-launch-template-public-ip-disabled • elastic-beanstalk-logs-to-cloudwatch • sagemaker-notebook-instance-inside-vpc • sagemaker-notebook-instance-root-access-check • security-account-information-provided • storagegateway-resources-protected-by-backup-plan • wafv2-rulegroup-not-empty • wafv2-webacl-not-empty	2022 年 12 月 9 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新的 Amazon CloudWatch RUM、亚马逊、亚马逊 EventBridge GuardDuty、亚马逊简单电子邮件服务 (Amazon SES) AWS Backup、 AWS DataSync、AWS Fault Injection Service 和 AWS FIS() 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 12 月 9 日

AWS Config 主动合规	在此版本中，AWS Config 支持在资源调配之前主动检查 AWS Config 规则的合规性。这允许您在创建或更新资源之前评估资源的配置设置。用于跟踪 AWS Config 对资源所做的配置更改（无论是预配置前还是置备后），并检查您的资源是否与所需的配置相匹配。 将添加以下数据类型： • GetResourceEvaluationSummary • StartResource评估 • ListResource评估 将更新以下数据类型： • DescribeConfigRulesFilters • GetComplianceDetailsBy资源 • EvaluationResult预选赛 • EvaluationMode配置 将更新开发人员指南中的以下页面： • AWS Config 规则的组成部分 • AWS Config 规则的评估模式和触发器类型 • AWS Config 托管规则 • AWS Config 自定义规则 • 管理您的 AWS Config 规则	2022 年 11 月 28 日

将偏差检测作为配置记录器的 AWS Config 配置项目 (CI)	在此版本中， AWS Config 跟踪对配置记录器的所有更改，以指示配置记录器的状态是否与其先前的状态不同或有所偏差；例如，是否有已启用 AWS Config 跟踪的资源类型的更新，是否已停止或启动配置记录器，或者是否已删除或卸载配置记录器。`AWS::Config::ConfigurationRecorder` 资源类型是系统资源类型，默认情况下 AWS Config ，所有支持的区域都启用了该资源类型的记录。`AWS::Config::ConfigurationRecorder` 资源类型的记录不收取额外费用。有关更多信息，请参阅配置记录器的偏差检测。	2022 年 11 月 18 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新、EC2 Image Builder AWS IoT Events、、AWS Cloud Map、Amazon Route 53 应用程序恢复控制器和亚马逊弹性容器注册表 (Amazon ECR) Elastic Registry 资源类型的配置更改。 AWS DataSync AWS Glue 有关更多信息，请参阅支持的资源类型。	2022 年 11 月 8 日

安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` `AWS_ConfigRole` 策略和策略授予的额外权限 AWS CloudFormation。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2022 年 11 月 7 日
AWS Config 支持新的一致性包	在此版本中， AWS Config 支持以下一致性包： • 刑事司法信息服务 (CJIS) 操作最佳实践 • Amazon 安全最佳实践 SageMaker • Amazon Elastic Container Registry 安全最佳实践 将更新以下合规包： • MAS TRMG 操作最佳实践 • NCSC 网络评估框架操作最佳实践 • NCSC 云安全原则操作最佳实践	2022 年 10 月 27 日

安全 IAM 更新	该AWSConfigServiceRolePolicy 政策和AWS_ConfigRole 政策现在为 Apache Airflow 的亚马逊托管工作流程 AWS Certificate Manager、、、Amazon Keyspaces、亚马逊、Amazon Connect、亚马逊弹性计算云 (Amazon EC2) AWS Amplify、AWS AppConfig亚马逊 Elastic Kubernetes Service（亚马逊 EKS）、亚马逊 AWS Glue DataBrew、、亚马逊 AWS Fault Injection Service欺诈探测器、亚马逊 FsX、Amazon Fraud Detector、Amazon FsX、Amazon FsX、Amazon Frud Detector、Amazon FsX、Amazon FsX、EventBridge Amazon FsX、Amazon、亚马逊、亚马逊定位 GameLift服务、、Amazon Lex、亚马逊 Lightsail、亚马逊 Pinpoint、、、、、 AWS IoT亚马逊、Amazon Relational CloudWatch AWS OpsWorks AWS Panorama AWS Resource Access Manager QuickSight数据库服务（亚马逊 RDS）、亚马逊 AWS RoboMaker Rekognition、、、Amazon Route 53 AWS Resource Groups、亚马逊简单存储服务 AWS Cloud Map(Amazon S3)、Amazon	2022 年 10 月 19 日

	Simple Storage Service 和。AWS Security Token Service 有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新的亚马逊弹性计算云 (Amazon EC2)、亚马逊简单电子邮件服务 (Amazon SES) AWS AppConfig、 AWS Cloud Map、和资源类型的配置更改。 AWS DataSync 有关更多信息，请参阅支持的资源类型。	2022 年 10 月 6 日
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录新的 Amazon GuardDuty、、 SageMaker AWS AppSync AWS Cloud Map、和 AWS DataSync 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 10 月 4 日
AWS Config 支持新的一致性包	在本版本中， AWS Config 更新了 SWIFT CSP 一致性包的运营最佳实践。	2022 年 10 月 4 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 支持以下一致性包： • CMMC 2.0 Level 1 操作最佳实践 • CMMC 2.0 Level 2 操作最佳实践 将更新以下合规包： • Amazon API Gateway 操作最佳实践 • Well-Architecte AWS d 框架可靠性支柱的运营最佳实践 • Well-Architecte AWS d Framework 安全支柱的最佳运营实践 • CMMC Level 1 操作最佳实践 • CMMC Level 2 操作最佳实践 • CMMC Level 3 操作最佳实践 • CMMC Level 4 操作最佳实践 • CMMC Level 5 操作最佳实践 • FFIEC 操作最佳实践 • FedRAMP(Low) 操作最佳实践 • MAS 第 655 号通知操作最佳实践 • NBC TRMG 操作最佳实践 • NIST 800 172 操作最佳实践	2022 年 9 月 30 日

安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` `AWS_ConfigRole` 策略和策略授予的额外权限 AWS Glue。有关更多信息，请参阅适用于 AWS Config 的AWS 托管策略。	2022 年 9 月 14 日
AWS Config 支持新的一致性包	在本版本中， AWS Config 支持 SWIFT CSP 一致性包的运营最佳实践。	2022 年 9 月 9 日

安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为亚马逊 AppFlow、亚马逊、亚马逊 R CloudWatch UM、Amazon Synth CloudWatch etics CloudWatch、Amazon Connect 客户档案、Amazon Connect 语音身份证、Amazon DevOps Guru、亚马逊弹性计算云 (Amazon EC2)、亚马逊 EC2 Auto Scaling、亚马逊 EMR、亚马逊、亚马逊架构、Amazon Fraud Detector、Amazon Fraud Detector、Amazon Fraud Detector、、Amazon EventBridge Fraud Detector、Amazon FinSpace亚马逊、亚马逊互动视频服务（亚马逊 IVS）Interactive Video Service GameLift、适用于 Apache Flink 的亚马逊托管服务、EC2 Image Builder、Amazon Lex、亚马逊 EventBridge Lightsail、亚马逊定位服务、亚马逊 Lookout for Equipment、亚马逊 Lookout for Metrics、亚马逊 Lookout for Vision、亚马逊托管区块链、亚马逊 MQ、 StudioAmazon 亚马逊 Nimble Pinpo QuickSight int、亚马逊 Route 53 Amazon Route 53 Resolver 应用程序恢复控制器、亚马逊简单存储服务（亚马逊	2022 年 9 月 7 日

S3）、亚马逊 SimpleDB、亚马逊简单电子邮件服务 (Amazon SES)、亚马逊 Timestream、、、

AWS Config 支持新的一致性包	在此版本中，AWS Config 支持以下一致性包： • Amazon 最佳运营实践 CloudWatch • 德国云计算合规性控制目录 (C5) 操作最佳实践 • IRS 1075 操作最佳实践 将更新以下合规包： • AWS Control Tower Detective Guardrails 一致性包 • CISA Cyber Essentials 操作最佳实践 • 适用于 SME 的 ENISA 网络安全指南操作最佳实践 • FDA 联邦法规第 21 篇第 11 部分操作最佳实践 • FedRAMP(Moderate) 操作最佳实践 • HIPAA 安全操作最佳实践 • NIST 隐私框架 v1.0 操作最佳实践 • NYDFS 23 操作最佳实践 • 印度储备银行 UCB 网络安全框架操作最佳实践 • RBI MD-ITF 操作最佳实践	2022 年 8 月 31 日

入门 AWS Config 和自定义一致性包更新	在此版本中， AWS Config 更新了 “控制台入门” AWS Config 和 “使用控制台 AWS Config 进行设置” 页面，引入了 “一键设置” 和 “手动设置” 页面。 AWS Config 还更新了自定义一致性包页面，其中包含有关如何从头开始创建一致性包 YAML 文件的演练。	2022 年 8 月 25 日
AWS Systems Manager 文档（SSM 文档）与一致性包集成	在此版本中，您可以使用 SSM 文档创建合规包模板。有关 SSM 文档的更多信息，请参阅《 AWS Systems Manager 用户指南》中的 AWS Systems Manager 文档。 将更新以下数据类型： • PutConformance包 • ConformancePack详情 • TemplatessSM DocumentDetails 将更新开发人员指南中的以下页面： • 使用控制台部署一致性包 AWS Config • 使用 AWS 命令行界面部署一致性包	2022 年 8 月 24 日

安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` 策略和`AWS_ConfigRole` 策略授予亚马逊简单电子邮件服务 (Amazon SES) AWS DataSync、 AWS Cloud Map 和的额外权限。有关更多信息，请参阅适用于 AWS Config 的AWS 托管策略。	2022 年 8 月 22 日
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录新的 Amazon Athena、Amazon Detective 、Amazon、Amazon Rout SageMaker e AWS Database Migration Service 53、()AWS DMS、() 和亚马逊简单电子邮件服务 (Amazon SES AWS Glue) AWS Key Managemen t Service Service (Amazon SES) 资源类型的配置更改 。AWS KMS有关更多信息，请参阅支持的资源类型。	2022 年 8 月 16 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 更新了以下一致性包： • NIST 1800 25 操作最佳实践 • NIST 800 181 操作最佳实践 • ABS CCIG 2.0 标准工作负载操作最佳实践 • ABS CCIG 2.0 重要工作负载操作最佳实践 • ACSC Essential 8 操作最佳实践 • ACSC ISM 操作最佳实践 • APRA CPG 234 操作最佳实践 • CIS AWS 基金会运营最佳实践基准 v1.4 第 1 级 • CIS AWS 基金会运营最佳实践基准 v1.4 第 2 级 • BNM RMiT 操作最佳实践 • NIST CSF 操作最佳实践	2022 年 8 月 1 日

合规包的合规性分数	在此版本中，AWS Config 引入了一致性包的合规性分数，它使您能够从高层次了解合规包的合规性状态。您可以使用此分数来识别、调查和了解合规包中的合规性级别。合规性分数是合规包中的合规规则资源组合数量与合规包中可能的规则资源组合总数的百分比。 将更新以下数据类型： • ListConformancePackCompliance分数 • ConformancePackComplianceScore 将更新开发人员指南中的以下页面： • 查看 AWS Config 控制面板 • 在“合规包”控制面板中查看合规性数据 • 管理合规包 (API)	2022 年 7 月 26 日
安全 IAM 更新	该`ConfigConformsServiceRolePolicy` 政策现在授予向亚马逊发布指标数据点的权限 CloudWatch。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2022 年 7 月 25 日

安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为亚马逊弹性容器服务 (Amazon ECS)、亚马逊、亚马逊、亚马逊 FSx、适用于 A ElastiCache pache Flink 的亚马逊托管服务、亚马逊定位服务、适用于 Apache Kafka 的亚马逊托管流媒体、亚马逊、亚马逊 Rekognition、 QuickSight亚马逊简单存储服务授予额外权限（亚马逊 S3) AWS RoboMaker、亚马逊简单电子邮件服务 (Amazon SES)、、、、、、、、、、、、、、（IAM 身份中心 AWS Amplify） AWS AppConfig、EC2 Image Bu AWS AppSync il AWS Billing Conductor der、 EventBridge AWS DataSync AWS Firewall Manager AWS Glue AWS IAM Identity Center 和 Elastic Load Balancing 有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2022 年 7 月 15 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新的亚马逊弹性计算云 (Amazon EC2) 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 7 月 8 日

AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新 AWS Global Accelerator 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 7 月 5 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • autoscaling-launch-template • ecs-task-definition-log-configuration • ecs-awsvpc-networking-enabled • nlb-cross-zone-load-balancing-enabled	2022 年 7 月 1 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 支持以下一致性包： • 加拿大网络安全中心 (CCCS) Medium Cloud Control Profile 操作最佳实践 • 《格雷姆-里奇-布里利法案》(GLBA) 操作最佳实践 • GxP 欧盟附件 11 操作最佳实践 • Amazon Elastic Kubernetes Service (Amazon EKS) 安全最佳实践 • Amazon Relational Database Service (Amazon RDS) 安全最佳实践 • 的安全最佳实践 AWS Lambda 将更新以下合规包： • 人工智能和机器学习操作最佳实践 • Amazon DynamoDB 操作最佳实践 • CIS 关键安全控制 v8 IG1 操作最佳实践 • CIS 关键安全控制 v8 IG2 操作最佳实践 • CIS 关键安全控制 v8 IG3 操作最佳实践 • HIPAA 安全操作最佳实践 • NIST 800-53 rev 5 操作最佳实践	2022 年 6 月 30 日

	• NIST CSF 操作最佳实践	
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录新 Amazon SageMaker 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 6 月 29 日
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录适用于Apache Kafka（亚马逊 MSK）、亚马逊 Route 53、亚马逊、（IAM Access AWS Database Migration Service Analyzer） WorkSpaces、AWS Batch(AWS DMS) 和 Elastic Load Balancing 的新资源类型的配置更改。AWS Identity and Access Management Access Analyzer AWS Step Functions有关更多信息，请参阅支持的资源类型。	2022 年 6 月 14 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • aurora-last-backup-recovery-point-created • dynamodb-last-backup-recovery-point-created • ebs-last-backup-recovery-point-created • ec2-last-backup-recovery-point-created • efs-last-backup-recovery-point-created • fsx-last-backup-recovery-point-created • rds-last-backup-recovery-point-created • s3-last-backup-recovery-point-created • storagegateway-last-backup-recovery-point-created • virtualmachine-last-backup-recovery-point-created	2022 年 6 月 13 日

AWS Config 与集成 AWS Security Hub	在此版本中，您可以在中查看 AWS Config 托管规则和自定义规则评估的结果 AWS Security Hub。Security Hub 会将规则评估转化为结果，从而提供有关受影响资源的更多信息，例如 Amazon 资源名称 (ARN) 和创建日期。这些结果可以与 Security Hub 的其他发现一起查看，提供您的安全态势的全面概述。有关更多信息，请参阅将规则评估发送到 Security Hub	2022 年 6 月 7 日
安全 IAM 更新	该`AWSConfigServiceRolePolicy` 政策和`AWS_ConfigRole` 政策现在为亚马逊 Athena、Amazon Detective、亚马逊、亚马 GuardDuty逊 Macie、亚马逊简单电子邮件服务 (Amazon AWS Glue S AWS Resource Access Manager ES)、、() 和授予额外权限。AWS RAM AWS IAM Identity Center有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2022 年 5 月 31 日

AWS Config 支持新的一致性包	在此版本中， AWS Config 支持以下一致性包： • Amazon Elastic Container Service (Amazon ECS) 安全最佳实践 • Amazon Elastic File System (Amazon EFS) 安全最佳实践 • Amazon 安全最佳实践 CloudFront • 的安全最佳实践 AWS Auto Scaling • 的安全最佳实践 AWS Network Firewall • 的安全最佳实践 AWS Secrets Manager	2022 年 5 月 31 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新 Amazon SageMaker 和 AWS Step Functions 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 5 月 26 日
AWS Config 支持新的一致性包	在此版本中， AWS Config 更新了 NERC CIP BCSI 一致性包的操作最佳实践。	2022 年 5 月 20 日

AWS Config 规则的组成部分	在此版本中，AWS Config 引入了 “AWS Config 规则组件” 页面。该页面讨论了规则定义的结构、规则元数据以及如何使用规则开发套件 (RDK) 和 AWS Config 规则开发套件库 (RDKLib) 使用 Python 编写 AWS Config 规则的最佳实践。	2022 年 5 月 9 日
组织合规包的服务限制有所增加	在此版本中，AWS Config 支持所有组织一致性包中每个账户 180 AWS Config 条规则。有关更多信息，请参阅 Service Limits。	2022 年 5 月 6 日
AWS Config 支持新的一致性包	在此版本中，AWS Config 支持以下一致性包： • Amazon OpenSearch 服务安全最佳实践 • Amazon Redshift 安全最佳实践 • 的安全最佳实践 AWS CloudTrail • 的安全最佳实践 AWS CodeBuild • 的安全最佳实践 AWS WAF	2022 年 4 月 29 日
AWS Config 更新托管规则	在此版本中，AWS Config 支持 s3 资源受备份计划保护的托管规则。	2022 年 4 月 11 日

安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` `AWS_ConfigRole` 策略和策略授予其他权限，以获取有关所有或指定 AWS CloudTrail 事件数据存储 (EDS) 的信息，获取有关所有或指定 AWS CloudFormation 资源的信息，获取 DynamoDB Accelerator (DAX) 参数组或子网组的列表，获取 AWS Database Migration Service 有关当前正在访问的区域中您的账户的AWS DMS() 复制任务的信息，以及获取指定类型的所有策略的列表。 AWS Organizations 有关更多信息，请参阅适用于 AWS Config的 AWS 托管策略。	2022 年 4 月 7 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • alb-desync-mode-check • autoscaling-capacity-rebalancing • autoscaling-launchconfig-requires-imdsv2 • autoscaling-launch-config-hop-limit • autoscaling-multiple-instance-types • clb-desync-mode-check • ecs-container-insights-enabled • ecs-fargate-latest-platform-version • netfw-policy-default-action-fragment-packets • netfw-policy-default-action-full-packets • netfw-policy-rule-group-associated • redshift-audit-logging-enabled • s3-lifecycle-policy-check • waf-regional-rule-not-empty • waf-regional-rulegroup-not-empty • waf-regional-webacl-not-empty • vpc-peering-dns-resolution-check	2022 年 4 月 22 日

AWS Config 自定义策略规则	在此版本中，AWS Config 允许您使用 AWS CloudFormation Guard（guard）创建 AWS Config 自定义策略规则。Guard 是一种允许您编写由其强制执行的策略的 policy-as-code 语言，AWS Config 而无需创建 Lambda 函数来管理您的自定义规则。使用 Guard 策略编写的规则可以从 AWS Config 控制台创建，也可以使用 AWS Config 规则 API 创建。 将更新开发人员指南中的以下页面： • AWS Config 自定义规则 • 使用 Guard 创建 AWS Config 自定义规则 将更新以下数据类型： • 源 • CustomPolicy详情 • ConfigRuleEvaluationStatus • GetCustomRulePolicy • GetOrganizationCustomRule政策 • OrganizationCustomPolicyRule元数据	2022 年 4 月 22 日

AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录新 Amazon EMR SecurityConfiguration 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 3 月 31 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持虚拟机资源受备份计划保护的托管规则。	2022 年 3 月 29 日
AWS Config 与 Amazon CloudWatch 指标集成	在此版本中， AWS Config 现在支持在 AWS Config 控制面板页面 CloudWatch 中 AWS Config 使用亚马逊跟踪您的使用情况和成功指标。CloudWatch metrics 是一项监控服务，可提供有关系统性能的数据，包括根据有关 AWS 资源的指标进行搜索、绘制图表和生成警报的能力。在 AWS Config 控制面板中，您可以看到哪些流量推动了您的 AWS Config 使用量，以及工作流程中出现的故障的关键指标。 将更新以下页面： • 查看 AWS Config 控制面板	2022 年 3 月 29 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新 Amazon Det GuardDuty ector 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 3 月 24 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • clb-multiple-az • cloudfront-no-deprecated-ssl-protocols • cloudfront-traffic-to-origin-encrypted • cloudwatch-alarm-action-enabled-check • ec2-no-amazon-key-pair • ec2-paravirtual-instance-check • ec2-token-hop-limit-check • ec2-transit-gateway-auto-vpc-attach-disabled • ecr-private-lifecycle-policy-configured • efs-access-point-enforce-root-directory • efs-access-point-enforce-user-identity • elbv2-multiple-az • kinesis-stream-encrypted • redshift-default-db-name-check • s3-event-notifications-enabled • sns-topic-message-delivery-notification-enabled • waf-global-rulegroup-not-empty • waf-global-rule-not-empty	2022 年 3 月 23 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 更新了以下一致性包： • CIS 关键安全控制 v8 IG1 操作最佳实践 • CIS 关键安全控制 v8 IG2 操作最佳实践 • CIS 关键安全控制 v8 IG3 操作最佳实践 • Well-Architecte AWS d Framework 安全支柱的最佳运营实践 • Esquema Nacional de Seguridad (ENS) Low 操作最佳实践 • Esquema Nacional de Seguridad (ENS) Medium 操作最佳实践 • Esquema Nacional de Seguridad (ENS) High 操作最佳实践 • MAS 第 655 号通知操作最佳实践 • NIST 1800-25 操作最佳实践	2022 年 3 月 16 日
安全 IAM 更新	`AWSConfigServiceRolePolicy` 策略和 `AWS_ConfigRole` 策略现在授予 AWS CloudFormation的更多权限。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2022 年 3 月 14 日

AWS Config 更新托管规则	在此版本中， AWS Config 更新了以下托管规则： • aurora-resources-protected-by-backup-plan • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	2022 年 3 月 10 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新 Amazon Elastic Container Registry 公共资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 3 月 4 日
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录新的 Amazon 弹性计算云资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 2 月 28 日

AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • codedeploy-auto-rollback-monitor-enabled • codedeploy-ec2-minimum-healthy-hosts-configured • codedeploy-lambda-allatonce-traffic-shift-disabled	2022 年 2 月 25 日
AWS Config 更新中的日志和监控	在此版本中， AWS Config 更新了 “AWS Config 使用亚马逊 EventBridge 事件监控” 页面，以取代对亚马逊 CloudWatch 事件的引用。亚马逊 EventBridge 是管理您的活动的首选方式。 CloudWatch 事件和 EventBridge 是相同的底层服务和 API，但 EventBridge 提供了更多功能。您在 CloudWatch 或中所做的更改 EventBridge 将显示在每个主机中。有关更多信息，请参阅 Amazon EventBridge。	2022 年 2 月 24 日
AWS 适用于 SDK 的页面 AWS Config	在此版本中， AWS Config 引入了 “AWS Config 使用 SAWS DK” 页面。 AWS 软件开发套件 (SDK) 可用于许多流行的编程语言。每个软件开发工具包都提供 API、代码示例和文档，使开发人员能够更轻松地以其首选语言构建应用程序。	2022 年 2 月 24 日

安全 IAM 角色信任策略更新	在此版本中， AWS Config 更新了 IAM 信任策略声明，在信任策略中加入了安全保护，这些保护措施限制了对 AWS Security Token Service (AWS STS) 操作`sourceAccountId` 的访问`sourceARN` 和/或访问。这有助于确保 IAM 角色策略仅代表预期用户和场景访问您的资源。 将更新以下页面： • 将 IAM 信任策略添加到您的角色	2022 年 2 月 18 日

对全局资源类型记录的更改	AWS Config 现在更改了录制中新的全局资源类型的 AWS Config 录制方式。全局资源类型是指不需要您在创建时指定区域的 AWS 资源。在此更改之前，您可以启用 AWS Config中所有支持区域中全局资源类型的记录。进行此更改后，新加入录制的全局资源类型只能在服务主区域 AWS Config 录制商业分区，（美国西部）只能在分区的 AWS GovCloud （美国西部）中录制。 AWS GovCloud (US) 现在，您只能在其所在地区和 AWS GovCloud （美国西部）查看这些新的全球资源类型的配置项目。有关 2022 年 2 月之后载入的全局资源类型的主区域列表，请参阅记录所有受支持的资源类型页面上的表格。	2022 年 2 月 18 日

安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` 策略和`AWS_ConfigRole` 策略授予以下权限：获取有关 Elastic Beanstalk 环境的详细信息以及对指定 Elastic Beanstalk 配置集的设置的描述，获取我们的 Elasticsearch 版本地图，描述数据库 OpenSearch 的可用的 Amazon RDS 选项组，以及获取有关部署配置的信息。CodeDeploy 现在，该策略还授予以下权限：检索附加到的指定备用联系人 AWS 账户、检索有关 AWS Organizations 策略的信息、检索 Amazon ECR 存储库策略、检索有关存档 AWS Config 规则的信息、检索 Amazon ECS 任务定义系列列表、列出指定子 OU 或账户的根或上级组织单位 (OU)，以及列出附加到指定目标根目录、组织单位或账户的策略。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2022 年 2 月 10 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • autoscaling-multiple-az • codebuild-project-artifact-encryption • codebuild-project-environment-privileged-check • codebuild-project-logging-enabled • codebuild-project-s3-logs-encrypted • ec2-security-group-attached-to-eni-periodic • ecr-private-image-scanning-enabled • ecr-private-tag-immutability-enabled • ecs-containers-nonprivileged • ecs-containers-readonly-access • ecs-no-environment-secrets • ecs-task-definition-memory-hard-limit • ecs-task-definition-nonroot-user • ecs-task-definition-pid-mode-check • eks-cluster-oldest-supported-version • eks-cluster-supported-version	2022 年 2 月 10 日

	• lambda-vpc-multi-az-check • nacl-no-unrestricted-ssh-rdp • netfw-stateless-rule-group-not-empty • rds-cluster-default-admin-check • rds-db-security-group-not-allowed • rds-instance-default-admin-check • redshift-default-admin-check • s3-bucket-acl-prohibited • s3-version-lifecycle-policy-check • waf-global-webacl-not-empty	
安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` 策略和`AWS_ConfigRole` 策略授予创建 Amazon CloudWatch 日志组和流以及向已创建的日志流写入日志的权限。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2022 年 2 月 2 日

AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • opensearch-access-control-enabled • opensearch-audit-logging-enabled • opensearch-data-node-fault-tolerance • opensearch-encrypted-at-rest • opensearch-https-required • opensearch-in-vpc-only • opensearch-logs-to-cloudwatch • opensearch-node-to-node-encryption-check	2022 年 1 月 31 日
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录 AWS CodeDeploy 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2022 年 1 月 5 日
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录新 Amazon SageMaker 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 12 月 20 日
AWS Config 支持新的一致性包	在此版本中， AWS Config 支持以下一致性包： • 适用于 SME 的 ENISA 网络安全指南操作最佳实践	2021 年 12 月 20 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 支持以下一致性包： • NIST 800 172 操作最佳实践 • NIST 800 181 操作最佳实践 将更新以下合规包： • K-ISMS 操作最佳实践	2021 年 11 月 18 日
AWS Config 支持新的一致性包	在此版本中，AWS Config 支持以下一致性包： • Amazon API Gateway 操作最佳实践 • 的操作最佳实践 AWS Backup • CISA Cyber Essentials 操作最佳实践 • 的操作最佳实践 DevOps • NIST 隐私框架 v1.0 操作最佳实践 将更新以下合规包： • FedRAMP(Low) 操作最佳实践 • FedRAMP(Moderate) 操作最佳实践	2021 年 10 月 29 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对新 Amazon S OpenSearch ervice 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 10 月 12 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 更新了以下一致性包： • MAS TRMG 操作最佳实践	2021 年 10 月 12 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 更新了以下一致性包： • ABS CCIG 2.0 重要工作负载操作最佳实践 • ABS CCIG 2.0 标准工作负载操作最佳实践 • ACSC Essential 8 操作最佳实践 • ACSC ISM 操作最佳实践 • BNM RMiT 操作最佳实践 • CMMC Level 1 操作最佳实践 • CMMC Level 2 操作最佳实践 • CMMC Level 3 操作最佳实践 • CMMC Level 4 操作最佳实践 • CMMC Level 5 操作最佳实践 • 适用于 FDA 联邦法规第 21 篇第 11 部分的运营最佳实践 • 适用于 FFIEC 的运营最佳实践 • MAS 第 655 号通知操作最佳实践 • NBC TRMG 操作最佳实践 • NERC CIP 操作最佳实践 • NIST 800-53 rev 5 操作最佳实践	2021 年 9 月 30 日

安全 IAM 更新	现在，该`AWS_ConfigRole` 策略和`AWSConfigServiceRolePolicy` 政策授予获取有关亚马逊 OpenSearch 服务（OpenSearch 服务）域/域的详细信息以及获取特定亚马逊关系数据库服务 (Amazon RDS) 数据库参数组的详细参数列表的权限。该政策还授予获取有关 Amazon ElastiCache 快照的详细信息的权限。有关更多信息，请参阅适用于 AWS Config 的AWS 托管策略。	2021 年 9 月 8 日
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录新的 Amazon 弹性计算云资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 9 月 7 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 更新了以下一致性包： • APRA CPG 234 操作最佳实践 • CIS AWS 基金会运营最佳实践基准 v1.4 第 1 级 • CIS AWS 基金会运营最佳实践基准 v1.4 第 2 级 • NCSC 云安全原则操作最佳实践 • NCSC 网络评估框架操作最佳实践 • NIST 800 171 操作最佳实践 • NIST CSF 操作最佳实践 • 印度储备银行 UCB 网络安全框架操作最佳实践 • RBI MD-ITF 操作最佳实践 • NYDFS 23 操作最佳实践 • PCI DSS 3.2.1 操作最佳实践	2021 年 8 月 30 日

AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • aurora-resources-protected-by-backup-plan • backup-plan-min-frequency-and-min-retention-check • backup-recovery-point-encrypted • backup-recovery-point-manual-deletion-disabled • backup-recovery-point-minimum-retention-check • dynamodb-resources-protected-by-backup-plan • ebs-resources-protected-by-backup-plan • ec2-resources-protected-by-backup-plan • efs-resources-protected-by-backup-plan • fsx-resources-protected-by-backup-plan • rds-resources-protected-by-backup-plan	2021 年 8 月 20 日
AWS Config 支持新的一致性包	在此版本中，AWS Config 支持以下一致性包： • NZISM 操作最佳实践	2021 年 8 月 20 日

安全 Amazon SNS 策略更新	在本版本中， AWS Config 更新了使用服务相关角色时的 Amazon SNS 主题的 IAM 政策声明，在主题策略`sourceAccountId` 中加入了限制访问权限`sourceARN` 的安全保护。这有助于确保 Amazon SNS 仅代表预期用户和场景访问您的资源。 将更新以下页面： • Amazon SNS 主题的权限	2021 年 8 月 17 日
安全 AWS Lambda 政策更新	在此版本中， AWS Config 更新了 AWS Config 自定义规则的 AWS Lambda 基于资源的策略，以包括限制使用调用请求`sourceARN` 和/或`sourceAccountId` 在调用请求中进行访问的安全保护。这有助于确保 AWS Lambda 仅代表预期的用户和场景访问您的资源。 将更新以下页面： • AWS::Config::ConfigRule • 为以下对象开发自定义规则 AWS Config	2021 年 8 月 12 日
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录对 Amazon Kinesis 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 8 月 6 日

AWS Config 支持新的一致性包	在此版本中， AWS Config 支持以下一致性包： • Esquema Nacional de Seguridad (ENS) High 操作最佳实践 将更新以下合规包： • Well-Architecte AWS d 框架可靠性支柱的运营最佳实践 • Well-Architecte AWS d Framework 安全支柱的最佳运营实践 • Esquema Nacional de Seguridad (ENS) Low 操作最佳实践 • Esquema Nacional de Seguridad (ENS) Medium 操作最佳实践 • HIPAA 安全操作最佳实践	2021 年 7 月 30 日
AWS Config 自定义规则的示例 AWS Lambda 函数	在此版本中，在AWS Config 规则示例函数 (Python) 中 AWS Config 提供了 Python 示例 AWS Lambda 函数。	2021 年 7 月 29 日

安全 IAM 更新	`AWSConfigServiceRolePolicy` 策略和 `AWS_ConfigRole` 策略现在授予列出日志组的标签，列出状态机的标签，以及列出所有状态机的权限。这些策略现在授予获取有关状态机的详细信息的权限。这些政策现在还支持亚马逊 EC2 Systems Manager (SSM)、亚马逊弹性容器注册表、亚马逊 FSx、Amazon Data Firehose、适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK）、亚马逊关系数据库服务（亚马逊 RDS）、亚马逊 Route 53、亚马逊、SageMaker亚马逊简单通知服务、、和。 AWS Database Migration Service AWS Global Accelerator AWS Storage Gateway有关更多信息，请参阅适用于 AWS Config的AWS托管策略。	2021 年 7 月 28 日
AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录 AWS Backup 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 7 月 14 日

AWS Config 支持新的一致性包	在此版本中，AWS Config 支持以下一致性包： • CIS 关键安全控制 v8 IG1 操作最佳实践 • CIS 关键安全控制 v8 IG2 操作最佳实践 • CIS 关键安全控制 v8 IG3 操作最佳实践 • NIST 1800 25 操作最佳实践	2021 年 7 月 9 日
AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • ssm-document-not-public • s3-account-level-public-access-blocks-periodic	2021 年 6 月 25 日
AWS Config 更新托管规则	在此版本中，AWS Config 支持以下托管规则： • ec2-instance-multiple-eni-check • elbv2-acm-certificate-required • autoscaling-launch-config-public-ip-disabled	2021 年 6 月 10 日

安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` 策略和`AWS_ConfigRole` 策略授予查看有关 IAM Access Analyzer 的 AWS Systems Manager 文档和信息的权限。这些策略现在支持亚马逊 Kinesis、亚马逊、亚马逊 EMR、 ElastiCache亚马逊 Route 53 和 AWS Network Firewall亚马逊关系数据库服务 (Amazon RDS) 的其他 AWS 资源类型。这些权限更改 AWS Config 允许调用支持这些资源类型所需的只读 API。这些策略现在还支持筛选 Lambda -inside-vpc 托管规则的 Lambda AWS Config @Edge 函数。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2021 年 6 月 8 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • elasticsearch-logs-to-cloudwatch • rds-cluster-multi-az-enabled • api-gw-associated-with-waf • iam-policy-no-statements-with-full-access	2021 年 5 月 19 日

AWS Config 支持新的资源类型	在此版本中，您可以使用 AWS Config 记录对 Amazon Elastic File System 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 5 月 13 日
安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` 策略和`AWS_ConfigRole` 策略授予允许 AWS Config 对 API Gateway 进行只读 GET 调用的权限，以支持 API Gateway 的配置规则。这些策略还增加了 AWS Config 允许调用亚马逊简单存储服务 (Amazon S3) 只读 API 的权限，这是支持`AWS::S3::AccessPoint` 新资源类型所必需的。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2021 年 5 月 10 日
AWS Config 自定义规则	将更新开发人员指南中的以下页面： • 自定义规则入门 AWS Config • 为以下对象开发自定义规则 AWS Config	2021 年 4 月 30 日

AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • aurora-mysql-backtracking-enabled • ec2-instance-profile-attached • ecs-task-definition-user-for-host-mode-check • no-unrestricted-route-to-igw • rds-automatic-minor-version-upgrade-enabled • redshift-enhanced-vpc-routing-enabled	2021 年 4 月 15 日
安全 IAM 更新	现在，该`AWSConfigServiceRolePolicy` `AWS_ConfigRole` 策略和策略授予查看有关 AWS Systems Manager 指定文档的信息的权限。这些政策现在还支持亚马逊弹性文件系统 AWS Backup、亚马逊、亚马逊简单存储服务 (Amazon S3) ElastiCache、亚马逊弹性计算云 (Amazon EC2)、Amazon Kinesis、亚马逊和亚马逊 Route 53 的其他 AWS 资源类型。 SageMaker AWS Database Migration Service这些权限更改 AWS Config 允许调用支持这些资源类型所需的只读 API。有关更多信息，请参阅适用于 AWS Config的AWS 托管策略。	2021 年 4 月 14 日

合规包的合规性作为配置项目 (CI)	在此版本中，AWS Config 支持将一致性包合规性作为配置项目。这使您能够： • 查看合规包的合规状态的变更时间线 • 汇总合规包跨多个账户和区域的合规性 • 使用高级查询来检查合规包的合规性 将更新以下数据类型： • DescribeAggregateComplianceByConformancePacks • GetAggregateConformancePackComplianceSummary 将更新开发人员指南中的以下页面： • 在“合规包”控制面板中查看合规性数据 • 查看合规包的合规性历史记录时间线 • 在聚合器控制面板中查看合规性数据 • 查询 AWS 资源的当前配置状态 • 支持的资源类型	2021 年 3 月 30 日

分页更新	在此版本中， AWS Config 高级查询功能现在支持对包含聚合函数（例如 COUNT 和 SUM）的查询进行分页。您现在可以使用高级查询通过分页获取聚合查询的完整结果，分页以前限制为 500 行。有关更多信息，请参阅查询 AWS 资源的当前配置状态	2021 年 3 月 26 日
区域支持	在此版本中 AWS Config ，亚太地区（大阪）地区现在支持 AWS Config 规则。	2021 年 3 月 4 日
AWS Config 支持新的资源类型	在此版本中，您可以使用记录 AWS Config 对亚马逊弹性容器注册表、亚马逊弹性容器服务和亚马逊弹性 Kubernetes Service 资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2021 年 2 月 25 日

KMS 加密支持	在此版本中， AWS Config 允许您对由 S3 存储桶交付的对象使用基于 KMS AWS Config 的加密。 将更新以下数据类型： • DeliveryChannel • PutDelivery频道 将更新开发人员指南中的以下页面： • KMS 密钥的权限 • 分配给的 IAM 角色的权限 AWS Config	2021 年 2 月 16 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • secretsmanager-secret-periodic-rotation • secretsmanager-secret-unused • secretsmanager-using-cmk	2021 年 2 月 16 日
已保存的查询区域支持	在此版本中， AWS GovCloud （美国东部）和 AWS GovCloud （美国西部）地区现在支持保存的查询。	2021 年 2 月 15 日
多账户多区域数据聚合区域支持	在此版本中，现已在非洲（开普敦）和欧洲地区（米兰）区域支持多账户多区域数据聚合。有关更多信息，请参阅多账户多区域数据聚合。	2021 年 2 月 15 日

高级查询区域支持	在此版本中，现已在非洲（开普敦）和欧洲地区（米兰）区域支持高级查询。有关更多信息，请参阅查询 AWS 资源的当前配置状态。	2021 年 2 月 15 日
AWS Config 可通过 RSS 提要获取文档历史记录通知	现在，您可以通过订阅 RSS 提要来接收有关 AWS Config 文档更新的通知。	2021 年 1 月 1 日

早期更新

下表描述了 2020 年 12 月 31 日 AWS Config 之前的文档发布历史。

更改	描述	发行日期
已保存的查询支持	在此版本中， AWS Config 允许您保存查询。保存查询后，您可以对其进行搜索，将其复制到查询编辑器，以及对其进行编辑或将其删除。有关如何保存查询的更多信息，请参阅查询使用 SQL 查询编辑器进行查询（控制台）和使用 SQL 查询编辑器 (AWS CLI) 进行查询。 有关 API 的更多信息，请参阅 AWS Config API 参考。 • PutStored查询 • GetStored查询 • ListStored查询 • DeleteStored查询 另请参阅Service Limits。	2020 年 12 月 21 日

更改	描述	发行日期
流程检查支持	在此版本中， AWS Config 支持流程检查，这是一种 AWS Config 规则，允许您跟踪需要作为一致性包一部分进行验证的外部和内部任务。通过流程检查，您可以在单个位置列出要求和操作的合规性。 有关流程检查的更多信息，请参阅AWS Config 在一致性包中进行流程检查主题和PutExternal评估 API。	2020 年 12 月 17 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • api-gw-ssl-enabled • api-gw-xray-enabled • beanstalk-enhanced-health-reporting-enabled • cloudfront-accesslogs-enabled • cloudfront-associated-with-waf • cloudfront-custom-ssl-certificate • elastic-beanstalk-managed-updates-enabled • rds-cluster-iam-authentication-enabled • redshift-cluster-kms-enabled • s3-bucket-level-public-access-prohibited • subnet-auto-assign-public-ip-disabled • vpc-network-acl-unused-check	2020 年 12 月 17 日

更改	描述	发行日期
AWS Config 支持 AWS Network Firewall	在此版本中，您可以使用记录 AWS Config 对 AWS Network Firewall FirewallPolicy RuleGroup、和防火墙资源类型的配置更改。有关更多信息，请参阅 支持的资源类型。	2020 年 12 月 4 日
文档更新	AWS Config 添加了对委派管理员帐户中组织范围的资源数据聚合的支持。您现在可以使用委派管理员账户聚合 AWS Organizations 中所有组织成员账户中的资源配置和合规性数据。 有关更多信息，请参阅PutConfiguration聚合器使用控制台设置聚合器和。注册委派管理员	2020 年 12 月 4 日
AWS Config 支持新的一致性包	• CMMC Level 3 操作最佳实践 • CMMC Level 4 操作最佳实践 • CMMC Level 5 操作最佳实践 • Esquema Nacional de Seguridad (ENS) Low 操作最佳实践 • Esquema Nacional de Seguridad (ENS) Medium 操作最佳实践 • NCSC 网络评估框架操作最佳实践 • 印度储备银行 UCB 网络安全框架操作最佳实践	2020 年 10 月 30 日

更改	描述	发行日期
AWS Config 支持新的一致性包	• ACSC Essential 8 操作最佳实践 • ACSC ISM 操作最佳实践 • 人工智能和机器学习操作最佳实践 • 资产管理操作最佳实践 • BCP 和 DR 操作最佳实践 • EC2 操作最佳实践 • K-ISMS 操作最佳实践 • 负载平衡操作最佳实践 • 日志记录操作最佳实践 • 监控操作最佳实践 • 无服务器操作最佳实践	2020 年 10 月 22 日
AWS Config 支持新的一致性包	• APRA CPG 234 操作最佳实践 • FedRAMP(Low) 操作最佳实践 • MAS 第 655 号通知操作最佳实践 • NBC TRMG 操作最佳实践 • NCSC 云安全原则操作最佳实践 • RBI MD-ITF 操作最佳实践	2020 年 10 月 15 日

更改	描述	发行日期
AWS Config 支持新的一致性包	• ABS CCIG 2.0 重要工作负载操作最佳实践 • ABS CCIG 2.0 标准工作负载操作最佳实践 • BNM RMiT 操作最佳实践 • 数据弹性操作最佳实践 • 数据湖和分析服务操作最佳实践 • 加密和密钥管理操作最佳实践 • FDA 联邦法规第 21 篇第 11 部分操作最佳实践 • 可公开访问资源操作最佳实践 • MAS TRMG 操作最佳实践 • NERC CIP BCSI 操作最佳实践 • NYDFS 23 操作最佳实践	2020 年 10 月 8 日
AWS Config 支持新的一致性包	• Well-Architecte AWS d 框架可靠性支柱的运营最佳实践 • Well-Architecte AWS d Framework 安全支柱的运营最佳实践 • CMMC Level 1 操作最佳实践 • CMMC Level 2 操作最佳实践 • 计算服务操作最佳实践 • 数据库服务操作最佳实践 • 管理和治理服务操作最佳实践 • 联网和内容交付服务操作最佳实践 • 安全性、身份和合规性操作最佳实践 • 存储服务操作最佳实践	2020 年 10 月 26 日

更改	描述	发行日期
AWS Config 支持新的一致性包	• FedRAMP(Moderate) 操作最佳实践 • FFIEC 操作最佳实践 • HIPAA 安全操作最佳实践 • NIST 800-53 rev 4 操作最佳实践 • NIST 800 171 操作最佳实践	2020 年 9 月 28 日
文档更新	将更新以下合规包主题： • 先决条件 • 使用 AWS Config 控制台部署一致性包 • 跨组织中的所有账户管理一致性包	2020 年 9 月 28 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • iam-customer-policy-blocked-kms-actions • iam-inline-policy-blocked-kms-actions	2020 年 9 月 17 日
AWS Config 支持 AWS WAF v2	在此版本中，您可以使用 AWS Config 记录对 AWS WAF v2 WebACL、IPset RegexPatternSet RuleGroup、 ManagedRuleSet 和资源类型的配置更改。有关更多信息，请参阅 支持的资源类型。	2020 年 9 月 1 日

更改	描述	发行日期
文档更新	完全访问权限 AWS Config 中添加了关于创建授予完全访问权限的自定义权限的注释。 已更新有关以下规则的文档： • s3-bucket-server-side-encryption-enabled • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-platform-check	2020 年 8 月 24 日
文档更新	更新了 PCI DSS 3.2.1 操作最佳实践 和 NIST CSF 操作最佳实践 模板。	2020 年 8 月 14 日
文档更新	添加了关系查询示例。有关更多信息，请参阅 关系查询示例。	2020 年 7 月 30 日
文档更新	将更新以下数据类型： • ConfigurationAggregator • RemediationConfiguration • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRule状态 • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePack状态 • GetOrganizationConformancePackDetailedStatus	2020 年 7 月 23 日

更改	描述	发行日期
AWS Config 支持 S AWS ystems Manager 资源类型	在此版本中，您可以使用 AWS Config 记录对 S AWS ystems Manager 文件数据资源类型的配置更改。有关更多信息，请参阅 支持的资源类型。	2020 年 7 月 9 日
文档更新	更新了 AWS Identity And Access Management 操作最佳实践 和 PCI DSS 3.2.1 操作最佳实践 模板。	2020 年 7 月 9 日

更改	描述	发行日期
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • account-part-of-organizations • alb-http-drop-invalid-header-enabled • alb-waf-enabled • cloudfront-default-root-object-configured • cloudfront-origin-access-identity-enabled • cloudfront-origin-failover-enabled • cloudfront-sni-enabled • cloudtrail-security-trail-enabled • cw-loggroup-retention-period-check • dax-encryption-enabled • dynamodb-in-backup-plan • ebs-in-backup-plan • ec2-imdsv2-check • efs-in-backup-plan • eks-endpoint-no-public-access • eks-secrets-encrypted • elasticsearch-node-to-node-encryption-check • elb-cross-zone-load-balancing-enabled • elb-tls-https-listeners-only • iam-no-inline-policy-check • rds-cluster-deletion-protection-enabled	2020 年 7 月 9 日

更改	描述	发行日期
	• rds-in-backup-plan • rds-instance-deletion-protection-enabled • rds-instance-iam-authentication-enabled • rds-logging-enabled • redshift-backup-enabled • waf-classic-logging-enabled • wafv2-logging-enabled 有关更多信息，请参阅 AWS Config 托管规则列表。	
多账户多区域数据聚合区域支持	在此版本中，亚太地区（香港）和中东（巴林）区域现已支持多账户多区域数据聚合。有关更多信息，请参阅 Multi-Account Multi-Region Data Aggregation 和 多账户多区域数据聚合的故障排除。	2020 年 7 月 1 日
高级查询区域支持	在此版本中，亚太地区（香港）和中东（巴林）区域现已支持高级查询。有关更多信息，请参阅 查询 AWS 资源的当前配置状态。	2020 年 7 月 1 日

更改	描述	发行日期
文档更新	已更新有关以下规则的文档： • ec2-managedinstance-association-compliance-status-check • iam-policy-no-statements-with-admin-access • required-tags • restricted-common-ports • rds-snapshots-public-prohibited • s3-bucket-policy-grantee-check	2020 年 6 月 30 日
文档更新	文档已更新，其中包含有关安全性的信息 AWS Config。请参阅 安全性 AWS Config。	2020 年 6 月 24 日
文档更新	AWS Control Tower Detective Guardrails 一致性包模板已更新。有关更多信息，请参阅 AWS Control Tower 探测防护机制合规包。	2020 年 6 月 4 日
AWS Config 支持新的一致性包	在此版本中， AWS Config 支持 NIST CSF 一致性包的操作最佳实践。有关更多信息，请参阅 NIST CSF 操作最佳实践 。	2020 年 5 月 29 日

更改	描述	发行日期
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • dynamodb-pitr-enabled • dynamodb-table-encrypted-kms • ec2-ebs-encryption-by-default • rds-snapshot-encrypted • redshift-require-tls-ssl • s3-bucket-default-lock-enabled • s3-default-encryption-kms • securityhub-enabled • sns-encrypted-kms 有关更多信息，请参阅 AWS Config 托管规则列表。	2020 年 5 月 28 日

更改	描述	发行日期
委派管理员支持	在此版本中，除了管理账户之外，您还可以从组织中的任何委托成员账户部署 AWS Config 规则和合规包。 有关 API 的更多信息，请参阅 AWS Config API 参考。 • PutOrganizationConfigRule • PutOrganizationConformancePack • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRule状态 • DeleteOrganizationConfigRule • DeleteOrganizationConformancePack • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePack状态 • GetOrganizationConformancePackDetailedStatus 有关更多信息，请参阅 Service Limits。	2020 年 5 月 27 日
AWS Config 规则区域支持	在此版本中，非洲（开普敦）和欧洲（米兰）地区支持的 AWS Config 规则很少。有关规则及支持它们的区域的详细列表，请参阅AWS Config 托管规则列表。	2020 年 4 月 28 日

更改	描述	发行日期
AWS Config 支持新的一致性包	在此版本中， AWS Config 支持两个一致性包。 • AWS Control Tower Detective Guardrails 一致性包 • CIS 操作最佳实践 有关更多信息，请参阅 一致性包示例模板。	2020 年 4 月 22 日
AWS Config 支持 S AWS ecrets Manager	在此版本中，您可以使用记录 AWS Config 对您的 Secrets Manager 密钥的配置更改。有关更多信息，请参阅 支持的资源类型。	2020 年 4 月 20 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • secretsmanager-rotation-enabled-check • secretsmanager-scheduled-rotation-success-check 有关更多信息，请参阅 AWS Config 托管规则列表。	2020 年 4 月 16 日
合规包区域支持	在此版本中，亚太地区（香港）和中东（巴林）现已支持合规包。有关更多信息，请参阅 Conformance Packs。	2020 年 4 月 8 日
文档更新	AWS Config 本开发者指南中提供了限制。有关更多信息，请参阅 Service Limits。	2020 年 4 月 8 日

更改	描述	发行日期
文档更新	通过 AWS CloudFormation 注册表管理（即创建/更新/删除）的第三方资源会自动作为配置项目进行跟踪。 AWS Config 有关更多信息，请参阅 记录第三方资源的配置。	2020 年 3 月 30 日
文档更新	AWS Config 托管规则已更新以包含 AWS 区域 信息。有关更多信息，请参阅 AWS Config 托管规则列表。	2020 年 3 月 27 日
AWS Config 支持 Amazon SNS 资源类型	在此版本中，您可以使用 AWS Config 记录对 Amazon SNS 主题的配置更改。有关更多信息，请参阅 支持的资源类型。	2020 年 3 月 6 日
多账户多区域数据聚合区域支持	在此版本中，多账户多区域数据聚合现在在欧洲（斯德哥尔摩）区域中受支持。有关更多信息，请参阅 Multi-Account Multi-Region Data Aggregation。	2020 年 3 月 5 日
高级查询区域支持	在此版本中，欧洲（斯德哥尔摩）区域现在支持高级查询。有关更多信息，请参阅 查询 AWS 资源的当前配置状态。	2020 年 3 月 5 日

更改	描述	发行日期
AWS Config 允许您使用配置聚合器运行高级查询	在此版本中， AWS Config 增加了对使用配置聚合器基于资源配置属性运行高级查询的支持，使您能够在多个账户和区域中运行相同的查询。有关更多信息，请参阅 查询 AWS 资源的当前配置状态。 在此版本中， AWS Config 添加了 `SelectAggregateResourceConfig` API。有关更多信息，请参阅 AWS Config API 参考SelectAggregateResourceConfig中的：	2020 年 2 月 28 日
AWS Config 支持 Amazon SQS 资源类型	在此版本中，您可以使用 AWS Config 记录对 Amazon SQS 队列的配置更改。 有关更多信息，请参阅 支持的资源类型。	2020 年 2 月 13 日

更改	描述	发行日期
AWS CloudFormation 对一致性包的支持	在此版本中，增加了对以下资源的 AWS CloudFormation 支持：`AWS::Config::ConformancePack` 和`OrganizationConformancePack` 。 • AWS::Config::ConformancePack 使用该`AWS::Config::ConformancePack` 资源创建合规包，该合规包是一组 AWS Config 规则，可以轻松地在账户、地区和 AWS 组织中部署。 • AWS::Config::OrganizationConformance包 使用该`AWS::Config::OrganizationConformancePack` 资源创建包含以下信息的组织合规包 在成员账户中 AWS Config 创建的合规包。	2020 年 2 月 13 日

更改	描述	发行日期
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • api-gw-execution-logging-enabled • ec2-stopped-instance • elasticache-redis-cluster-automatic-backup-check • emr-master-no-public-ip • guardduty-non-archived-findings • rds-enhanced-monitoring-enabled • s3-account-level-public-access-blocks • sagemaker-endpoint-configuration-kms-key-configured • service-vpc-endpoint-enabled 有关更多信息，请参阅 AWS Config 托管规则列表。	2019 年 12 月 20 日
记录自定义资源类型的配置	在此版本中， AWS Config 引入了对自定义资源类型记录配置的支持。您可以使用 AWS Config 控制台和 API 将第三方资源的配置数据发布到 AWS Config 并查看和监控资源清单和配置历史记录。有关更多信息，请参阅 记录第三方资源的配置。 有关 API 的更多信息，请参阅 AWS Config API 参考。 • DeleteResourceConfig • PutResourceConfig	2019 年 11 月 20 日

更改	描述	发行日期
合规包	在此版本中， AWS Config 引入了一致性包。Conformance Packs 使您能够打包一系列 AWS Config 规则和补救措施，然后将这些规则和补救措施作为单个实体一起部署到整个 AWS 组织中。有关更多信息，请参阅 Conformance Packs。 有关 API 的更多信息，请参阅 AWS Config API 参考。 • DeleteOrganizationConformancePack • DeleteOrganizationConformancePack • DescribeConformance包 • DescribeConformance包 • DescribeConformancePackStatus • DescribeOrganizationConformancePacks • DescribeOrganizationConformancePack状态 • GetConformancePackCompliance详情 • GetConformancePackCompliance摘要 • GetOrganizationConformancePackDetailedStatus, • PutConformance包 • PutOrganizationConformancePack	2019 年 11 月 19 日

更改	描述	发行日期
AWS Config 支持 Amazon OpenSearch 服务和 AWS Key Management Service 资源类型	在此版本中，您可以使用记录 AWS Config 对您的 Amazon S OpenSearc h ervice 域和 AWS Key Management Service 密钥的配置更改。 有关更多信息，请参阅 支持的资源类型。	2019 年 11 月 11 日
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • dms-replication-not-public • emr-kerberos-enabled • internet-gateway-authorized-vpc-only • kms-cmk-not-scheduled-for-d eletion • sagemaker-notebook-no-direct-internet-access • sagemaker-notebook-instance-kms-key-configured • shield-drt-access 有关更多信息，请参阅 AWS Config 托管规则列表。	2019 年 10 月 10 日
AWS Config 支持 Amazon RDS 资源类型	在此版本中，您可以使用记录 AWS Config 对亚马逊关系数据库服务 (Amazon RDS) dbCluster 和数据库 ClusterSnapshot的配置更改。 有关更多信息，请参阅 支持的资源类型。	2019 年 9 月 17 日

更改	描述	发行日期
AWS Config 支持 Amazon QLDB 资源类型	在此版本中，您可以使用记录 AWS Config 对亚马逊量子账本数据库 (QLDB) 账本资源类型的配置更改。 有关更多信息，请参阅 支持的资源类型。	2019 年 9 月 10 日
AWS Config 允许您根据规则对不合规的资源进行 AWS Config 自动修复	在本版本中，根据 AWS Config 规则的评估， AWS Config 引入了使用 AWS Systems Manager 自动化文档对不合规资源应用自动补救的支持。有关更多信息，请参阅 使用规则修复不合规的资源 AWS Config。 在此版本中， AWS Config 添加了以下新 API。有关更多信息，请参阅 AWS Config API 参考： • PutRemediation例外情况 • DescribeRemediation例外情况 • DeleteRemediation例外情况	2019 年 9 月 5 日

更改	描述	发行日期
AWS Config 更新托管规则	在此版本中， AWS Config 支持以下托管规则： • alb-http-to-https-redirection-check • api-gw-cache-enabled-and-encrypted • api-gw-endpoint-type-check • cloudtrail-s3-dataevents-enabled • cloudwatch-log-group-encrypted • ebs-snapshot-public-restorable-check • elb-deletion-protection-enabled • lambda-concurrency-check • lambda-dlq-check • lambda-inside-vpc • shield-advanced-enabled-autorenew • vpc-vpn-2-tunnels-up 有关更多信息，请参阅 AWS Config 托管规则列表。	2019 年 8 月 22 日

更改	描述	发行日期
AWS Config 更新托管规则	在此版本中， AWS Config 更新了以下托管规则： • cloudfront-viewer-policy-https • ec2-instance-no-public-ip • ec2-security-group-attached-to-eni • efs-encrypted-check • elasticsearch-encrypted-at-rest • elasticsearch-in-vpc-only • redshift-cluster-public-access-check • vpc-sg-open-only-to-authorized-ports 有关更多信息，请参阅 AWS Config 托管规则列表。	2019 年 7 月 31 日
AWS Config 支持 Amazon EC2 资源类型	在此版本中，您可以使用记录 AWS Config 以下 Amazon EC2 资源的配置更改：vpcendPoint、VPC 和 VPC EndpointService。PeeringConnection 有关更多信息，请参阅 支持的资源类型。	2019 年 7 月 12 日

更改	描述	发行日期
AWS Config 允许您在组织 AWS 账户 内管理所有 AWS Config 规则	在此版本中， AWS Config 引入了对管理组织 AWS 账户 内所有 AWS Config 规则的支持。您可以集中创建、更新和删除组织中所有账户的 AWS Config 规则。有关更多信息，请参阅 管理组织中所有账户的 AWS Config 规则。 有关 API 的更多信息，请参阅 AWS Config API 参考。 • PutOrganizationConfigRule • DescribeOrganizationConfigRules • GetOrganizationConfigRuleDetailedStatus • DescribeOrganizationConfigRule状态 • DeleteOrganizationConfigRule	2019 年 7 月 9 日
AWS Config 支持 Amazon S3 和亚马逊 EC2 资源类型	在此版本中，您可以使用 AWS Config 记录对 Amazon S3 AccountPublicAccessBlock 资源和以下 Amazon EC2 资源的配置更改； NatGateway EgressOnlyInternet Gateway、和 FlowLog。 有关更多信息，请参阅 支持的资源类型。	2019 年 5 月 17 日

更改	描述	发行日期
AWS Config 更新托管规则	在此版本中， AWS Config 更新了以下托管规则： • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited 有关更多信息，请参阅 AWS Config 托管规则列表。	2019 年 5 月 7 日
AWS Config 允许您使用删除修复操作 AWS Management Console。	在此版本中， AWS Config 引入了对使用删除修复操作的支持 AWS Management Console。有关更多信息，请参阅 使用规则修复不合规的资源 AWS Config。	2019 年 4 月 24 日
AWS Config 支持新的托管规则	此版本支持新的托管规则：fms-shield-resource-policy-check。 有关更多信息，请参阅 AWS Config 托管规则列表。	2019 年 4 月 7 日
AWS Config 支持 Amazon API Gateway 资源类型	在此版本中，您可以使用记录 AWS Config 对以下 Amazon API Gateway 资源的配置更改：Api (API)、(REST WebSocket API)、阶段 RestApi （ API 阶段 ）和阶段（ REST WebSocket API 阶段 ）和阶段（ REST API 阶段 ）。 有关更多信息，请参阅 支持的资源类型。	2019 年 3 月 20 日

更改	描述	发行日期
AWS Config 允许你运行高级查询	在此版本中， AWS Config 增加了对基于资源配置属性运行高级查询的支持。有关更多信息，请参阅 查询 AWS 资源的当前配置状态。 在此版本中， AWS Config 添加了 `SelectResourceConfig` API。有关更多信息，请参阅 AWS Config API 参考中的 SelectResourceConfig：	2019 年 3 月 19 日
AWS Config 允许您为 AWS Config 资源分配标签	在此版本中， AWS Config 引入了对三种 AWS Config 资源的基于标签的访问控制的支持 — `ConfigRule`, `ConfigurationAggregator`, 和`AggregationAuthorization` 。有关更多信息，请参阅 标记您的 AWS Config 资源。 在此版本中，您可以使用以下数据类型添加、删除或列出您的 AWS Config 资源中的标签。有关更多信息，请参阅 AWS Config API 参考： • ListTagsForResource • TagResource • UntagResource	2019 年 3 月 14 日

更改	描述	发行日期
AWS Config 允许您根据规则对不合规的资源进行 AWS Config 修复	在此版本中， AWS Config 引入了使用 AWS Systems Manager 自动化文档对不合规资源进行补救的支持，这些资源由 AWS Config Rules 评估。有关更多信息，请参阅 使用规则修复不合规的资源 AWS Config。 在此版本中， AWS Config 添加了以下新 API。有关更多信息，请参阅 AWS Config API 参考： • DeleteRemediation配置 • DescribeRemediation配置 • DescribeRemediationExecutionStatus • PutRemediation配置 • StartRemediation处决	2019 年 3 月 12 日

更改	描述	发行日期
AWS Config 支持中国（宁夏）区域的 AWS Config 规则	此版本仅支持中国（宁夏）区域的 54 AWS Config 条规则。有关更多信息，请参阅 AWS Config 托管规则列表。 但是，目前 AWS Config 不支持中国（宁夏）区域的以下规则： • acm-certificate-expiration-check • cmk-backing-key-rotation-enabled • cloudformation-stack-drift-detection-check • cloudformation-stack-notification-check • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check • dynamodb-table-encryption-enabled • elb-acm-certificate-required • encrypted-volumes • fms-webacl-resource-policy-check • fms-webacl-rulegroup-association-check • guardduty-enabled-centralized	2019 年 3 月 12 日

更改	描述	发行日期
	• lambda-function-public-access-prohibited • lambda-function-settings-check • rds-storage-encrypted • root-account-mfa-hardware-mfa-enabled • root-account-mfa-enabled • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-grantee-check • s3-bucket-policy-not-more-p ermissive • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited • s3-bucket-server-side-encryption-enabled • s3-bucket-ssl-requests-only	
AWS Config 支持新的托管规则	此版本支持以下新托管规则： • iam-user-mfa-enabled • s3-bucket-policy-grantee-check 有关更多信息，请参阅 AWS Config 托管规则列表。	2019 年 1 月 21 日
AWS Config 支持 Service Catalog 资源类型	在此版本中，您可以使用记录 AWS Config 对以下 Service Catalog 资源的配置更改： CloudFromation 产品、预配置产品和产品组合。有关更多信息，请参阅 支持的资源类型。	2019 年 1 月 11 日

更改	描述	发行日期
服务关联 AWS Config 规则支持	在此版本中， AWS Config 添加了一个新的托管配置规则，该规则支持其他 AWS 服务在您的账户中创建 AWS Config 规则。有关更多信息，请参阅 服务相关规则 AWS Config。	2018 年 11 月 20 日
AWS Config 允许您聚合 AWS 资源的配置数据	在此版本中， AWS Config 引入了对聚合 AWS 资源配置数据的支持。有关更多信息，请参阅 在聚合器控制面板中查看合规性和清单数据。 在此版本中， AWS Config 添加了以下新 API。有关更多信息，请参阅 AWS Config API 参考： • BatchGetAggregateResourceConfig • GetAggregateDiscoveredResource计数 • GetAggregateResourceConfig • ListAggregateDiscoveredResources	2018 年 11 月 19 日
AWS Config 支持新的托管规则	此版本支持以下新托管规则： • cloudformation-stack-drift-detection-check • codepipeline-deployment-count-check • codepipeline-region-fanout-check 有关更多信息，请参阅 AWS Config 托管规则列表。	2018 年 11 月 19 日

更改	描述	发行日期
AWS Config 支持新的托管规则	此版本支持以下新托管规则： • access-keys-rotated • cloud-trail-cloud-watch-logs-enabled • cloud-trail-encryption-enabled • cloud-trail-log-file-validation-enabled • cmk-backing-key-rotation-enabled • iam-policy-no-statements-with-admin-access • iam-role-managed-policy-check • iam-root-access-key-check • iam-user-unused-credentials-check • mfa-enabled-for-iam-console-access • multi-region-cloudtrail-enabled • root-account-hardware-mfa-enabled • vpc-flow-logs-enabled 有关更多信息，请参阅 AWS Config 托管规则列表。	2018 年 11 月 12 日

更改	描述	发行日期
AWS Config 支持新的托管规则	此版本支持以下新托管规则： • dynamodb-table-encryption-enabled • elb-logging-enabled • rds-instance-public-access-check • vpc-default-security-group-closed 有关更多信息，请参阅 AWS Config 托管规则列表。	2018 年 10 月 24 日
合规性历史记录支持	在此版本中， AWS Config 现在支持存储 AWS Config 规则评估的资源的合规性历史记录。有关更多信息，请参阅 查看资源的合规性历史记录时间线。	2018 年 10 月 18 日
多账户多区域数据聚合区域支持	在此版本中，多账户多区域数据聚合现在可在六个新区域中受支持。有关更多信息，请参阅 Multi-Account Multi-Region Data Aggregation。	2018 年 10 月 4 日
AWS Config 支持 AWS Config 规则 API 操作的资源级权限	在此版本中， AWS Config 支持某些 AWS Config 规则 API 操作的资源级权限。有关支持的 API 的更多信息，请参阅AWS Config 规则 API 操作支持的资源级权限。	2018 年 10 月 1 日
AWS Config 支持 CodePipeline 资源类型	在此版本中 AWS Config ，您可以使用记录 AWS CodePipeline 资源类型的配置更改。有关更多信息，请参阅 支持的资源类型。	2018 年 9 月 12 日

更改	描述	发行日期
AWS Config 支持新的托管规则	此版本支持以下新托管规则： • ec2-instance-managed-by-systems-manager • ec2-managedinstance-association-compliance-status-check • ec2-managedinstance-patch-compliance-status-check • guardduty-enabled-centralized • rds-snapshots-public-prohibited • s3-bucket-blacklisted-actions-prohibited • s3-bucket-policy-not-more-permissive 有关更多信息，请参阅 AWS Config 托管规则列表。	2018 年 9 月 5 日
AWS Config 支持 S AWS ystems Manager 资源类型	在此版本中，您可以使用 AWS Config 记录对 S AWS ystems Manager 补丁合规性和关联合规性资源类型的配置更改。有关更多信息，请参阅 支持的资源类型。	2018 年 8 月 9 日
AWS Config 允许您使用删除 AWS Config 数据 AWS Management Console	在此版本中， AWS Config 引入了对保留期的支持 AWS Management Console。在中 AWS Management Console，您可以为自己的自定义数据保留期限`ConfigurationItems` 。有关更多信息，请参阅 删除 AWS Config 数据。	2018 年 8 月 7 日

更改	描述	发行日期
AWS Config 支持 AWS Shield 资源类型	在此版本中，您可以使用记录 AWS Config 对 AWS Shield 保护资源类型的配置更改。有关更多信息，请参阅支持的资源类型。	2018 年 8 月 7 日
AWS Config 支持 AWS PrivateLink	在此版本中 AWS PrivateLink， AWS Config 支持在亚马逊虚拟私有云 (VPC) Private Cloud (VPC) 之间 AWS Config 以及完全在网络内 AWS 路由数据。有关更多信息，请参阅 AWS Config 与接口 Amazon VPC 终端节点一起使用。	2018 年 7 月 31 日
AWS Config 允许您删除 AWS Config 数据	在此版本中， AWS Config 引入了对保留期的支持。 AWS Config 允许您通过为自己的数据指定保留期来删除数据`ConfigurationItems` 。有关更多信息，请参阅 删除 AWS Config 数据。 在此版本中， AWS Config 添加了以下新 API。有关更多信息，请参阅 AWS Config API 参考： • PutRetention配置 • DescribeRetention配置 • DeleteRetention配置	2018 年 5 月 25 日

更改	描述	发行日期
AWS Config 支持新的托管规则	此版本支持以下两新的托管规则： • lambda-function-settings-check • s3-bucket-replication-enabled • iam-policy-blacklisted-check 有关更多信息，请参阅 AWS Config 托管规则列表。	2018 年 5 月 10 日
AWS Config 支持 AWS X-Ray 资源类型	在此版本中 AWS Config ，您可以使用记录 AWS X-Ray EncryptionConfig 资源类型的配置更改。有关更多信息，请参阅 支持的资源类型。	2018 年 5 月 1 日
AWS Config 支持 AWS Lambda 资源类型和一个新的托管规则	在此版本中，您可以使用 AWS Config 来记录对 AWS Lambda 函数资源类型的配置更改。有关更多信息，请参阅 支持的资源类型。 此版本还支持 lambda-function-public-access-prohibited 托管规则。有关更多信息，请参阅 AWS Config 托管规则。	2018 年 4 月 25 日
AWS Config 支持 AWS Elastic Beanstalk 资源类型	在此版本中，您可以使用记录 AWS Config 对 AWS Elastic Beanstalk 应用程序、应用程序版本和环境资源的配置更改。 有关更多信息，请参阅 支持的资源类型。	2018 年 24 月 4 日

更改	描述	发行日期
AWS Config 支持新的托管规则	此版本支持以下两新的托管规则： • fms-webacl-resource-policy-check • fms-webacl-rulegroup-association-check 有关更多信息，请参阅 AWS Config 托管规则列表。	2018 年 4 月 4 日

更改	描述	发行日期
多账户多区域数据聚合	在此版本中， AWS Config 引入了多账户多区域数据聚合。此功能允许您将来自多个账户或一个组织以及多个地区的 AWS Config 数据聚合到一个聚合器账户中。有关更多信息，请参阅 Multi-Account Multi-Region Data Aggregation。 在此版本中， AWS Config 添加了以下新 API。有关更多信息，请参阅 AWS Config API 参考： • PutConfiguration聚合器 • DescribePendingAggregationRequests • DeletePendingAggregationRequest • PutAggregation授权 • DescribeAggregation授权 • GetAggregateConfigRuleComplianceSummary • DescribeAggregateComplianceByConfigRules • GetAggregateComplianceDetailsByConfig规则 • DescribeConfiguration聚合器 • DescribeConfigurationAggregatorSources状态 • DeleteAggregation授权 • DeleteConfiguration聚合器	2018 年 4 月 4 日

更改	描述	发行日期
AWS Config 使用 Amazon CloudWatch 事件进行监控	在此版本中，使用 Amazon CloudWatch Events 来检测 AWS Config 事件状态的变化并做出反应。 有关更多信息，请参阅 AWS Config 使用 Amazon 进行监控 EventBridge。	2018 年 3 月 29 日
新的 API 操作	在此版本中， AWS Config 增加了对 BatchGetResourceConfigAPI 的支持，允许您批量检索一个或多个资源的当前状态。	2018 年 3 月 20 日
AWS Config 支持 AWS WAF RuleGroup 资源类型	在此版本中，您可以使用 AWS Config 记录对 AWS WAF RuleGroup 和 AWS WAF RuleGroup 区域资源的配置更改。 有关更多信息，请参阅 支持的资源类型。	2018 年 2 月 15 日

更改	描述	发行日期
AWS Config 支持新的托管规则	此版本支持以下新托管规则： • elb-acm-certificate-required • elb-custom-security-policy-ssl-check • elb-predefined-security-policy-ssl-check • codebuild-project-envvar-awscred-check • codebuild-project-source-repo-url-check • iam-group-has-users-check • s3-bucket-server-side-encryption-enabled 有关更多信息，请参阅 AWS Config 托管规则列表。	2018 年 1 月 25 日
AWS Config 支持 Elastic Load Balancing 资源类型	在此版本中，您可以使用 AWS Config 记录对 Elastic Load Balancing 经典负载均衡器的配置更改。 有关更多信息，请参阅 支持的资源类型。	2017 年 11 月 17 日

更改	描述	发行日期
AWS Config 支持 Amazon CloudFront 和 AWS WAF 资源类型	在此版本中，您可以使用 AWS Config 记录 CloudFront 分发和直播分发的配置更改。 在此版本中，您可以使用记录 AWS Config 对以下资源 AWS WAF 和 AWS WAF 区域资源的配置更改；基于费率的规则、规则和 Web ACL。 有关更多信息，请参阅 支持的资源类型。	2017 年 11 月 15 日
AWS Config 支持 AWS CodeBuild 资源类型	在此版本中，您可以使用 AWS Config 来记录 AWS CodeBuild 项目的配置更改。 有关更多信息，请参阅 支持的资源类型。	2017 年 10 月 20 日
AWS Config 支持 Auto Scaling 资源和一条新的托管规则	在此版本中，您可以使用记录 AWS Config 以下 Auto Scaling 资源的配置更改：组、启动配置、计划操作和扩展策略。 有关更多信息，请参阅 支持的资源类型。 此版本还支持以下托管规则： • autoscaling-group-elb-healthcheck-required 有关更多信息，请参阅 AWS Config 托管规则。	2017 年 9 月 18 日

更改	描述	发行日期
AWS Config 支持 AWS CodeBuild 资源类型	在此版本中，您可以使用 AWS Config 来记录 AWS CodeBuild 项目的配置更改。 有关更多信息，请参阅 支持的资源类型。	2017 年 10 月 20 日
AWS Config 支持 Auto Scaling 资源和一条新的托管规则	在此版本中，您可以使用记录 AWS Config 以下 Auto Scaling 资源的配置更改：组、启动配置、计划操作和扩展策略。 有关更多信息，请参阅 支持的资源类型。 此版本还支持以下托管规则： • autoscaling-group-elb-healthcheck-required 有关更多信息，请参阅 AWS Config 托管规则。	2017 年 9 月 18 日
AWS Config 支持 DynamoDB 表资源类型和一个新的托管规则	在此版本中，您可以使用记录 AWS Config 对您的 DynamoDB 表的配置更改。 有关更多信息，请参阅 支持的资源类型。 此版本支持以下托管规则： • dynamodb-autoscaling-enabled 有关更多信息，请参阅 AWS Config 托管规则。	2017 年 9 月 8 日

更改	描述	发行日期
AWS Config 支持两条适用于 Amazon S3 的新托管规则	此版本支持两条新的托管规则： • s3-bucket-public-read-prohibited • s3-bucket-public-write-prohibited 有关更多信息，请参阅 AWS Config 托管规则。	2017 年 8 月 14 日
AWS Config 控制台中的新页面	您可以使用 AWS Config 控制台中的控制面板查看以下内容： • 资源总数 • 规则总数 • 不合规资源数 • 不合规规则数 有关更多信息，请参阅 查看 AWS Config 控制面板。	2017 年 7 月 17 日
新的 API 操作	您可以使用该GetDiscoveredResourceCounts操作为您返回资源类型的数量、每种资源类型的数量以及在某个区域中记录的 AWS Config 资源总数 AWS 账户。	2017 年 7 月 17 日

更改	描述	发行日期
AWS Config 支持 AWS CloudFormation 堆栈资源类型和一个新的托管规则	在此版本中，您可以使用 AWS Config 来记录 AWS CloudFormation 堆栈的配置更改。 有关更多信息，请参阅 支持的资源类型。 此版本支持以下托管规则： • cloudformation-stack-notification-check 有关更多信息，请参阅 AWS Config 托管规则。	2017 年 6 月 7 日
新增和更新的内容	此版本增加了对加拿大（中部）地区和南美洲（圣保罗）地区 AWS Config 规则的支持。 有关所有支持 AWS Config 和 Config 规则的区域，请参阅中的AWS 区域和终端节点AWS 一般参考。	2017 年 7 月 5 日
新增和更新的内容	AWS Config 该 AWS GovCloud (US) 地区提供规则。有关更多信息，请参阅 AWS GovCloud (US) 《用户指南》。 有关支持的区域 AWS Config，请参阅中的AWS 区域 和终端节点AWS 一般参考。	2017 年 6 月 8 日

更改	描述	发行日期
AWS Config 支持 Amazon CloudWatch 警报资源类型和三个新的托管规则	在此版本中，您可以使用记录 AWS Config 对您的 Amazon CloudWatch 警报的配置更改。 有关更多信息，请参阅 支持的资源类型。 此版本支持三条新的托管规则： • cloudwatch-alarm-action-check • cloudwatch-alarm-resource-check • cloudwatch-alarm-settings-check 有关更多信息，请参阅 AWS Config 托管规则。	2017 年 6 月 1 日
新增和更新的内容	此版本支持为以下托管规则指定应用程序版本号： • ec2-managedinstance-applications-blacklisted • ec2-managedinstance-applications-required 有关更多信息，请参阅 AWS Config 托管规则。	2017 年 6 月 1 日
新增和更新的内容	此版本增加了对亚太地区（孟买）地区 AWS Config 规则的支持。有关更多信息，请参阅《AWS 一般参考》中的 AWS 区域 和端点。	2017 年 4 月 27 日

更改	描述	发行日期
新增和更新的内容	此版本支持更新的控制台体验，可让您首次将 AWS Config 托管规则添加到您的账户。 首次或在新区域设置 AWS Config 规则时，可以按名称、描述或标签搜索 AWS 托管规则。您可以选择 Select all 以选择所有规则，或者选择 Clear all 以清除所有规则。 有关更多信息，请参阅添加、查看、更新和删除规则（控制台）。	2017 年 4 月 5 日
AWS Config 支持新的托管规则	此版本支持以下新托管规则： • acm-certificate-expiration-check • ec2-instance-detailed-monitoring-enabled • ec2-managedinstance-inventory-blacklisted • ec2-volume-inuse-check • iam-user-group-membership-check • iam-user-no-policies-check • s3-bucket-ssl-requests-only 有关更多信息，请参阅 AWS Config 托管规则列表。	2017 年 2 月 21 日
新增和更新的内容	此版本增加了对欧洲（伦敦）区域 AWS Config 规则的支持。有关更多信息，请参阅《AWS 一般参考》中的 AWS 区域 和端点。	2017 年 2 月 21 日

更改	描述	发行日期
新增和更新的内容	此版本为 AWS Config 托管规则添加了 AWS CloudFormation 模板。您可以使用这些模板为您的账户创建托管规则。有关更多信息，请参阅 使用 AWS CloudFormation 模板创建 AWS Config 托管规则。	2017 年 2 月 16 日
新增和更新的内容	此版本增加了对 `PutEvaluations` API 的新测试模式的支持。在自定义规则中将 `TestMode` 参数设置为 true 以验证 AWS Lambda 函数是否将评估结果传送到 AWS Config。不会更新现有评估，并且不会将评估结果发送到 AWS Config。 有关更多信息，请参阅 AWS Config API 参考PutEvaluations中的。	2017 年 2 月 16 日
新增和更新的内容	此版本增加了对亚太地区（首尔）和美国西部（加利福尼亚北部）区域的 AWS Config 规则的支持。有关更多信息，请参阅《AWS 一般参考》中的 AWS 区域 和端点。	2016 年 12 月 21 日
新增和更新的内容	此版本增加了对 AWS Config 欧洲（伦敦）地区的支持。有关更多信息，请参阅《AWS 一般参考》中的 AWS 区域 和端点。	2016 年 12 月 13 日
新增和更新的内容	此版本增加了对 AWS Config 加拿大（中部）地区的支持。有关更多信息，请参阅《AWS 一般参考》中的 AWS 区域 和端点。	2016 年 12 月 8 日

更改	描述	发行日期
AWS Config 支持 Amazon Redshift 资源类型和两个新的托管规则	在此版本中，您可以使用 AWS Config 记录对 Amazon Redshift 集群、集群参数组、集群安全组、集群快照、集群子网组和事件订阅的配置更改。 有关更多信息，请参阅 支持的资源类型。 此版本支持两条新的托管规则： • redshift-cluster-configuration-check • redshift-cluster-maintenancesettings-check 有关更多信息，请参阅 AWS Config 托管规则列表。	2016 年 12 月 7 日
新增和更新的内容	此版本增加了对新托管规则的支持： • dynamodb-throughput-limit-check 有关更多信息，请参阅 AWS Config 托管规则列表。	2016 年 12 月 7 日
新增和更新的内容	此版本增加了以下支持：可在一个账户中针对每个区域创建多达 50 条规则。有关更多信息，请参阅《AWS 一般参考》中的 AWS Config 限制。	2016 年 12 月 7 日

更改	描述	发行日期
AWS Config 支持 Amazon EC2 Systems Manager 的托管实例清单资源类型和三个新的托管规则	在此版本中，您可以使用 AWS Config 记录托管实例的软件配置更改，并支持托管实例清单。 有关更多信息，请参阅 Recording Software Configuration for Managed Instances。 此版本支持三条新的托管规则： • ec2-managedinstance-inventory-blacklisted • ec2-managedinstance-applications-required • ec2-managedinstance-platform-check 有关更多信息，请参阅 AWS Config 托管规则列表。	2016 年 12 月 1 日
AWS Config 支持 Amazon S3 存储桶资源和两个新的托管规则	在此版本中，您可以使用 AWS Config 记录对 Amazon S3 存储桶的配置更改。有关更多信息，请参阅 支持的资源类型。 此版本支持两条新的托管规则： • s3-bucket-logging-enabled • s3-bucket-versioning-enabled 有关更多信息，请参阅 AWS Config 托管规则。	2016 年 10 月 18 日

更改	描述	发行日期
新增和更新的内容	此版本增加了对美国东部（俄亥俄州）地区的支持 AWS Config 和 AWS Config 规则。有关更多信息，请参阅《AWS 一般参考》中的 AWS 区域 和端点。	2016 年 10 月 17 日
新增和更新的管理规则	此更新添加了对八个新的管理规则的支持： • approved-amis-by-id • approved-amis-by-tag • db-instance-backup-enabled • desired-instance-type • ebs-optimized-instance • iam-password-policy • rds-multi-az-support • rds-storage-encrypted 您可以为以下规则指定多个参数值： • desired-instance-tenancy • required-tags 有关更多信息，请参阅 AWS Config 托管规则列表。	2016 年 10 月 4 日
AWS Config 主机的新内容和更新内容	此更新增加了对在 AWS Config 时间轴中查看 AWS CloudTrail API 活动的支持。如果您的账户 CloudTrail 正在登录，则可以查看资源配置更改的创建、更新和删除 API 事件。有关更多信息，请参阅 查看配置和合规性历史记录。	2016 年 9 月 6 日

更改	描述	发行日期
AWS Config 支持 Elastic Load Balancing 资源类型	在此版本中，您可以使用 AWS Config 记录对 Elastic Load Balancing 应用程序负载均衡器的配置更改。有关更多信息，请参阅 支持的资源类型。	2016 年 8 月 31 日
新增和更新的内容	此版本增加了对亚太地区（新加坡）和亚太地区（悉尼）区域的 AWS Config 规则的支持。有关更多信息，请参阅《AWS 一般参考》中的 AWS 区域 和端点。	2016 年 8 月 18 日
《AWS Config 规则》的新内容和更新内容	此更新增加了支持，用以创建一个既可按配置更改触发、又可按您选择的定期频率触发的规则。有关更多信息，请参阅 AWS Config 规则的评估模式和触发器类型。 此更新还增加了支持，用以手动按照规则评估您的资源和删除评估结果。有关更多信息，请参阅 使用 AWS Config 规则评估您的资源。 此更新还增加了支持，用以使用自定义规则来评估其他资源类型。有关更多信息，请参阅 评估其他资源类型。	2016 年 7 月 25 日

更改	描述	发行日期
AWS Config 支持 Amazon RDS 和 AWS Certificate Manager (ACM) 资源类型	在此版本中，您可以使用 AWS Config 记录对 Amazon Relational Database Service (Amazon RDS) 数据库实例、数据库安全组、数据库快照、数据库子网组和事件订阅的配置更改。您还可以使用记录 AWS Config 对 ACM 提供的证书的配置更改。 有关更多信息，请参阅 支持的资源类型。	2016 年 7 月 21 日
有关管理配置记录器的更新信息	此更新增加了步骤，用以重命名和删除 管理配置记录器 的配置记录器。	2016 年 7 月 7 日
简化的角色创建过程和更新策略	通过此更新，简化了为创建 IAM 角色 AWS Config 的过程。支持 Config 规则的区域中均提供了此增强功能。为支持此增强功能，使用控制 AWS Config 台进行设置 中的步骤、AWS Config 传送渠道的 Amazon S3 存储桶的权限 中的示例策略及 基于身份的策略示例 AWS Config 中的示例策略均已进行更新。	2016 年 3 月 31 日
Config 规则的示例函数和事件	此更新在 AWS Config 规则的示例 AWS Lambda 函数 (Node.js) 中提供了更新的示例函数，并在 AWS Config 规则的示例事件 中添加了示例事件。	2016 年 3 月 29 日
AWS Config 规则 GitHub 存储库	此更新将有关AWS Config 规则 GitHub 存储库的信息添加到使用 AWS Config 规则评估资源。此存储库为 AWS Config 用户开发和贡献的自定义规则提供了示例函数。	2016 年 3 月 1 日

更改	描述	发行日期
AWS Config 规则	此版本引入了 AWS Config 规则。通过规则，您可以使用 AWS Config 来评估您的 AWS 资源是否符合所需的配置。有关更多信息，请参阅 使用 AWS Config 规则评估资源。	2015 年 12 月 18 日
AWS Config 支持 IAM 资源类型	在此版本中，您可以使用记录 AWS Config 对您的 IAM 用户、群组、角色和客户托管策略的配置更改。有关更多信息，请参阅 支持的资源类型。	2015 年 12 月 10 日
AWS Config 支持 EC2 专用主机	在此版本中，您可以使用 AWS Config 记录您的 EC2 专用主机的配置更改。有关更多信息，请参阅 支持的资源类型。	2015 年 11 月 23 日
更新的权限信息	此更新添加了有关以下 AWS 托管策略的信息 AWS Config： • `AWS_ConfigRole` – 为 AWS Config 授予获取有关您的资源的配置详细信息的权限。有关更多信息，请参阅 用于获取配置详细信息的 IAM 角色策略。 • `AWSConfigUserAccess` — 向 AWS Config 用户授予只读访问权限。有关更多信息，请参阅 只读访问权限 AWS Config。	2015 年 10 月 19 日
AWS Config 规则预览	此版本引入了 AWS Config 规则预览版。通过规则，您可以使用 AWS Config 来评估您的 AWS 资源是否符合所需的配置。有关更多信息，请参阅 使用 AWS Config 规则评估资源。	2015 年 10 月 7 日

更改	描述	发行日期
新增和更新的内容	此版本增加了查找 AWS Config 已发现资源的功能。有关更多信息，请参阅 查找由以下人员发现的资源 AWS Config。	2015 年 8 月 27 日
新增和更新的内容	此版本增加了选择 AWS Config 记录哪些类型资源的功能。有关更多信息，请参阅 录制 AWS 资源。	2015 年 6 月 23 日
新增和更新的内容	此版本添加了对以下区域的支持：亚太地区（东京）、亚太地区（新加坡）、欧洲地区（法兰克福）、南美洲（圣保罗）和美国西部（加利福尼亚北部）。有关更多信息，请参阅AWS 区域 和端点。	2015 年 4 月 6 日
新指南	此版本引入了 AWS Config。	2014 年 11 月 12 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。