



AMS 高级概念和程序

AMS 高级用户指南



版本 October 3, 2025

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

AMS 高级用户指南: AMS 高级概念和程序

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

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

Table of Contents

什么是 AWS Managed Services ? 1

关于本指南 2

运营计划 2

加快运营计划 2

高级操作计划 2

入门 3

关键术语 3

服务描述 8

AWS Managed Services (AMS) AMS 高级运营计划功能 8

我们做什么，不做什么 12

AMS 责任矩阵 (RACI) 13

AMS 环境基本组件 30

AMS 账户限额 32

AMS 服务级别目标 (SLOs) 34

支持的 AWS 服务 35

支持的配置 38

不支持的操作系统 40

AMS 高级接口 41

VPC 端点 42

AMS 保护的命名空间 43

AMS 保留的前缀 44

AMS 维护窗口 45

AMS 信息资源 45

AMS 合规性 46

AMS 支持的合规标准 46

责任共担 49

AMS Amazon 机器映像 (AMIs) 49

安全性得到增强 AMIs 52

AD FS 和 AMS 之间的集成是如何工作的 52

AMS 托管活动目录 53

应用程序部署 56

服务管理 57

账户治理 57

服务开始 57

客户关系管理 (CRM)	58
CRM 流程	59
CRM 会议	59
CRM 会议安排	60
CRM 月度报告	61
成本优化	62
成本优化框架	62
成本优化责任矩阵	64
服务时间	65
获取帮助	65
计划中的活动管理	67
AMS PEM 标准	67
PEM 的类型	67
AMS PEM 流程	68
PEM FAQs	68
网络架构	70
MALZ 网络架构	70
关于多账号 landing zone 网络架构	70
选择单个 MALZ 或多个 MALZs	72
多账号着陆区账号	75
SALZ 网络架构	103
AMS 单账号 landing zone 共享服务	104
设置 AMS	105
AMS 默认设置	105
DNS 解析默认值 (MALZ)	106
EC2 IAM 实例配置文件	106
来自 AMS 基线监测的警报	113
默认日志保留和轮换	125
使用 AMS 控制台	126
使用 AMS API 和 CLI	127
用于 REST 调用的 AMS API HTTP	128
安装或升级 AMS CLI	128
在 CLI、Ruby、Python 和 Java 中使用 AMS API	129
AMS 自备 EPS	138
为你的账户开启 BYOEPS	139
接收 AMS 通知	142

带有 SNS 的 AMS AMI 通知	143
服务通知	146
RFC 状态变更通知	147
设置私有和公有 DNS	150
AMS 出口流量管理	151
部署 IAM 资源	152
自动配置 IAM	153
使用 IAM 角色和个人资料设置权限	168
请求新的 IAM 用户角色或实例配置文件	169
使用 IAM 角色策略声明限制权限	169
使用 EC2 Amazon IAM 实例配置文件限制权限	171
AD FS 声明规则和 SAML 设置	171
ADFS 声明规则配置	171
Web 控制台	172
使用 SAML 访问 API 和 CLI	172
使用网络 ACL 进行限制	176
Outposts 上的 AMS	176
AWS Outposts 安装和运营管理	176
在上配置 AMS 托管资源 AWS Outposts	178
AMS 开启的局限性 AWS Outposts	179
AMS 关于 AWS Outposts 合规性	180
AMS 开启 AWS Outposts FAQs	180
使用标签	182
AMS 基础设施自动标记	183
AMS 推荐的标签	185
标记批量更新注意事项	188
资源调度程序	189
部署资源调度器	190
自定义资源调度器	191
使用资源调度器	191
AMS 资源调度器成本估算器	192
AMS 资源调度器最佳实践	193
AWS Systems Manager 在 AMS 高级版中	194
可用的 AMS 高级 SSM 文档	194
AMS 高级 SSM 文档版本	195
Systems Manager 定价	195

离线 AMS 账户	195
从单账号 landing zone 账户中脱颖而出	196
从多账号 landing zone 账户中脱颖而出	199
更改管理模式	214
模式概述	215
AMS 中的模式和账户类型	215
AMS 模式 and 应用程序或工作负载	218
AMS 模式的真实用例	222
RFC 模式	225
了解有关 RFCs	225
什么是变更类型？	257
对 RFC 错误进行故障排除	268
直接更改模式	276
直接更改模式入门	277
安全性和合规性	279
直接更改模式下的变更管理	283
使用“直接更改”模式创建堆栈	285
直接更改模式用例	288
开发者模式	289
开发者模式入门	290
安全与合规	291
变更管理	293
预调配基础设施	297
侦测性控制	298
记录、监控和事件管理	298
事件管理	298
补丁管理	298
连续性管理	298
安全和访问管理	299
AMS 中的自助服务配置模式	299
AMS 中的 SSP 模式入门	300
Amazon API Gateway	300
Alexa for Business	301
亚马逊 AppStream 2.0	302
Amazon Athena	304
Amazon Bedrock	305

亚马逊 CloudSearch	306
Amazon S CloudWatch ynthetic	307
Amazon Cognito	308
Amazon Comprehend	309
Amazon Connect	310
Amazon Data Firehose	311
Amazon DevOps Guru	312
Amazon DocumentDB (与 MongoDB 兼容)	313
Amazon DynamoDB	314
Amazon Elastic Container Registry	315
EC2 Image Builder	316
Amazon ECS 已开启 AWS Fargate	317
亚马逊 EKS 开启 AWS Fargate	319
Amazon EMR	322
Amazon EventBridge	324
Amazon Forecast	326
Amazon FSx	328
FSx 适用于 OpenZFS 的亚马逊	330
FSx 适用于 NetApp ONTAP 的亚马逊	331
Amazon Inspector Classic	332
Amazon Kendra	333
Amazon Kinesis Data Streams	334
Amazon Kinesis Video Streams	334
Amazon Lex	335
Amazon MQ	336
适用于 Apache Flink 的亚马逊托管服务	337
Amazon Managed Streaming for Apache Kafka	338
Amazon Managed Service for Prometheus	339
Amazon Personalize	339
亚马逊 QuickSight	342
Amazon Rekognition	343
亚马逊 SageMaker AI	344
Amazon Simple Email Service	347
Amazon Simple Workflow Service	348
Amazon Textract	348
Amazon Transcribe	349

Amazon WorkSpaces	350
AMS 代码服务	351
AWS Amplify	354
AWS AppSync	355
AWS App Mesh	356
AWS Audit Manager	356
AWS Batch	357
AWS Certificate Manager	358
AWS 私有证书颁发机构	359
AWS CloudEndure	362
AWS CloudHSM	363
AWS CodeBuild	364
AWS CodeCommit	365
AWS CodeDeploy	367
AWS CodePipeline	368
AWS Compute Optimizer	369
AWS DataSync	370
AWS Device Farm	371
AWS Elastic Disaster Recovery	372
AWS Elemental MediaConvert	373
AWS Elemental MediaLive	374
AWS Elemental MediaPackage	374
AWS Elemental MediaStore	375
AWS Elemental MediaTailor	376
AWS Global Accelerator	377
AWS Glue	377
AWS Lake Formation	379
AWS Lambda	380
AWS License Manager	381
AWS Migration Hub	382
AWS Outposts	382
AWS Resilience Hub	383
AWS Secrets Manager	384
AWS Security Hub CSPM	386
AWS Service Catalog AppRegistry	387
AWS Shield	388

AWS Snowball Edge	389
AWS Step Functions	390
AWS Systems Manager 参数存储	391
AWS Systems Manager 自动化	392
AWS Transfer Family	394
AWS Transit Gateway	395
AWS WAF	396
AWS Well-Architected Tool	397
AWS X-Ray	398
VM Import/Export	399
客户管理模式	400
开始使用客户管理模式	400
AMS 和 AWS Service Catalog	400
Service Catalog 入门	401
开始之前 AMS 中的 Service Catalog	401
查找您需要的数据 (SKMS)	404
什么是服务知识管理？	404
查找 VPC IDs	405
查找子网 IDs	407
查找 AMI IDs	409
查找安全组 (SG) IDs	410
查找 IAM 实体	411
查找堆栈 IDs	411
查找实例 IDs 或 IP 地址	413
查找 ARNs	415
通过 ARN 查找资源	417
查找账户设置	418
查找 FQDNs	419
查找可用区 (AZs)	420
查找 SNS 话题	420
查找备份设置	421
访问权限管理	422
什么是访问管理？	422
我们访问您的账户的原因和时间	423
如何以及何时使用 root	427
AMS 高级控制台和 Amazon EC2 访问权限	428

访问 AWS 管理控制台和 AMS 控制台	428
临时访问 AMS 控制台	428
使用堡垒访问实例	429
DNS 友好的堡垒名称	431
节省购买单账户着陆区 (SALZ) 堡垒的成本	432
使用堡垒 IP 地址	432
实例访问示例	433
AMS 账户中基于团队或角色的访问控制	442
自动配置 EC2 实例	443
自动配置实例的先决条件	443
SSM 代理自动安装	444
先决条件	444
请求自动安装 SSM 代理	445
SSM 代理自动安装的工作原理	445
自动更改	445
在 Linux 实例上自动更新代码	446
在 Linux 实例上自动更新 PBIS	446
自动更新 SSM 和 CloudWatch 代理的最低版本	447
CloudWatch 配置文件，更新详细信息	448
自动配置的日志	448
监控和事件管理	450
什么是监控？	451
AMS 监控系统监控什么？	452
单账户登录区主动监控 Active Directory 信任	452
监控的工作原理	452
EC2 实例分组通知	453
基于标签的警报通知	454
查看账户的监控配置	455
更改账户的监控配置	455
AMS 中的应用程序感知事件通知	456
AppRegistry 在您的 AMS 账户中配置并创建应用程序	456
创建标签以丰富案例	456
为您的应用程序自定义 AMS 支持案例的严重性	457
查看所需权限	457
使用 OpsCenter	458
警报通知	459

接收警报	459
基于标签的警报通知	459
AMS 自动修复警报	460
创建其他 CloudWatch 警报	467
创建自定义 CloudWatch 指标和警报	468
使用适用于 .Net 和 SQL 服务器的 CloudWatch 应用程序见解	469
AMS 事件路由器	470
AMS 部署的 Amazon EventBridge 托管规则	470
为 AMS 创建托管规则	471
编辑 AMS 的托管规则	471
删除 AMS 的托管规则	471
受信任的修正者	471
主要优势	471
可信修正者的工作原理	472
关键术语	472
开始使用“可信修正者”	473
支持的 Compute Optimizer 建议	476
支持的 Trusted Advisor 支票	478
配置检查补救措施	521
执行模式决策工作流程	524
配置补救教程	524
处理补救措施	526
修复日志	530
最佳实践	533
FAQs	533
日志管理	535
什么是日志管理？	535
AMS 日志的工作原理	535
访问 日志	535
AMS 聚合服务日志	536
AMS 共享服务日志	548
亚马逊弹性计算云 (Amazon EC2)-系统级日志	550
与 Splunk 集成	552
自定义您的日志配置	552
更改 CloudWatch 日志保留期	552
为支持的服务启用日志记录	553

安全管理	554
AMS 中的数据保护	554
Amazon Macie	555
GuardDuty	556
亚马逊 Route 53 解析器 DNS 防火墙	558
AWS Certificate Manager (ACM) 证书	559
AMS 中的数据加密	560
身份和访问管理	561
多账户登录区 (MALZ) IAM 保护措施	561
使用身份进行身份验证	562
安全事件日志记录和监控	582
端点安全 (EPS)	582
恶意软件缓解流程	586
亚马逊 Inspector 安全	588
AMS 事件响应	589
合规性验证	590
多账户登录区查看您的合规状态 AWS Config 规则	590
AMS 多账户 landing zone 服务控制策略限制	591
恢复能力	591
基础结构安全性	592
安全最佳实践	622
AMS 多账号 landing zone EPS 非默认设置	622
AMS 护栏	622
MALZ 服务控制策略	622
安全事件响应	622
工作原理	623
准备	623
Detect	624
分析	625
遏制	626
根除	627
恢复	628
事故后报告	628
安全事件响应操作手册	629
在 AMS Advanced 中更改请求安全审查	633
客户安全风险管理工作流程	633

AMS 高级技术标准	634
AMS 高级版中的标准控件	635
在您的环境中引入高或非常高的安全风险의更改	654
连续性管理	657
什么是连续性管理？	657
连续性管理的工作原理	657
备份计划	657
备份保管库	661
Backup 更改类型	662
监控和报告备份	662
灾难恢复响应	663
灾难恢复计划	663
多站点或高可用性 (HA)	664
温备用	665
指示灯	666
备份与还原	667
补丁管理	671
AMS Patch Orchestrator : 基于标签的修补模型	672
使用补丁编排器	673
补丁编排器先决条件	676
补丁窗口	677
补丁通知	678
补丁基准	680
补丁 Orchestrator 保留标签	681
按需修补	681
AMS 标准补丁	681
支持的操作系统	682
支持的补丁	683
修补和基础架构设计	685
AMS 标准补丁的工作原理	685
AMS 标准修补失败	689
您可以在 AMS 标准修补中采取的操作	690
AMS 标准补丁 FAQs	692
修补服务承诺	694
标准修补	694
关键补丁	696

报告和选项	699
应要求报告	699
AMS 补丁报告	699
AMS Backup 报告	706
“已防止的事件和监控热门话题者” 报告	709
账单费用明细报告	711
可信修正者报告	712
自助报告	714
内部 API 操作	715
补丁报告（每日）	718
Backup 报告（每日）	726
事件报告（每周）	729
账单报告（每月）	732
汇总报告	734
AMS 自助服务报告仪表板	736
数据保留策略	741
从 SSR 中脱颖而出	742
获取支持	743
事件管理	743
什么是事件管理？	744
事件管理服务承诺	745
事件管理示例	747
服务请求管理	752
何时使用服务请求	753
服务请求管理的工作原理	753
测试服务请求	754
创建服务请求	754
监控和更新服务请求	756
响应 AMS 生成的服务请求	758
账单问题	758
按需运营	759
按需请求 AMS 操作	764
对按需运营产品进行更改	764
文档历史记录	766
早期更新	778
.....	dccc

什么是 AWS Managed Services ?

欢迎来到 AWS Managed Services (AMS)，这是亚马逊网络服务的基础设施运营管理 (AWS)。AMS 是一项企业服务，可为您的 AWS 基础设施提供持续管理。

本用户指南面向 IT 和应用程序开发专业人员。假设对 IT 功能、网络和应用程序部署术语和实践有基本的了解。

AMS 实施最佳实践并维护您的基础架构，以降低您的运营开销和风险。AMS 提供全生命周期服务，用于配置、运行和支持您的基础架构，并自动执行变更请求、监控、补丁管理、安全和备份服务等常见活动。AMS 会强制执行您的企业和安全基础设施政策，并使您能够使用首选的开发方法开发解决方案和应用程序。

要更好地了解 AMS 架构，请参阅[以下图表](#)。

主题

- [关于本 AMS 用户指南](#)
- [AMS 作战计划](#)
- [开始使用 AWS Managed Services](#)
- [AMS 关键术语](#)
- [服务描述](#)
- [AMS 信息资源](#)
- [AMS 合规性](#)
- [AMS Amazon 机器映像 \(AMIs\)](#)
- [AD FS 和 AMS 之间的集成是如何工作的](#)
- [AMS 托管活动目录](#)
- [AMS 应用程序部署](#)

Note

AWS 区域 经常添加新内容。有关最新的 AMS 支持和最新的 AMS 支持的操作系统 AWS 区域，请参阅[支持的配置](#)。
要了解更多信息 AWS 区域，请参阅[管理 AWS 区域](#)。

AMS 力求根据您的反馈不断改进我们的服务。我们使用多种机制来实现您的自助服务，自动执行重复性任务，AWS 服务 并在新功能发布时实施这些功能。您可以随时提交 AMS 服务申请，以提出新功能或功能改进建议。

AMS 的工作时间为每年 365 天、每周 7 天、每天 24 小时。

AMS 遵循一套 IT 服务管理 (ITSM) 实践，重点是 IT 服务与您的业务需求保持一致。

关于本 AMS 用户指南

本用户指南适用于拥有多个账户或单账户登录区域的 AMS Advanced 客户。有关 AMS 着陆区产品的更多详情，请参阅 [AMS 关键条款](#)；另请参阅[多账户着陆区架构](#)和[单账户着陆区架构](#)。

AMS 作战计划

AWS Managed Services (AMS) 有两个运营计划可供选择：AMS Accelerate 和 AMS Advanced。运营计划提供一组特定的功能，并且具有不同的服务级别、技术能力、要求、价格和限制。我们的运营计划使您可以灵活地为每个 AWS 工作负载选择合适规模的运营能力。本节概述了与每个计划相关的功能和差异，以及与每个计划相关的责任、功能和好处，以便您可以了解哪种运营计划最适合您的客户。

有关两个运营计划的详细功能比较，请参阅 [AWS Managed Services 功能](#)。

AMS 加快运营计划

AMS Accelerate 是 AMS 运营计划，可帮助您对新环境或现有 AWS 环境进行 day-to-day 基础设施管理。AMS Accelerate 提供运营服务，例如监控、事件管理和安全。AMS Accelerate 还为需要定期修补的 EC2 基于 Amazon 的工作负载提供了可选的补丁插件。

使用 AMS Accelerate，AWS 账户 您可以决定希望 AMS Accelerate 运营哪个 AWS 区域、您希望 AMS Accelerate 运营的 AWS 区域、所需的附加组件以及所需的服务级别协议 (SLAs)。有关更多详细信息，请参阅[使用 AMS Accelerate 运营计划](#)和[服务描述](#)。

AMS 高级操作计划

AMS Advanced 提供全生命周期服务，用于配置、运行和支持您的基础架构。除了 AMS Accelerate 提供的运营服务外，AMS Advanced 还包括其他服务，例如着陆区管理、基础设施变更和配置、访问管理和端点安全。

AMS Advanced 会部署一个着陆区，您可以将 AWS 工作负载迁移到该着陆区并获得 AMS 运营服务。我们的托管多账户登录区域预先配置了基础设施，以促进身份验证、安全、联网和日志记录。

AMS Advanced 还包括变更和访问管理系统，该系统通过防止未经授权的访问或对您的 AWS 基础设施进行风险更改来保护您的工作负载。客户需要使用我们的变更管理系统创建变更申请 (RFC)，才能在您的 AMS Advanced 账户中实施大多数更改。您可以根据由我们的安全和运营团队预先审查的自动变更库进行创建 RFCs，或者如果认为这些更改既安全又受到 AMS Advanced 支持，则可以申请手动更改，然后由我们的运营团队进行审查和实施。

AMS Advanced 还提供不同的功能 SLAs。有关更多信息，请参阅 [AWS Managed Services AMS 高级服务说明](#)。

开始使用 AWS Managed Services

有关开始使用多账户 landing zone [one AMS 服务的详细信息](#)，请参阅 [AWS Managed Services 入门简介](#)。这两份入门指南提供了服务的描述和需要考虑的问题，以帮助您入门。在 [AWS Managed Services 资源中查看功能集](#) [AWS Managed Services 功能和当前资源](#)。

AMS 关键术语

- AMS Advanced：AMS 高级文档的“服务描述”部分中描述的服务。参见 [服务说明](#)。
- AMS 高级 AWS 账户：始终符合 AMS 高级入职要求中所有要求的账户。有关 AMS Advanced 权益、案例研究以及联系销售人员的信息，请参阅 [AWS Managed Services](#)。
- AMS 加速 AWS 账户：始终满足 AMS 加速入职要求中所有要求的账户。请参阅 [AMS 加速入门](#)。
- AWS Managed Services：AMS 和/或 AMS 加速。
- AWS Managed Services 账户：AMS 账户和/或 AMS Accelerate 账户。
- 关键建议：AWS 通过服务请求发布的建议，告知您必须采取行动来防范潜在的风险或资源中断或。AWS 服务如果您决定在指定日期之前不遵守关键建议，则您应对您的决定造成的任何损害承担全部责任。
- 客户请求的配置：以下文件中未标识的任何软件、服务或其他配置：
 - 加速：[支持的配置](#)或 [AMS 加速；服务描述](#)。
 - AMS 高级：[支持的配置](#)或 [AMS 高级；服务描述](#)。
- 事件沟通：AMS 通过在 AMS Accelerate 的 Support Center 和 AMS 控制台中创建的事件向您传达事件，或者您通过在 AMS Accelerate 的 AMS 控制台中创建的事件请求与 AMS 发生的事件。AMS Accelerate 控制台在控制面板上提供事件和服务请求摘要，并提供指向 Support Center 的链接以获取详细信息。

- 托管环境：由 AMS 运营的 AMS 高级账户和/或 AMS Accelerate 账户。

对于 AMS Advanced，这些账户包括多账户着陆区 (MALZ) 和单账户着陆区 (SALZ) 账户。

- 账单开始日期：AWS 收到您在 AWS Managed Services 入职电子邮件中要求的信息后的下一个工作日。AWS Managed Services 入职电子邮件是指向您发送的电子邮件，AWS 用于收集在您的账户上激活 AWS Managed Services 所需的信息。

对于您随后注册的账户，账单开始日期为 AWS Managed Services 为已注册账户发送 AWS Managed Services 激活通知后的第二天。AWS Managed Services 激活通知发生在以下情况下：

1. 您授予对兼容 AWS 账户的访问权限并将其移交给 AWS Managed Services。
 2. AWS Managed Services 设计和建立 AWS 托管服务账户。
- 服务终止：您可以出于任何原因终止所有 AWS Managed Services 账户的 AWS Managed Services 账户的 AWS 托管服务，方法是通过服务请求提供至 AWS 少 30 天的通知。在服务终止日期，可以：
 1. AWS 将所有 AWS Managed Services 账户或指定的 AWS Managed Services 账户（如果适用）的控制权移交给您，或者
 2. 双方删除 AWS 允许从所有 AWS Managed Services 账户或指定的 AWS Managed Services 账户进行访问的 AWS Identity and Access Management 角色（如果适用）。
 - 服务终止日期：服务终止日期是必需的 30 天终止通知期结束后的日历月的最后一天。如果必要的终止通知期限在日历月的第20天之后，则服务终止日期为下一个日历月的最后一天。以下是终止日期的示例方案。
 - 如果终止通知是在4月12日提供的，则为期30天的通知将于5月12日结束。服务终止日期为5月31日。
 - 如果在4月29日发出终止通知，则为期30天的通知将于5月29日结束。服务终止日期为 6 月 30 日。
 - 提供 AWS Managed Services：从服务开始之日起，您可以访问和使用每个 AWS 托管服务账户的 AWS 托管服务。
 - 终止指定的 AWS Managed Services 账户：您可以出于任何原因终止指定 AWS Managed Services 账户的 AWS 托管服务，方法是通过服务请求（“AMS 账户终止申请”）AWS 发出通知。

事件管理条款：

- 事件：您的 AMS 环境发生了变化。
- 警报：每当来自支持的事件 AWS 服务 超过阈值并触发警报时，系统就会创建警报并将通知发送到您的联系人列表。此外，还会在您的事件列表中创建事件。

- 事件：您的 AMS 环境或 AWS Managed Services 的计划外中断或性能降级，导致影响，如 AWS Managed Services 或您所报告的那样。
- 问题：一个或多个事件共同根本原因。
- 事件解决或解决事件：
 - AMS 已将与该事件相关的所有不可用 AMS 服务或资源恢复到可用状态，或者
 - AMS 已确定不可用的堆栈或资源无法恢复到可用状态，或者
 - AMS 已启动经您授权的基础设施恢复。
- 事件响应时间：创建事件与 AMS 通过控制台、电子邮件、服务中心或电话提供初始响应之间的时间差。
- 事件解决时间：AMS 或您创建事件与事件解决时间之间的时间差。
- 事件优先级：AMS 或您如何将事件的优先级分为“低”、“中”或“高”。
 - 低：您的 AMS 服务存在非严重问题。
 - 中：您的托管环境中的 AWS 服务可用，但未按预期运行（根据适用的服务描述）。
 - 高：(1) AMS 控制台或托管环境 APIs 中的一个或多个 AMS 不可用；或 (2) 托管环境中的一个或多个 AMS 堆栈或资源不可用，且不可用会使您的应用程序无法执行其功能。

AMS 可以根据上述指南对事件进行重新分类。

- 基础设施恢复：根据受影响堆栈的模板重新部署现有堆栈，并在无法解决事件时根据上次已知的还原点启动数据恢复，除非您另行指定。

基础设施条款：

- 托管生产环境：客户生产应用程序所在的客户帐户。
- 托管的非生产环境：仅包含非生产应用程序（例如用于开发和测试的应用程序）的客户帐户。
- AMS 堆栈：由 AMS 作为一个单元管理的一组或多个 AWS 资源。
- 不可变基础设施：Amazon A EC2 uto Scaling 组 (ASGs) 的典型基础设施维护模式，在这种模式中 AWS，每次部署都会替换更新的基础设施组件（在 AMI 中），而不是就地更新。不可变基础架构的优势在于，所有组件都保持同步状态，因为它们总是从同一个基础生成的。不可变性独立于任何用于构建 AMI 的工具或工作流程。
- 可变基础设施：一种典型的基础设施维护模型，适用于不是 Amazon A EC2 uto Scaling 组且包含单个实例或仅包含几个实例的堆栈。该模型最接近于传统的、基于硬件的系统部署，即在系统生命周期开始时部署系统，然后随着时间的推移将更新分层到该系统上。系统的任何更新都将单独应用于实例，并且可能由于应用程序或系统重启而导致系统停机（取决于堆栈配置）。

- 安全组：您的实例的虚拟防火墙，用于控制入站和出站流量。安全组在实例级别运行，而不是子网级别。因此，您的 VPC 子网中的每个实例都可以为其分配一组不同的安全组。
- 服务级别协议 (SLAs)：与您签订的 AMS 合同的一部分，其中定义了预期的服务级别。
- SLA 不可用和不可用：
 - 您提交的导致错误的 API 请求。
 - 您提交的控制台请求生成 5xx HTTP 响应（服务器无法执行请求）。
 - 如 Service Health Dashboard 所示，在 AMS 管理的基础设施中构成堆栈或资源的任何 AWS 服务产品都处于“[服务](#)中断”状态。
 - 在确定服务积分资格时，不考虑因 AMS 排除而直接或间接导致的不可用性。除非服务符合不可用标准，否则视为可用。
- 服务级别目标 (SLOs)：与您签订的 AMS 合同的一部分，其中定义了 AMS 服务的具体服务目标。

修补条款：

- 强制补丁：关键安全更新，用于解决可能危及您的环境或账户安全状态的问题。“关键安全更新”是由 AMS 支持的操作系统的供应商评为“严重”的安全更新。
- 已发布补丁与计划发布补丁：补丁通常按计划发布和发布。紧急补丁是在发现需要补丁时宣布的，通常不久之后，补丁就会发布。
- 补丁附加组件：针对 AMS 实例进行基于标签的修补，它利用 AWS Systems Manager (SSM) 功能，因此您可以使用基准和您配置的窗口标记实例并对这些实例进行修补。
- 补丁方法：
 - 就地修补：通过更改现有实例完成的修补。
 - AMI 替换补丁：通过更改现有 Amazon EC2 Auto Scaling 组启动配置的 AMI 参考参数来完成的修补。
- 补丁提供商（操作系统供应商、第三方）：补丁由应用程序的供应商或管理机构提供。
- 补丁类型：
 - 关键安全更新 (CSU)：被支持的操作系统的供应商评为“严重”的安全更新。
 - 重要更新 (IU)：被支持的操作系统的供应商评为“重要”的安全更新或评级为“严重”的非安全更新。
 - 其他更新 (OU)：供应商对不是 CSU 或 IU 的支持的操作系统的更新。
- 支持的补丁：AMS 支持操作系统级补丁。供应商发布升级是为了修复安全漏洞或其他错误或提高性能。有关当前支持的列表 OSs，请参阅 [Support 配置](#)。

安全条款：

- **Det@@ective Controls**：由 AMS 创建或启用的监控器组成的库，用于持续监督客户托管的环境和工作负载，以发现与安全、运营或客户控制不一致的配置，并通过通知所有者、主动修改或终止资源来采取行动。

服务请求条款：

- **服务请求**：您请求采取行动，希望 AMS 代表您采取行动。
- **警报通知**：AMS 在触发 AMS 警报时在您的服务请求列表页面上发布的通知。为您的账户配置的联系人也会通过配置的方法（例如电子邮件）收到通知。如果您的实例/资源上有联系人标签，并且已同意您的云服务交付经理 (CSDM) 接收基于标签的通知，则还会通知标签中的联系人信息（密钥值）以获取自动的 AMS 警报。
- **服务通知**：AMS 发布到您的服务请求列表页面的通知。

其他术语：

- **AWS Managed Services 接口**：适用于 AMS：AWS Managed Services 高级控制台、AMS CM AP 支持 I 和 API。对于 AMS Accelerate：支持 控制台和 支持 API。
- **客户满意度 (CSAT)**：AMS CSAT 通过深入分析获得信息，包括每个案例或信件的案例信件评级（如果给出）、季度调查等。
- **DevOps**：DevOps 是一种开发方法，强烈倡导在所有步骤上实现自动化和监控。DevOps 旨在通过在自动化基础上整合传统上独立的开发和运营功能，缩短开发周期，提高部署频率和更可靠的发布。当开发人员可以管理运营，运营为开发提供信息时，问题和问题就会更快地发现和解决，业务目标也更容易实现。
- **ITIL**：信息技术基础设施库（称为 ITIL）是一个 ITSM 框架，旨在标准化 IT 服务的生命周期。ITIL 分为五个阶段，涵盖了 IT 服务生命周期：服务策略、服务设计、服务过渡、服务运营和服务改进。
- **IT 服务管理 (ITSM)**：一套让 IT 服务与您的业务需求保持一致的实践。
- **托管监控服务 (MMS)**：AMS 运营自己的监控系统，即托管监控服务 (MMS)，该系统使用 AWS 健康事件并汇总亚马逊数据 AWS 服务和其他数据，将通过 CloudWatch 亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题创建的任何警报通知 AMS 操作员（全天候在线）。
- **命名空间**：在创建 IAM 策略或使用 Amazon 资源名称 (ARNs) 时，您可以使用命名空间来识别。AWS 服务 您可以使用命名空间来标识操作和资源。

服务描述

AMS Advanced (AMS) 是 AWS Managed Services 服务的一项运营计划，用于管理您的 AWS 基础设施的运营。AMS Advanced 提供日常基础设施操作，例如补丁、连续性管理、安全管理，以及 IT 管理流程，例如事件、变更和服务请求管理。有关支持的服务的列表，请参阅 [支持的 AWS 服务](#)。

YouTube 视频：[AMS 如何帮助我在云端实现卓越运营？](#)

主题

- [AWS Managed Services \(AMS\) AMS 高级运营计划功能](#)
- [我们做什么，不做什么](#)
- [AMS 责任矩阵 \(RACI\)](#)
- [AMS 环境基本组件](#)
- [AMS 账户限额](#)
- [AMS 服务级别目标 \(SLOs\)](#)
- [支持的 AWS 服务](#)
- [支持的配置](#)
- [适用于 AMS 中不支持的操作系统的功能](#)
- [AMS 高级接口](#)
- [AMS VPC 终端节点](#)
- [AMS 保护的命名空间](#)
- [AMS 保留的前缀](#)
- [AMS 维护窗口](#)

AWS Managed Services (AMS) AMS 高级运营计划功能

AMS Advanced 为支持的 AWS 服务提供以下功能：

- 记录、监控、防护和事件管理：

AMS 配置和监控您的托管环境以记录活动，并根据各种运行状况检查定义警报。AMS 会针对适用的 AWS 服务对警报进行调查，对您使用这些服务产生负面影响的警报会导致事件的产生。AMS 汇总并存储在、中执行所有操作后生成的所有日志 CloudWatch CloudTrail，并将系统日志存储在 Amazon S3 中。您可以要求设置其他警报。除了 AMS 的预防性控制措施外，AMS 还部署了配置护栏和侦测

控件，以持续保护您免受可能降低托管账户运营和安全完整性的错误配置的影响，从而加强您的控制措施，例如标记和合规性。当检测到受监控的控件时，会生成警报，根据您可以修改的预定义的 AMS 默认值发出通知、修改或终止资源。

- 连续性管理 (Backup and Restore) :

AMS 使用标准的现有 AWS Backup 功能按您确定的计划间隔提供资源备份。AMS 可使用您的 RFC 执行从特定快照中恢复操作。在快照间隔之间发生的数据更改由您负责备份。您可以为计划间隔之外的备份或快照请求提交 RFC。如果某个 AWS 区域的可用区 (AZ) 不可用，在您允许的情况下，AMS 会根据模板和受影响堆栈的可用的 EBS 快照重新创建新的堆栈，从而恢复托管环境。

- 安全和访问管理 :

AMS 提供端点安全 (EPS)，例如配置防病毒和防恶意软件保护。您也可以使用自己的 EPS 工具和流程，而不是使用名为“自带 EPS (BYOEPS)”的功能将 AMS 用于 EPS。AMS 还会配置您在入职期间批准的默认 AWS 安全功能，例如 AWS Identity and Access Management (IAM) 角色和亚马逊 EC2 安全组，并使用标准 AWS 工具（例如 Amazon Macie AWS Security Hub CSPM、Amazon GuardDuty on) 来监控和响应安全问题。您可以通过您提供的经批准的目录服务来管理您的用户。有关批准的目录服务的列表，请参阅[支持的配置](#)。

AMS 包括端点安全 (EPS) (包括防病毒 (AV)) 和反恶意软件保护、恶意软件和入侵检测 (趋势科技)。安全组是根据堆栈模板定义的，并在启动时根据应用程序 (公共/私有) 安全组的可见性进行修改。

通过变更管理变更请求 (RFCs) 来请求访问系统。访问管理提供对不同资源的访问权限，例如 Amazon EC2 实例 AWS 管理控制台、和 APIs。在入职和联合到 AWS 期间与 AMS Microsoft Active Directory 部署建立单向信任后，您可以使用现有的公司证书进行所有互动。

- 补丁管理 :

AMS 会为支持的操作系统 (OSs) 和预先安装有支持的操作系统的应用的 EC2 实例应用和安装更新。有关支持的操作系统的列表，请参阅[支持的配置](#)。

AMS 提供两种修补模式 :

- AMS 标准补丁，用于传统的基于账户的修补，以及
- AMS Patch Orchestrator，用于基于标签的修补。

在 AMS 标准补丁中，您可以选择每月维护时段，让 AMS 执行大多数修补活动。AMS 在选定的维护时段之外应用关键安全更新 (带有相应的通知)，并在选定的维护时段内应用重要更新。AMS 还会在选定的维护时段内对基础设施管理工具进行更新。如果需要，您可以将堆栈从补丁管理中排除或拒绝更新。

使用 AMS Patch Orchestrator，每个账户的默认维护窗口由您定义，让 AMS 执行修补活动。您可以为 AMS 安排额外的自定义维护时段，以便使用标签修补您定义的一组特定实例。AMS 会应用所有可用更新，但您可以通过创建自定义补丁基准来筛选或拒绝更新。对于这两种型号，如果您批准或拒绝补丁管理下提供的更新，但后来改变了主意，则您有责任通过 RFC 启动更新。AMS 会跟踪资源的补丁状态，并在月度业务评估中重点介绍不是最新的系统。补丁管理仅限于托管环境中的堆栈，包括所有 AMS 托管应用程序和具有修补功能的支持 AWS 服务（例如 RDS）。为了在发布更新时支持所有类型的基础设施配置，AMS a) 更新 EC2 实例，b) 提供更新后的 AMS AMI 供您使用。您有责任安装、配置、修补和监控上面未具体介绍的任何其他应用程序。

- 变更管理：

AMS 变更管理是您控制托管环境中变更的机制。AMS 结合使用预防和检测控制来简化这一过程，并根据所选的 AMS 模式提供不同的控制级别和相关风险。

您的 AMS 环境中的所有操作都已登录 AWS CloudTrail。

有关 AMS 变更管理和不同模式的更多信息，请参阅 [AMS 变更管理指南](#) 和 [AMS 模式](#)。

- 自动化和自助式资源调配管理：

您可以通过多种方式在 AMS Advanced 上配置 AWS 资源：

- 提交配置和配置更改请求 (RFCs)
- 通过 AWS 服务目录进行部署
- 通过“[直接更改](#)”模式部署
- 通过[开发者模式](#)部署。请记住，通过开发者模式创建的资源不由 AMS 管理。
- 使用精选服务的自助配置直接配置 AWS 服务 AWS 服务（参见[支持的 AWS 服务](#)）。

- 事件管理：

AMS 会主动通知您 AMS 检测到的事件。AMS 会对客户提交的事件和 AMS 生成的事件做出回应，并根据事件优先级解决事件。除非您另有指示，否则 AMS 认定对您的托管环境安全构成风险的事件以及与 AMS 和其他 AWS 服务可用性有关的事件，均会主动采取行动。获得您的授权后，AMS 会对所有其他事件采取行动。问题管理流程可以解决反复出现的事件。

- 问题管理：

AMS 进行趋势分析以识别和调查问题并确定根本原因。问题可以通过变通方法或永久解决方案进行修复，以防止将来再次出现类似的 future 服务影响。任何“高”事件一经解决，均可要求提供事后报告 (PIR)。PIR 捕捉了根本原因和采取的预防措施，包括预防措施的实施。

- 报告：

AMS 为您提供月度服务报告，其中汇总了 AMS 的关键绩效指标，包括执行摘要和见解、运营指标、托管资源、AMS 服务水平协议 (SLA) 遵守情况，以及有关支出、节省和成本优化的财务指标。报告由分配给您的 AMS 云服务交付经理 (CSDM) 交付。

- 服务请求管理：

要请求有关您的托管环境、AMS 或 AWS 服务产品的信息，请使用 AMS 控制台提交服务请求。您可以提交服务申请，询问有关 AWS 服务和功能的“操作方法”问题，也可以申请其他 AMS 服务。

- 服务台：

AMS 为工程运营配备全职亚马逊员工，以满足非自动化的请求，包括事件管理、服务请求管理和变更管理。服务台每年 365 天全天候运营。

- 指定资源：

为每位客户分配一名云服务交付经理 (CSDM) 和一名云架构师 (CA)。

- CSDMs 可以直接联系。他们在实施、迁移和运营生命周期的所有阶段进行服务审查、交付报告和见解。CSDMs 每月进行业务审查，并详细说明财务支出、成本节约建议、服务利用率和风险报告等项目。他们深入研究运营绩效统计数据，并就需要改进的领域提供建议。
- CAs 可以直接联系并提供技术专业知识和帮助您优化 AWS 云的使用。CA 活动示例，包括：选择要迁移的工作负载，协助新增账户和工作负载，在游戏日、灾难恢复测试、问题管理等运营活动中担任技术主管，以及充分利用 AMS 的技术建议。AWS CAs 推动组织各个层面的技术讨论，并协助进行事件管理、权衡取舍、建立最佳实践和技术风险缓解。
- 开发者模式：

此功能允许您直接访问 AWS 服务 APIs 和 AWS 控制台以及访问 AMS 变更管理流程，从而使您能够在 AMS 配置的账户 [1] 中快速迭代基础设施设计和部署。在变更管理流程之外配置或配置了开发者模式权限的资源由您负责管理（请参阅“自动和自助配置管理”）。与 AMS 上的其他变更管理配置的工作负载一样，支持通过 AMS 变更管理流程配置的资源。

- AWS 支持：

AMS 客户可以选择他们需要的 AWS Support 级别来补充其 AMS 运营计划。在 AMS 注册的账户可以订阅 Business Support 或企业支持。要了解支持计划的区别，请参阅 [AWS Support 计划](#)。

- 客户管理的账户：

此功能使您能够在同一个托管环境中申请 AWS 账户，但这些账户中工作负载和 AWS 资源的持续操作则由您负责。AMS 会提供客户管理的账户，但是一旦创建了账户，就不会向这些账户提供其他

AMS 功能或服务。AWS 不会在企业级高级支持中注册客户管理账户。您有责任按照您选择的支持费率在 AWS Support 中注册客户管理的账户。

- 防火墙管理：

AMS 为支持的防火墙服务提供了可选的托管防火墙解决方案，该解决方案允许对托管环境中的网络进行互联网流量过滤。这包括不使用 AWS 网络基础设施且其流量直接流向互联网的面向公众的服务。该解决方案将业界领先的防火墙技术与 AMS 基础设施管理功能相结合，用于部署、监控、管理、扩展和恢复防火墙基础架构。

当您加入 AMS 时，您会收到 AMS 网络基础设施的完整列表。要随时获取为支持 AMS 基础设施而运行的服务的最新列表，请提交服务请求，详细说明您想要的信息。要请求更改您的网络设计，请创建服务请求，描述您要进行的更改，例如，添加 VPC 或请求更改安全组规则。

我们做什么，不做什么

AMS 为您提供部署 AWS 基础设施的标准化方法，并提供必要的持续运营管理。有关角色、职责和支持的服务的完整描述，请参阅[服务描述](#)。

Note

要请求 AMS 提供其他 AWS 服务，请提交服务请求。有关更多信息，请参阅[提出服务请求](#)。

- 我们做什么：

完成入职后，AMS 环境可以接收变更请求 (RFCs)、事件和服务请求。您与 AMS 服务的交互围绕着应用程序堆栈的生命周期。新堆栈是从预先配置的模板列表中订购的，启动到特定的虚拟私有云 (VPC) 子网，在运行期间通过更改请求 (RFCs) 对其进行修改，并全天候监控事件和事件。

主动应用程序堆栈由 AMS 监控和维护，包括修补，除非需要更改或堆栈已停用，否则在堆栈的生命周期内无需采取任何进一步的操作。AMS 检测到的影响堆栈运行状况和功能的事件会生成通知，可能需要也可能不需要您采取措施来解决或验证。可以通过提交服务请求来提出操作方法问题和其他查询。

此外，AMS 还允许您启用不由 AMS 管理的兼容 AWS 服务。有关兼容 AWS-AMS 的服务的信息，请参阅[自助服务配置模式](#)。

- 我们不做什么：

虽然 AMS 通过提供许多手动和自动选项来简化应用程序部署，但您需要负责应用程序的开发、测试、更新和管理。AMS 为影响应用程序的基础设施问题提供故障排除帮助，但 AMS 无法访问或验证您的应用程序配置。

AMS 责任矩阵 (RACI)

Note

为了及时履行其义务，AWS Managed Services (AMS) 可能需要您提供意见，以决定适当的行动方案。AMS 将联系指定的客户联系人，了解所有此类说明和意见。AMS 预计会在 24 个工作日内回复此类询问。如果 24 个工作日内没有回复，AMS 可能会代表您选择采取行动。

负责任、负责、咨询和知情的 AMS (RACI) 矩阵将各种活动的主要责任分配给客户或 AMS。

AMS 管理您的 AWS 基础设施。下表概述了在 AMS 托管环境中运行的应用程序生命周期中客户和 AMS 的责任。

AMS 对客户管理账户或其内运行的基础设施的以下任何活动概不负责；因此，本 RACI 不适用。

- R 代表负责任的一方，负责完成任务。
- C 代表咨询；征求意见的当事方，通常是作为主题专家征求意见的当事方；并与之进行双边沟通。
- 我代表知情；一个通报进展情况的当事方，通常只有在任务或可交付成果完成后才会被告知。
- 自助服务配置是指客户通过 AWS API 或控制台通过自助服务配置的资源，包括开发人员模式和自助配置服务。

Note

有些部分包含针对 AMS 和客户的“R”。这是因为，在责任 AWS 共担模式中，AMS 和客户共同拥有应对基础设施和应用程序问题的所有权。

为了提供自助服务配置功能，AMS 创建了具有权限界限的提升的 IAM 角色，以限制直接访问 AWS 服务的意外更改。角色并不能阻止所有变更，您有责任遵守内部控制和合规性，并验证所使用的所有 AWS 服务是否符合所需的认证。我们称之为自助服务配置模式。有关 AWS 合规性要求的详细信息，请参阅[AWS 合规性](#)。

对于您通过自助服务配置的资源，AMS 通过服务请求提供事件管理、侦探控制和护栏、报告、指定资源（云服务交付经理和云架构师）、安全和访问以及技术支持。此外，在适用的情况下，您负责在 AMS 变更管理系统之外配置或配置的资源连续性管理、补丁管理、基础设施监控和变更管理。

活动	Customer	AWS Managed Services (AMS)
应用程序生命周期		
应用程序开发	R	我
应用基础设施需求分析和设计	R	C
非标准 AMS 堆栈的设计和优化	R	C
AMS 标准堆栈的设计和优化	我	R
应用程序部署	R	C
AWS 基础设施部署	C	R
应用程序监控	R	我
应用程序测试/优化	R	我
AWS 基础设施优化指南	我	R
AWS 基础设施监控	我	R
对应用程序问题进行故障排除和解决	R	C
排查和解决 AWS 网络问题	C	R
对操作系统和基础架构问题进行故障排除和解决	C	R
自助配置	R	C
应用程序和 ITSM 集成		
应用程序与 AWS 服务产品集成	R	C

活动	Customer	AWS Managed Services (AMS)
ITSM 与 AWS Managed Services 接口集成	R	C
联网		
托管环境 VPC 和 VPC 的设置和配置	C	R
为 VPCs (例如 /16) 分配私有地址空间	R	C
配置和运营非 AWS 托管服务 , 由客户管理 Firewalls/Proxy/Bastions/HOSTs	R	C
在托管环境Groups/NAT/Customer Bastions/ NACL中配置和运行 AWS 安全	我	R
客户网络中的网络 (例如 DirectConnect) 配置和实施	R	C
在托管环境中配置和实施网络	C	R
托管环境配置		
为基准堆栈模板定义默认 Auto Scaling 设置	我	R
推荐 RI 优化	C	R
购买 RI 和 PIOP 容量	R	C
容量过剩时移除容量 (当客户应用程序支持时)	C	R
创建/更新 AWS Managed Services 的 AWS 客户特定信息	C	R
S3 配置	C	R
自助配置	R	C
冰川配置	C	R

活动	Customer	AWS Managed Services (AMS)
定义存档策略	R	C
存档策略配置	C	R
选择客户维护时段	R	我
AWS RDS 管理		
监控source/replica/RO复制运行状况	我	R
确定源故障转移的 RCA	我	R
自动快照（备份）配置	C	R
自助配置	R	C
协调和安排数据库引擎补丁管理	C	R
自助配置	R	C
推荐数据库存储空间和 PIOP 容量	C	R
自助配置	R	C
为正在运行的数据库推荐实例大小	C	R
自助配置	R	C
建议对托管环境进行 RI 优化	C	R
自助配置	R	C
RDS 性能监控 (CloudWatch)	C	R
自助配置	R	C
RDS 事件订阅配置 (SNS)	C	R
自助配置	R	C

活动	Customer	AWS Managed Services (AMS)
RDS 安全组配置	C	R
自助配置	R	C
RDS 引擎 parameter/option 配置	R	C
数据库表设计	R	我
数据库索引	R	我
数据库日志分析	R	我
AMS 变更管理		
创建客户 RFCs (例如访问资源creating/updating/deleting managed stacks, deploying/updating应用程序、更改 AWS 服务产品配置)	R	我
批准客户 RFCs	我	R
创建 AWS Managed Services RFCs (例如 , 访问资源、代表客户创建资源、在补丁管理中将更新应用到操作系统)	我	R
批准非自动化 RFCs	R	我
提交新变更类型的请求	R	C
创建新的变更类型	我	R
维护应用程序变更日历	R	C
维护窗口即将到来的通知	我	R
AWS Service Catalog		
创建产品组合和产品	R	我

活动	Customer	AWS Managed Services (AMS)
向最终用户分发产品	R	我
创建标签和标签选项库	R	C
与最终用户共享产品组合和产品	R	我
修改/更新产品组合和产品	R	我
为产品组合和产品创建和分配约束条件	R	C
将服务操作与产品关联	R	C
使用新版本的产品更新已配置的资源	R	我
预置		
AWS Managed Services 基准 AMI 中针对客户的新增内容	R	C
配置用于置备堆栈模板的其他已批准的更改类型	C	R
启动通过 AMS 变更管理流程或 AWS Service Catalog 提交的托管堆栈和相关 AWS 资源。 自助配置	我	R
	R	我
Install/Update 通过 AMS 变更管理流程或 AWS Service Catalog 配置的实例上的自定义应用程序和第三方应用程序。	R	我
资源调配-堆栈架构		
提供操作系统许可 (包括适用的 AWS 服务的使用费, 例如 EC2 和 RDS) 自助配置	我	R
	R	I

活动	Customer	AWS Managed Services (AMS)
通过 AMS 变更管理系统为应用程序部署定义基准基础设施模板（堆栈）。	我	R
	R	I
自助配置		
创建基准已获批准 AMIs ⁸	我	R
评估客户应用程序库存并确定是否适合可用基础架构模板（堆栈）	R	C
定义除基本模板产品之外的独特堆栈	R	C
记录、监控和事件管理		
记录 AWS 基础设施变更日志	我	R
记录所有应用程序更改日志	R	C
安装和配置代理和脚本，用于修补、安全、监控通过 AMS 变更管理流程配置的 AWS 基础设施等。	我	R
	R	C
自助配置		
定义客户特定的监控和事件要求	R	C
为托管环境配置警报	我	R
监控所有 AMS 配置的警报	我	R
自助配置	R	C
调查基础设施警报以获取事故通知	我	R
自助配置	R	C
调查应用程序警报	R	C

活动	Customer	AWS Managed Services (AMS)
事件管理		
根据监控主动通知 AWS 基础设施上的事件	我	R
自助配置	R	C
处理应用程序性能问题和中断	R	我
对事件优先级进行分类	我	R
提供事件响应	我	R
提供事件解决方案/恢复基础架构	C	R
Note SLAs 不适用于在 AMS 变更管理之外配置的基于实例的资源，包括使用自助服务配置和开发者模式配置的资源。		
问题管理		
识别托管环境中的问题	C	R
对托管环境中的问题执行 RCA	C	R
修复托管环境中的问题	C	R
识别和修复应用程序问题	R	我
安全管理		
客户基础设施安全为客户入职期间确定和同意的安全合规流程 and/or 建立基准。	C	R
	R	C
自助配置		

活动	Customer	AWS Managed Services (AMS)
维护托管 EPS 的有效许可证	R	C
配置托管 EPS	我	R
自助配置	R	C
更新托管 EPS	我	R
自助配置	R	C
监控通过 AMS CM 流程配置的实例上的恶意软件。	我	R
	R	C
自助配置		
维护和更新病毒特征。	我	R
自助配置	R	C
修复感染恶意软件的实例。	C	R
自助配置	R	C
安全事件管理	C	R
安全-访问管理		
管理用户的生命周期及其对本地目录服务的权限，这些服务用于访问 AWS Managed Services	R	我
操作联合身份验证系统，以便客户访问 AWS 控制台/ APIs	R	C
接受并维护 AWS Managed Services AD 对客户托管 AD 的活动目录 (AD) 信任	R	C
在入职期间，在每个托管账户中创建跨账户 IAM 管理员角色	R	C

活动	Customer	AWS Managed Services (AMS)
保护每个 AWS 账户的根凭证	我	R
为托管环境定义 IAM 资源	C	R
管理 AMS 工程师访问操作系统的特权凭证	我	R
管理 AMS 向客户提供的操作系统访问权限的特权凭证	R	我
安全事件响应-准备		
通讯		
提供客户安全联系人详细信息，以便 AMS 在安全事件、通知和安全升级期间使用	R	我
存储和管理提供的客户安全联系人详细信息，以便在安全事件和安全升级期间使用	CI	R
训练		
在事件响应过程中向客户提供支持 AMS 的文档	我	R
在安全比赛日的事故响应流程中实践责任共担	RI	RC
资源管理		
AWS 服务 为警报、警报关联、降噪和其他规则配置支持的安全管理	我	R
维护资产 (AWS 资源) 库存，了解资产的价值和重要性。这些信息在事件遏制策略中很有用	R	CI
使用 AWS 标签来识别资源和工作负载	R	CI
定义和配置日志保留和存档	CI	R
配置 AWS 账户、策略和访问管理的安全基准	CI	RC

活动	Customer	AWS Managed Services (AMS)
安全事件响应-检测		
记录、指标和监控		
配置日志记录和监控以启用实例和账户的事件管理	CI	R
支持显示安全警报 AWS 服务 的监视器	我	R
部署和管理端点安全工具	CI	R
使用 AMS 支持的端点安全工具监控实例上的恶意软件	我	R
通过出站消息通知客户检测到的事件	我	R
针对特定客户和工作负载向决策者发送通知和任何后续更新，以缩短事件响应时间	R	CI
定义、部署和维护 AMS 标准检测服务（例如 Amazon GuardDuty 和 AWS Config）	CI	R
记录 AWS 基础架构变更日志	我	RC
启用和配置日志记录、监控以启用应用程序的事件管理	R	C
在支持 AWS 的安全服务（例如 Amazon）上实施和维护允许名单、拒绝名单和自定义检测 GuardDuty	RCI	R
安全事件报告		
将可疑活动或正在进行的安全调查通知AMS	R	CI
将检测到的安全事件和事件通知客户	我	R
通知可能触发安全事件响应流程的计划事件	R	CI

活动	Customer	AWS Managed Services (AMS)
安全事件响应-分析		
调查和分析		
对支持的检测源生成的支持安全警报执行初始响应	我	RC
使用现有数据评估 false/true 阳性	RI	RC
生成受影响实例的快照，以便在需要时与客户共享	我	R
执行取证任务，例如监管链、文件系统分析、内存取证和二进制分析	R	CI
收集应用程序日志以帮助调查	R	我
收集数据和日志，以帮助调查安全警报	RCI	RC
SMEs 参与 AWS 服务 安全调查	CI	R
在调查期间与第三方供应商接触（例如，进行 EPS 反恶意软件调查和与 TrendMicro 支持团队接触）	RCI	我
在调查期间与客户共享支持 AWS 服务 人员的调查日志	我	R
沟通		
从 AMS 检测源为托管资源发送警报和通知	我	R
管理应用程序安全事件的警报和通知	R	我
在安全事件调查期间与客户安全联系人接触	R	我
安全事件响应-包含		

活动	Customer	AWS Managed Services (AMS)
遏制策略和执行		
决定执行商定的遏制策略，并就可能影响控制窗口期间服务可用性的后果达成一致	R	CI
备份受影响的系统以供进一步分析	CI	R
包含应用程序和工作负载（通过应用程序特定的配置或响应活动）	R	CI
根据安全事件和受影响的资源定义遏制策略	CI	R
启用受影响系统的时间点备份的加密和安全存储	CI	R
对 AWS 资源（包括 EC2 实例、网络 and IAM）执行支持的遏制操作	CI	R
安全事件响应-根除		
根除策略和执行		
根据安全事件和客户应用程序工作负载上受影响的资源定义清除选项	R	CI
决定商定的根除策略、执行根除的时间和后果	R	CI
根据安全事件和 AMS 托管工作负载上受影响的资源定义根除步骤	CI	R
消灭和强化 AWS 资源，包括 EC2 实例、网络和 IAM 根除	CI	R
消除和强化应用程序和工作负载（通过应用程序特定的配置或响应活动）	R	我
安全事件响应-恢复		
恢复准备和执行		

活动	Customer	AWS Managed Services (AMS)
根据客户的要求配置备份计划 and 目标	R	我
查看备份计划以恢复 AMS 托管的工作负载	CI	R
对支持的资源执行备份恢复活动 AWS 服务	我	R
备份客户应用程序、应用程序配置和部署设置，并查看备份计划，以便在事后恢复客户应用程序和工作负载	R	我
恢复应用程序和客户工作负载（通过应用程序特定的恢复步骤）	R	我
安全事件响应-事后报告		
事后报告		
根据需要与客户在事后分享适当的经验教训和行动项目	我	R
补丁管理 ⁹		
监控支持的操作系统的适用更新，以及预先安装了支持的操作系统的软件 EC2。	我	R
	R	C
自助配置		
通知客户即将推出的更新（仅适用于 AMS 标准补丁）	我	R
将 and/or 某些更新从修补活动中排除某些堆栈	R	我
定义默认和自定义维护时段计划以及其他参数（例如维护时段持续时间）以应用补丁（适用于 AMS Patch）	R	我
仅限管弦乐器）		

活动	Customer	AWS Managed Services (AMS)
定义自定义补丁基准以筛选和排除特定补丁（仅适用于 AMS Patch Orchestrator）	R	我
标记实例以将其与自定义维护窗口和补丁基准相关联（仅适用于 AMS Patch Orchestrator）	R	我
跟踪资源的补丁状态，并在每月业务评估中突出显示不是最新的系统。	C	R
修补安装在操作系统上的 Windows 操作系统和受 Windows 更新控制的微软软件包 自助配置	我	R
	R	-
修补未由 Windows Update 管理的已安装的应用程序、软件或应用程序依赖关系 自助配置	R	我
	R	-
修补 Linux 操作系统和任何允许操作系统原生软件包管理器管理的软件包（例如 Yum、Apt、Zypper） 自助配置	我	R
	R	-
修补未由 Linux 操作系统的本机软件包管理器管理的已安装应用程序、软件或应用程序依赖项 自助配置	R	我
	R	-
连续性管理		
指定备份时间表	R	我
按计划执行备份。	我	R
自助配置	R	C

活动	Customer	AWS Managed Services (AMS)
验证备份	R	我
请求备份恢复活动	R	我
执行备份恢复活动。	我	R
自助配置	R	C
恢复受影响的堆栈和 VPCs	我	R
自助配置	R	C
恢复受影响的自定义/第三方应用程序	R	C
报告		
准备并提交月度服务报告	我	R
AMS 开启 AWS Outposts	R	我
按需配置和检索 API 审计历史记录 (CloudTrail)。	我	R
	R	我
自助配置		
通过 AWS Managed Services 接口提供对事件历史记录的访问权限	我	R
通过 AWS Managed Services 界面提供对变更历史记录的访问权限。	我	R
	不适用	不适用
自助配置		
服务请求管理		
使用服务请求请求信息	R	我
回复服务请求	我	R

活动	Customer	AWS Managed Services (AMS)
托管防火墙		
请求部署 AMS 管理的防火墙	R	我
AMS 管理的防火墙架构的设计和优化	我	R
部署 AWS 基础设施和 AMS 管理的防火墙设备	我	R
提供防火墙许可（包括适用 AWS 服务的使用费，例如 EC2）	R	我
定义默认域名允许名单	我	R
请求添加、修改和删除自定义允许列表和安全策略	R	我
为 AMS 管理的防火墙配置警报	我	R
监控所有 AMS 管理的防火墙配置的警报	我	R
执行防火墙配置的备份	我	R
请求备份恢复活动	R	我
使用新版本的产品更新已配置的资源	我	R
记录 AMS 管理的防火墙日志	我	R
将日志从 AMS 管理的防火墙转发到 CloudWatch	我	R
在 AMS 管理的防火墙中请求配置更改	R	我
批准 AMS 管理的防火墙中的配置更改	我	R
在 AMS 管理的防火墙中执行配置更改	我	R

⁸ AMS EC2 仅 AMIs 适用于亚马逊

⁹ OSES 只有当客户与操作系统供应商签署延长支持协议时，AMS 才对生命周期终止负责

AMS 环境基本组件

Multi-Account Landing Zone

这是对核心账户中基础设施的组成部分和潜在成本的估计。这不包括其他费用，例如带宽、CloudWatch 详细监控、记录、警报、Route53、Amazon S3、Simple Notification Service、快照或亚马逊预留实例。EC2

您需要为 AMS 管理的 AWS landing zone 基础设施所需的组件付费。据估计，普通的 AMS 多账户 landing zone 环境的费用为每月 2,450 美元，普通应用程序账户的费用为 50 美元。

有关定价的信息，请参阅 [AWS 定价](#)。

基本环境组件

组件	东部时间 成本	说明
管理账户	60 美元	AWS Organizations 管理账户；创建成员账户并对其进行财务管理。它包含 AWS 着陆区 (ALZ) 框架、账户配置堆栈集和 AWS 组织服务控制策略 (SCPs)。 • Directory Service : 35 • CloudTrail: 7 美元 • CloudWatch: 6 美元 • 其他 : 12 美元
共享服务账户	2000 美元	包含访问管理 (即 Active Directory)、端点安全管理 (趋势科技) 和堡垒 (SSH/RDP) 所需的基础设施和资源；估计为每月 2400 美元。此估算值不包括趋势科技许可证的费用。 • EC2: 800 美元 (堡垒数量最少) • RDS : 300 美元 (每股收益) • VPC (终端节点) : 400 美元 • Directory Service : 300 • CloudWatch: 100 美元 • GuardDuty : 15 美元

组件	东部时间 成本	说明
		• Secrets Manager : 10 美元 • 数据传输 : 10 美元 • Config : 10 美元 • 其他 : 45 美元
社交账号	350 美元	在 AMS 账户、您的本地网络和互联网出口流量之间进行网络路由的中心枢纽。此外，还包含公共 DMZ 堡垒 (AMS 工程师访问您的 AMS 环境中主机的入口点)。价格可能会上涨，具体取决于通过 Transit Gateway 和 Direct Connect 的流量。 • EC2: 250 美元 (堡垒) • VPC : 80 美元 • 其他 : 20 美元
日志存档账户	20 美元	一个 S3 存储桶，其中包含来自您的每个 AMS 环境账户的 AWS CloudTrail 和 AWS Config 日志文件的副本。收集的日志越多，成本就会增加。 • S3 : 10 美元 • CloudWatch: 5 美元 • 其他 : 5 美元
安全账户	20 美元	安全相关操作的中心枢纽，也是向 AMS 控制飞机服务发送通知和警报的主要点。此外，还有 Amazon Guard 值班管理账户。随着使用 Amazon 分析更多事件，成本也会增加 GuardDuty。 • CloudWatch: 15 美元 • 其他 : 5 美元

Single-Account Landing Zone

下表列出了 AMS 管理的示例基础设施的组件。

基本环境组件，最后更新时间 2020/07/09

名称	实例类型	OS	组件数量	
mc-eps-dsm	m5.large	Linux	2	
mc-管理层	m5.large	Windows	2	
mc-bastion-dmz-ssh	m5.large	Linux	2	
mc-bastion-customer-rdp	m5.large	Windows	2	
mc-eps-relay	m5.large	Linux	2	
目录服务	不适用	不适用		
其他组件	不适用	不适用		

有关定价的信息，请参阅 [AWS 定价](#)。

AMS 账户限额

AMS 多账户着陆区内有三种不同类型的限制需要考虑：AMS API 限制、AMS 资源限制和 AWS 限制。

AMS 单账户着陆区内有两种不同类型的限制需要考虑：AMS API 限制和 AWS 限制。

AMS 账户 API 限制

本节介绍账户级别限制，超过该限制后 AWS Managed Services (AMS) 会限制 AMS SKMS API 服务。这意味着，如果您在一秒钟内拨打列出的电话 APIs 超过 10 次，则其中一个呼叫被“限制”（您会收到）。ThrottleException在极少数情况下，外部或下游依赖关系可能会限制 AMS API，然后 AMS 可能会以可能更低的速率限制您的 API 调用。

 Note

有关 AMS SKMS API 的信息，请通过 AWS Artifact 控制台的“报告”选项卡下载参考资料。

对于列出的每个 AMS SKMS API，该操作在 10 TPS（每秒交易量）后会受到限制：

- GetStack
- GetSubnet
- GetVpc
- ListAmis
- ListStackSummaries
- ListSubnetSummaries
- ListVpcSummaries

AMS 多账户 landing zone 账户资源限制

账户资源限制与 AMS 多账户 landing zone 应用程序账户 VPCs 和子网有关。

应用程序账户资源限制

每个组织有 50 个应用程序帐户的软限制。如果您有超过 50 个应用程序帐户的用例，请联系您的云服务交付经理 (CSDM)，转达您的需求。

VPCs 和子网资源限制

在为该组织预定义的 AWS 区域内，VPCs 每个应用程序账户的软限制为 10 个。

每个 VPC 可能有 1 到 10 个私有子网层，跨越 2 到 3 个可用区。此外，每个 VPC 可能有 0 到 5 个公有子网层，跨越 2 到 3 个可用区。如果您的要求超出这些限制，请通知您的 CSDM 或云架构师查看您的用例。

AMS 多账户 landing zone 申请与账户比例

AMS 多账户着陆区支持每个应用程序一个账户；但是，每个应用程序账户的费用很小，您需要为每小时与 Transit Gateway 的连接次数以及流经 AWS Transit Gateway 的流量收费。因此，账户中隔离的应用程序越多 VPCs，或者成本就越高。

为了降低成本并同时确保适当的职责分工，AMS 建议您 1) 按业务流程紧密耦合的团队对应用程序进行分组，以及 2) 不要混合处于不同阶段（生产与非生产）或由不同团队管理的应用程序。这样，您将拥有更少的帐户，访问管理和职责分工将更加容易，并且可以降低流量成本。

例如：一家企业在生产中有一个交易应用程序和一个投资组合管理应用程序，这两个应用程序都由投资 IT 团队管理，并且相互交换大量流量。在这种情况下，公司可以从将两个应用程序分组到同一个账户和同一个 VPC 中受益，因为投资 IT 团队不必请求访问多个应用程序账户，而且公司将节省流量成本。在这种情况下，公司应为处于开发阶段的相同应用程序创建另一个帐户，并向开发团队提供访问权限。

在另一种情况下，企业在生产中有一个薪资应用程序和一个会计应用程序，分别由人力资源 IT 和会计 IT 团队管理。尽管工资单应用程序必须与会计应用程序交换信息，但我们建议将两个应用程序分成不同的帐户，每个团队一个，并 VPCs 使用网络帐户在两个应用程序之间建立连接。通过这种方式，公司将防止人力资源IT团队请求更改影响会计应用程序基础架构，而他们对此一无所知。

有关如何将帐户分组为组织单位的提示 (OUs)。OU 是一种逻辑分组机制，使您能够对帐户进行分类 (分组)，并根据这些组对帐户应用策略和配置。建议的创建方法 OUs 是将它们建立在需要应用于特定账户组的策略的基础上，而不是基于报告结构中团队的内部层次结构。OU 不等同于 Active Directory 的 OU，因此不鼓励尝试在中复制 AD OU 结构，AWS Organizations 这会导致 and/or 操作结构难以维护。

AWS 账户限制

AWS 账户限制适用于您的 AWS Managed Services (AMS) 账户。确定 AWS 服务默认和当前限制的最简单方法是利用 S [AWS service Quotas](#)。AMS 建议将单个服务限制调整到适当的大小，以便在账户中运行服务。限额就像护栏一样，可以保护您的账户安全并降低逃跑成本。如果您想提高具体限额，请向 AMS 提交服务申请，AMS Operations 将代表您提高限额。例如，RDS 实例的默认限制 (或配额) 为 40；如果您的工作负载需要 50 个 RDS 实例，请向 AMS Operations 提出服务请求，将限制提高到所需的值。

AMS 服务级别目标 (SLOs)

下表描述了 AWS Managed Services (AMS) 服务的目标。AMS 服务其他方面 (包括事件管理SLAs) 的服务等级协议 () 包含在您订阅 AMS 时与您共享的 SLA 文档中。如需更多信息，请咨询您的 CSDM。

AMS 服务级别目标

功能	绩效指标 (PI)	再加上 (Business Days, M-F 8AM to 6PM local time)	高级 (Calendar Days, 24 x 7)
变更管理	自动安排或拒绝所花 费的时间 RFCs	<=30 分钟	<=30 分钟
	调度的启动时间 RFCs 与计划执行时间的比 较	<=1 分钟	<=1 分钟

功能	绩效指标 (PI)	再加上 (Business Days, M-F 8AM to 6PM local time)	高级 (Calendar Days, 24 x 7)
	approve/reject 非自动化所花费的时间 RFCs，可在 CT 目录中找到	<=48 小时	<=24 小时
	CT 目录中 RFCs 未提供 approve/reject 非自动化所花费的时间	<=5 天	<=5 天
问题管理	完成根本原因分析 (RCA) 所花费的时间	<=10 天	<=10 天
服务请求管理	第一次和后续每个回复的回复时间	<=8 小时	<=4 小时

支持的 AWS 服务

AWS Managed Services (AMS) 为以下服务提供运营管理支持 AWS 服务。每种 AWS 服务都是不同的，因此，AMS 的运营管理和支持水平因基础 AWS 服务的性质和特征而异。根据 AMS 提供的运营管理支持 AWS 服务的复杂性和范围对特定服务进行分组。

Note

在 2021 年 3 月 16 日之前，根据支持计划（Plus 或 Premium），A、B 和 C 这三个组表示了 AMS 客户的定价占每个账户每月总支出的百分比。2021 年 3 月 16 日之后加入的 AMS 客户应提交服务申请以获取更多定价信息。A 组表示不收取额外费用。B 组表示额外收费 12%（增值）或 18%（高级版）。C 组表示额外收费 25%（加价）或 42%（高级版）。

一颗星 (*) 表示客户使用 AWS 控制台和，在 AMS 托管环境中部署的服务 APIs。有关以这种方式调配和配置服务时客户责任 [AWS Managed Services \(AMS\) AMS 高级运营计划功能](#) 的更多详细信息，请参阅中的“自动和自助配置管理”。

两颗星 (**) 表示 Amaz EC2 on on AWS Outposts 将按照 B 组服务计费；托管的所有其他资源 AWS Outposts 将按其标准费率计费。

支持的 AWS 服务

A 组	B 组	C 组
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon CloudFront Amazon Elastic File System Amazon Glacier Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation* AWS Well Architected Tool* VM Import/ Export*	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon Bedrock* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect* Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon Elastic Container Service (ECS) on AWS Fargate* Amazon Elastic Kubernetes Service (EKS) on Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage* Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kendra* Amazon Kinesis Analytics* Amazon Kinesis Data Stream*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic, application, and network; not gateway) Amazon ElastiCache Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift Amazon Relational Database Service Amazon Route 53 Amazon Route 53 Resolver DNS Firewall Amazon Simple Email Service Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service

A 组	B 组	C 组
	Amazon Kinesis Firehose* Amazon Kinesis Video Streams* Amazon Lex* Amazon Managed Service for Prometheus* Amazon MQ* Amazon Personalize** Amazon Quantum Ledger Database (QLDB)* Amazon QuickSight* Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkSpaces* AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM* AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Resilience Hub* AWS Secrets Manager* AWS Security Hub* AWS Service Catalog	AWS Systems Manager (SSM)

A 组	B 组	C 组
	AWS Service Catalog AppRegistry* AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

如果您请求 AWS Managed Services 为下文未明确确定为支持的软件或服务提供服务，则根据服务条款，为此类客户请求的配置提供的任何 AWS 托管服务都将被视为“测试版服务”。

支持的配置

以下是 AWS Managed Services (AMS) 支持的配置：

- 语言：AMS 提供英语版本。
- 防火墙服务：
 - 亚马逊 Route 53 解析器 DNS 防火墙
 - Palo Alto VM 系列下一代防火墙
- 安全软件：趋势科技提供的趋势科技服务器深度安全防护系统（必需）。AWS Marketplace: [趋势科技深度安全防护系统](#)
- 批准的目录服务：微软 Active Directory (AD)
- [支持的 AWS 服务](#).
- 支持的 AWS 区域：

AMS 仅在“美国东部（弗吉尼亚北部）”AWS 地区运营；但是，AMS 仅 API/CLI 在“美国东部（弗吉尼亚北部）”地区运营。如果您在非美国东部地区运行 AMS 变更管理 API (amscm) 或 AMS 服务知识管理 API (amsskms))，则必须--region us-east-1向命令中添加内容。

- 美国东部（弗吉尼亚）
- 美国西部（加利福尼亚北部）
- 美国西部（俄勒冈州）
- 美国东部（俄亥俄州）

- 加拿大 (中部)
- 南美洲 (圣保罗)
- 欧洲 (爱尔兰)
- 欧洲 (法兰克福)
- 欧洲 (伦敦)
- 欧盟西部 (巴黎)
- 亚太地区 (孟买)
- 亚太地区 (首尔)
- 亚太地区 (新加坡)
- 亚太地区 (悉尼)
- 亚太地区 (东京)
- Amazon 机器映像 (AMIs) : AMS 根据 CIS 1 级基准为 AMS 支持的部分操作系统提供安全增强映像 (AMIs)。要查找具有安全增强镜像的操作系统, 请参阅 AMS 安全用户指南。要访问本指南, 请在中 AWS Artifact 筛选 AWS Managed Services 的“报告”选项卡。要进行访问 AWS Artifact, 请联系您的 CSDM 或参阅 [“AWS Artifact 入门”](#)。

- 支持的操作系统 :

支持的操作系统 (x86-64)

- Amazon Linux 2023
- 亚马逊 Linux 2 (预计 AMS 支持截止日期为 2026 年 6 月 30 日)
- 甲骨文 Linux 9.x、8.x
- 红帽企业 Linux (RHEL) 9.x、8.x
- SUSE Linux 企业服务器 15 SP6
- 适用于 SAP 15 SP3 及更高版本的 SUSE Linux 企业服务器
- 微软 Windows Server 2022、2019、2016
- Ubuntu 20.04、22.04、24.04

支持的操作系统 (ARM64)

- Amazon Linux 2023
- 亚马逊 Linux 2 (预计 AMS 支持截止日期为 2026 年 6 月 30 日)

- 支持的终止支持 (EOS) 操作系统 :

 Note

End of Support (EOS) 操作系统不在操作系统制造商的一般支持期内，因此安全风险增加。只有当 AMS 要求的代理支持操作系统并且... 时，EOS 操作系统才被视为支持的配置

1. 您已获得操作系统供应商的扩展支持，允许您接收更新，或者
2. 任何使用 EOS 操作系统的实例都要遵守 AMS 在高级用户指南中指定的[安全控制措施](#)，或者
3. 您遵守 AMS 要求的任何其他补偿性安全控制措施。

如果 AMS 无法再支持 EOS 操作系统，AMS 会发布升级操作系统的[关键建议](#)。

AMS 所需的代理可能包括但不限于：CloudWatch、AWS Systems Manager亚马逊、端点安全 (EPS) 代理和 Active Directory (AD) Bridge (仅限 Linux)。

- Ubuntu Linux 18.04
- SUSE Linux 企业服务器 15 SP3 SP4、和 SP5
- 适用于 SAP 的 SUSE Linux 企业服务器 15 SP2
- SUSE Linux 企业服务器 12 SP5
- 适用于 SAP 的 SUSE Linux 企业服务 12 SP5
- 微软 Windows Server 2012/2012 R2
- 红帽企业 Linux (RHEL): 7.x
- 甲骨文 Linux 7.5-7.9

适用于 AMS 中不支持的操作系统的功能

不支持的操作系统是指未在中列出的任何操作系统。[支持的配置](#)AMS 将操作系统不支持的实例视为“客户请求的配置”，受测试版[和预览版服务AWS 条款的](#)约束。

以下有限的 AMS 功能适用于操作系统不支持的实例：

功能	备注
事件管理	AMS 提供事件响应。
服务请求管理	AMS 会对服务请求做出回应。

功能	备注
变更申请 (RFCs)	AMS 会评估 RFCs 执行情况。不支持的操作系统可能会影响执行 RFCs能力。
监控	AMS 监控并响应 Amazon EC2 系统状态检查和实例状态检查。系统状态检查包括：网络连接中断、系统电源中断、物理主机上的软件问题以及影响网络可访问性的物理主机上的硬件问题。 实例状态检查包括：网络或启动配置不正确、内存耗尽、文件系统损坏以及内核不兼容。
安全管理	AMS 会监控并回应 Amazon 的 EC2 GuardDuty 调查结果 。
备份管理	AMS 在 AMS Advanced 中为 EC2 使用 AMS 定制的 AWS Backup 计划和保管库提供连续性管理 。

AMS 高级接口

- AMS Advanced 控制台：您可以使用 AMS Advanced 控制台创建 RFCs、报告和响应事件、提出服务请求以及查找有关现有堆栈 VPCs 和堆栈的信息。如果不确定该怎么做，或者需要有关 AMS 或托管资源的帮助，请使用此界面创建服务请求。
- AWS 管理控制台：许多 AWS 控制台都可用于查看 AMS 信息，例如：
 - 亚马逊 EC2 控制台：用于查看实例信息，包括堡垒 IP 地址、Amazon A EC2 uto Scaling 组和负载均衡器。
 - 多账户着陆区 AWS Config 规则合规性：您可以查看各个账户的合规状态并识别不合规的资源。
 - AWS CloudFormation 控制台：用于查看堆栈信息，包括堆栈 IDs（您可以 IDs 在此处找到 Amazon RDS 堆栈和 Amazon RDS 实例，以及事件信息）。
 - Amazon RDS 控制台：用于查看事件信息，例如在您账户的网站上向 WordPress 应用程序发布的帖子。请注意，您必须拥有 Amazon RDS 实例 ID。

根据您的登录角色模式，您对 AWS 管理控制台的访问权限会有所不同。有关模式的更多信息，请参阅 [AMS 模式](#)。

- AMS 高级变更管理 API — 读/写：使用变更管理 API (CM API) 请求对托管基础设施进行添加和特定更改，包括资源监控、日志、备份和补丁配置。此外，使用此 API 请求访问资源、删除资源 AMIs、创建和创建 IAM 实例配置文件。您可以通过 AMS CLI 访问 CM API 和 SDKs。
- AMS SKMS API — 只读：使用此 API 列出托管资源并获取报告或准备变更请求所需的信息。
- 支持 API：使用标准支持 API 以编程方式创建和响应事件和服务请求。要了解更多信息，请参阅[入门支持](#)。
- AWS APIs— 只读：您的主要 IT 管理员可以使用查看管理的所有资源、查看 CloudTrail 日志、账单信息以及许多其他读取功能。AWS APIs

AMS VPC 终端节点

VPC 终端节点允许您私密连接您的 VPC，AWS 服务 而无需互联网网关。VPC 中的实例无需公有 IP 地址便可与服务中的资源通信。

终端节点是虚拟设备。这些是水平扩展、冗余且具备高可用性的 VPC 组件，通过使用这些组件，可以在 VPC 中的实例与服务之间进行通信，而不会对网络通信带来可用性风险或带宽限制。要了解更多信息，请参阅[VPC 终端节点](#)。

VPC 终端节点有两种类型：接口终端节点和网关终端节点。

- 网关终端节点：账户中的 VPC 默认启用了 Amazon S3 网关终端节点。
- 接口终端节点：您的 AMS 环境中的实例无需离开 Amazon 网络即可与支持的服务通信。对于单账户 landing zone，这是可选的，默认情况下该账户未启用该功能；请向 AMS 运营部门提交服务请求以启用此功能。但是，对于多账户 landing zone，默认情况下，共享服务帐户中的接口端点处于启用状态。

AMS 支持的接口终端节点列表：

- AWS CloudFormation
- AWS CloudTrail
- AWS Config
- 亚马逊 EC2 API
- AWS Key Management Service
- Amazon CloudWatch
- 亚马逊 CloudWatch 活动
- Amazon CloudWatch 日志

- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

AMS 保护的命名空间

AWS Managed Services (AMS) 的受保护命名空间列表。在使用 AWS 资源时，请不要使用这些命名空间，以防止与 AMS 发生冲突。有关其他 AWS 服务命名空间的详细信息，请参阅 A [amazon 资源名称 \(ARNs\) 和 AWS 服务命名空间](#)。

- `ams-*` (这是新资源的首选命名标准)
- `/ams/*` (这是基于路径的资源的首选命名标准)
- `AWSManagedServices*` (在适当的情况下 CamelCase ，这是资源的首选命名标准)
- `ams*` 和 `AMS*` 和 `Ams*`
- `AWS_*` 和 `aws*`
- `*/aws_reserved/*`
- `CloudTrail*` 和 `Cloudtrail*`
- `codedeploy_service_role`
- `customer-mc-*`
- `eps` 和 `EPS`
- `EPSTMarketplaceSubscriptionRole`
- `EPSDB*`
- `IAMPolicy*`
- `INGEST*`
- `LandingZone*`
- `Managed_Services*`
- `managementhost`
- `mc*` 和 `MC*` 和 `Mc*`
- `MMS*`
- `ms-`

- NewAMS*
- Root*
- sentinel* 和 Sentinel*
- sentinel.int.
- StateMachine*
- StackSet-ams*
- StackSet-AWS-Landing-Zone
- TemplateId*
- UnhealthyInServiceBastion
- VPC_*

AMS 保留的前缀

AMS 资源属性必须符合某些模式；例如，IAM 实例配置文件 BackupVault 名称、名称、标签名称等，不得以 AMS 保留前缀开头。这些保留的前缀是：

```
*/aws_reserved/*
ams-*
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
```

```
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

AMS 维护窗口

AWS Managed Services 维护窗口 (或维护窗口) 为 AWS Managed Services (AMS) 执行维护活动，并在太平洋时间每个月的第二个星期四下午 3 点至下午 4 点重复。AMS 可能会在 48 小时通知后更改维护时段。这适用于 AWS Managed Services (AMS)；用于为托管基础设施执行维护活动，例如部署新的 AMS AMIs。

您的维护时段是 AMS 将应用补丁并由您在入职时确定维护时段的时间。您也可以同意修补服务通知中提供的拟议修补窗口，或者建议不同的窗口。

有关创建维护时段的指导，请参阅[维护时段](#)。

AMS 信息资源

AMS 提供了多种信息资源来帮助您取得成功。

- AMS Accelerate 用户指南：帮助您了解 AMS Accelerate 提供的组件和功能以及如何使用它们。在此处查看 AMS Accelerate 背景信息以及有关默认设置、查找资源和操作方法示例的详细信息。[HTML 索引](#)，[PDF](#)
- AMS 高级用户指南：帮助您了解 AMS Advanced 提供的组件和功能以及如何使用它们。请在此处查看 AMS Advanced 背景信息以及有关默认设置、查找资源和操作方法示例的详细信息。[HTML 索引](#)，[PDF](#)
- AMS 高级应用程序指南：描述将应用程序部署到 AWS Managed Services 基础设施的步骤。请在此处查看有关应用程序部署和维护方法及注意事项的信息。[HTML 索引](#)，[PDF](#)。

- **AMS 高级入门指南**：描述在 AMS 账户中创建基本 AWS Managed Services 多账户或单账户着陆区基础设施的初始步骤。在此处查看有关 AMS 账户基础知识、验证和问题的信息，让你为加入 AMS 做好准备。[HTML 索引](#)，[PDF](#)。
- **AMS 高级更改类型参考**：提供有关 AWS Managed Services 提供的当前变更类型的参考资料，包括变更类型架构以及每种变更类型的示例演练和提示。包括有关变更类型的一般信息帮助您了解变更请求 (RFCs) 和 AMS 变更类型 (CTs) 的各个方面。请在此处查看有关变更类型的详细信息，包括相关信息的链接。[HTML 索引](#)，[PDF](#)。
- **AMS CM (变更管理) API 参考**：介绍 AWS Managed Services CM API，它提供创建和监控变更请求的操作，并提供有关托管服务管理的资源的信息。[HTML 索引](#)。
- **AMS 安全指南**：描述 AMS 专有安全信息。

私有；在 AWS Artifact 控制台的“AMS 报告”选项卡上可用。

- **AMS 开发者资源**：访问 amscm 和 amsskms 的 AMS CLI 和 SDK。请参阅<https://console.aws.amazon.com/managedservices/>。
- **AMS YouTube 视频**：视频中解释了关键的客户操作。请参阅 [AWS Managed S YouTube erVICES 教学视频](#)。
- **AMS 博客文章**：有关 AWS Managed Services 的专业信息。请参阅 [AWS 博客](#)。

AMS 合规性

AMS 已经过以下标准的审计，并且有资格作为解决方案的一部分使用，您必须获得合规性认证。

AMS 支持的合规标准

AMS 支持 AWS 合规标准。要了解有关 AWS 合规计划的更多信息，请参阅[AWS 合规性](#)。

这些是 AMS 支持的当前合规标准。

Fed RAMP：美国联邦政府致力于以最具创新性、最安全和最具成本效益的方式向美国人民提供服务。云计算在联邦政府如何提高运营效率和按需创新以在全国范围内推进其使命方面发挥着关键作用。这就是为什么当今许多联邦机构都在使用 AWS 云服务来处理、存储和传输联邦政府数据的原因。

有关更多信息，请参阅 [FedRAMP](#)。

HIPAA : [AWS 扩大了其《健康保险流通与责任法案》\(HIPAA\) 合规计划，将 AMS 列为符合 HIPAA 资格的服务。](#) 如果您与 AWS 签订了商业伙伴协议 (BAA)，则可以使用 AMS 来帮助构建符合 HIPAA 标准的应用程序。

请参阅以 [HIPAA 为重点的白皮书](#)，了解如何利用 AMS 来处理和存储健康信息。有关更多信息，请参阅 [HIPAA 合规性](#)。

HITRUST : 健康信息信托联盟共同安全框架 (HITRUST CSF) 利用国内和国际公认的标准和法规，例如 GDPR、ISO、NIST、PCI 和 HIPAA，来创建一套全面的基准安全和隐私控制措施。

有关更多信息，请参阅 [HITRUST CSF](#)。

ISO 27001 : ISO/IEC 27001:2013 是一项安全管理标准，它根据 2700 ISO/IEC 2 最佳实践指南规定了安全管理最佳实践和全面的安全控制。该认证的基础是制定和实施严格的安全计划，其中包括开发和实施信息安全管理系统 (ISMS)，该系统定义了 AWS 如何以整体、全面的方式永久管理安全。

欲了解更多信息，请参阅 [ISO/IEC 27001:2013](#)。

ISO 27017: ISO/IEC 27017:2015 为云计算的信息安全方面提供了指导，建议实施针对云的信息安全控制措施，以补充 27002 和 27001 标准的指导。ISO/IEC 本行为准则提供了专门针对云服务提供商的其他信息安全控制实施指南。

有关更多信息，请参阅 [ISO/IEC 27017:2015](#) 合规性。

ISO 27018 : ISO/IEC 27018:2019 是一份侧重于保护云端个人数据的行为准则。它基于 ISO/IEC 信息安全标准 27002，提供了适用于公有云个人身份信息 (PII) 的 ISO/IEC 27002 控件的实施指南。它还提供了一组其他控制措施和相关指南，旨在满足现有 ISO/IEC 27002 控制集未满足的公共云 PII 保护要求。

有关更多信息，请参阅 [ISO/IEC 27018:2019](#) 合规性。

ISO 9001 : ISO 9001:2015 概述了一种以流程为导向的方法，用于记录和审查组织内实现有效质量管理所需的结构、职责和程序。该标准的特定部分包含有关主题的信息，例如：

- 质量管理体系的要求，包括质量手册的记录、文件控制和确定过程交互作用
- 管理层的责任
- 资源管理，包括人力资源和组织的工作环境
- 服务开发，包括从设计到交付的各个步骤
- 客户满意度
- 通过内部审计、纠正和预防措施等活动，衡量、分析和改进质量管理体系

有关更多信息，请参阅 [ISO 9001:2015](#) 合规性。

PCI : AMS 已获得支付卡行业 (PCI) 数据安全标准 (DSS) 3.2 版合规性认证，属于服务提供商级别 1。使用 AWS 产品和服务存储、处理或传输持卡人数据的客户可以使用 AMS 来管理自己的 PCI DSS 合规认证。

有关 PCI DSS 的更多信息，包括如何申请 AWS PCI Compliance Package 的副本，请参阅 [PCI](#) DSS 第 1 级。重要的是，您必须在 AMS 中配置精细的密码策略，使其与 PCI DSS 版本 3.2 标准保持一致。有关必须强制执行哪些策略的详细信息，请参阅[为您的 AWS Microsoft AD 目录启用 PCI 合规性](#)。

SOC : AMS 系统和组织控制 (SOC) 报告是独立的第三方检查报告，展示了 AMS 如何实现关键合规控制和目标。这些报告的目的是帮助您和您的审计师了解为支持运营和合规而建立的 AMS 控制措施。AMS SOC 报告有三种类型：

- AWS SOC 1 报告——使用 [AWS Artifact 下载](#)
- AWS SOC 2 : 安全、可用性和机密性报告—— [使用 AWS Artifact 下载](#)
- [AWS SOC 3 : 安全、可用性和保密性报告](#)

有关更多信息，请参阅 [SOC 合规性](#)。

责任共担

安全，包括 PCI 合规性，是一项[共同的责任](#)。重要的是要明白，AMS 合规性状态不会自动应用于您在 AWS 云端运行的应用程序。您需要确保您对 AWS 服务的使用符合标准。有关 AMS 如何在特定活动中与客户合作的更多详细信息，请参阅 AMS [AMS 责任矩阵 \(RACI\)](#)。

AMS Amazon 机器映像 (AMIs)

AMS 每月都会为支持 AMS 的操作系统生成更新的亚马逊系统映像 (AMIs)。此外，AMS 还基于 CIS 1 级基准测试为 [AMS 支持的部分操作系统](#) 生成安全增强映像 (AMIs)。要了解哪些操作系统具有安全增强型映像，请参阅 AMS 安全用户指南，该指南可通过 AWS Managed Services 筛选的 AWS Artifact > Reports 页面（在左侧导航窗格中找到“报告”选项）获得。要访问 AWS Artifact，可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。

要在新 AMS 发布时收到提醒，您可以订阅名为“AMS AMI”的亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 通知主题。有关详细信息，请参阅通过 [SNS 发送的 AMS AMI 通知](#)。

AMS AMI 的命名惯例是:customer-ams-<operating system>-<release date> -<version>. （例如，customer-ams-rhel6-2018.11-3）

仅使用 AMIs 以开头的 AMS customer。

AMS 建议始终使用最新的 AMI。您可以通过以下任一方式找到最新 AMIs 的：

- 在 AMS 控制台中查看，在 AMIs 页面上。
- 查看最新的 AMS AMI CSV 文件，该文件可从您的 CSDM 中获得，也可以通过此 ZIP 文件获得：[AMS 11.2024 AMI 内容和 ZIP 格式的 CSV 文件](#)。

有关过去的 AMI ZIP 文件，请参阅[文档历史记录](#)。

- 运行此 AMS SKMS 命令（需要 AMS SKMS 开发工具包）：

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId,CreationTime]" --output table
```

按操作系统 (OS) 向基础 AWS AMIs 版添加的 AMS AMI 内容

- Linux AMIs :
 - [AWS CLI 工具](#)
 - [NTP](#)
 - [趋势科技端点保护服务代理](#)
 - [代码部署](#)
 - [PBIS/Beyond Trust 广告桥](#)
 - [SSM Agent](#)
 - Yum 升级关键补丁
 - AMS 自定义脚本/管理软件（控制启动、AD 加入、监控、安全和日志记录）
- Windows 服务器 AMIs :
 - [微软.NET 框架 4.5](#)
 - [PowerShell 5.1](#)
 - [AWS 适用于 Windows 的工具 PowerShell](#)
 - AMS PowerShell 模块控制启动、AD 加入、监控、安全和日志记录
 - [趋势科技端点保护服务代理](#)
 - [SSM Agent](#)
 - [CloudWatch Agent](#)
 - EC2Config 服务（通过 Windows Server 2012 R2）
 - EC2发布（2016 年 Windows Server 和 2019 年 Windows 服务器）
 - EC2LaunchV2（Windows Server 2022 及更高版本）

基于 Linux AMIs :

- 亚马逊 Linux 2023 (最新次要版本) (不支持最低 AMI)
- 亚马逊 Linux 2 (最新次要版本)
- 亚马逊 Linux (2ARM64)
- 红帽企业 7 (最新次要版本)
- 红帽企业 8 (最新次要版本)
- 红帽企业 9 (最新次要版本)
- SUSE Linux 企业服务器 15 SP6
- Ubuntu Linux 18.04
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- 亚马逊 Linux : 有关产品概述、定价信息、使用信息和支持信息 , 请参阅[亚马逊 Linux AMI \(HVM/64 位 \)](#) 和[亚马逊 Linux 2](#)。

有关更多信息 , 请参阅[亚马逊 Linux 2 FAQs](#)。

- RedHat 企业 Linux (RHEL) : 有关产品概述、定价信息、使用信息和支持信息 , 请参阅[红帽企业 Linux \(RHEL\) 7 \(HVM\)](#)。
- Ubuntu Linux 18.04 : 有关产品概述、定价信息、使用信息和支持信息 , 请参阅 [Ubuntu](#) 18.04 LTS-Bionic。
- 适用于 SAP 应用程序的 SUSE Linux 企业服务器 15 SP6 :
 - 每个账户运行以下步骤一次 :
 1. 导航到 AWS Marketplace。
 2. 搜索 SUSE 15 SAP 产品。
 3. 选择继续订阅。
 4. 选择接受条款。
 - 每次需要启动适用于 SAP Applications 的新 SUSE Linux 企业服务器 15 SP6 实例时 , 请完成以下步骤 :
 1. 记下订阅的适用于 SAP Applications 的 SUSE Linux 企业服务器 15 AMI 的 AMI ID。
 2. 创建部署 | 高级堆栈组件 | 堆 EC2 栈 | 创建更改类型 ct-14027q0sjyt1h RFC。 *InstanceAmiId* 替换为您订阅的 AWS Marketplace AMI ID。

基于 Windows AMIs :

微软 Windows 服务器 (2016、2019 和 2022 年) , 基于最新的 Windows AMIs。

有关创建的示例 AMIs , 请参阅[创建 AMI](#)。

离职 AMS AMIs :

AMS 不会在离职期间取消与您的任何 AMIs 共享信息 , 以免对您的任何依赖项造成影响。如果您想 AMIs 从您的账户中移除 AMS , 则可以使用 `cancel-image-launch-permission` API 隐藏特定内容 AMIs。例如 , 您可以使用以下脚本来隐藏之前与您的账户共享 AMIs 的所有 AMS :

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
do
    aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

您必须安装 AWS CLI v2 , 脚本才能毫无错误地执行。有关 AWS CLI 的安装步骤 , 请参阅[安装或更新最新版本的 AWS CLI](#)。有关该 `cancel-image-launch-permission` 命令的详细信息 , 请参阅[cancel-image-launch-permission](#)。

安全性得到增强 AMIs

AMS 根据 CIS 1 级基准为 AMS 支持的部分操作系统提供安全增强镜像 (AMIs)。要了解哪些操作系统具有可用的安全增强映像 , 请参阅 AWS Managed Services (AMS) 客户安全指南。要访问本指南 , 请打开 AWS Artifact , 在左侧导航窗格中选择 “报告” , 然后筛选 AWS Managed Services。有关如何访问的说明 AWS Artifact , 请联系您的 CSDM 或参阅[入门 AWS Artifact](#)以了解更多信息。

AD FS 和 AMS 之间的集成是如何工作的

本地网络和 AMS 域之间的单向信任是访问堆栈和 VPCs 的默认方式。创建 VPC 和堆栈后 , 将通过预先配置的 Active Directory 安全组授予访问权限。此外 , AWS 管理控制台 可以使用 Active Directory 联合身份验证服务 (AD FS) 或任何支持 SAML 的联合软件来配置对管理控制台的单点登录 (SSO) 的 AWS 访问权限。

Note

AMS 可以联合到许多联邦服务 , 例如 Ping、Okta 等。您不仅限于 AD FS ; 我们在此举例说明了一种可供您使用的联合技术。

此处的信息来自这篇博客文章：[启用联合身份验证到 AWS 使用 Windows Active Directory、AD FS 和 SAML 2.0。](#)

1. 当用户（我们称他为 Bob）浏览 AD FS 示例网站 (<https://Fully.Qualified.Domain.Name.Here/adfs/ls/IdpInitiatedSignOn.aspx>) 在他的域名内。安装 AD FS 时，您的默认网站会有一个名为 adfs 的新虚拟目录，其中包括此页面。
2. 登录页面会根据 AD 对 Bob 进行身份验证。根据 Bob 使用的浏览器，系统可能会提示他输入 AD 用户名和密码。
3. Bob 的浏览器会收到来自 AD FS 的身份验证响应形式的 SAML 断言。
4. Bob 的浏览器将 SAML 断言发布到 SAML 的 AWS 登录端点 (/saml)。https://signin.aws.amazon.com 在幕后，登录使用 [AssumeRoleWithSAML](#) API 请求临时安全证书，然后为构造登录网址。AWS 管理控制台
5. Bob 的浏览器收到登录 URL 并被重定向到控制台。

从鲍勃的角度来看，这个过程是透明的。他从一个内部网站开始，最后到了 AWS 管理控制台，无需提供任何 AWS 凭证。

Note

有关向 AMS 控制台配置联合身份验证的更多信息，请参阅：

- 多账户登录区域：向 [AMS 控制台配置联合](#)
- 单账户登录区：向 [AMS 控制台配置联合](#)

此外，请参阅[附录：AD FS 声明规则和 SAML 设置](#)。有关使用 AWS Microsoft AD 在 AWS 云中支持受合规性要求约束的 Active Directory 感知应用程序的信息，请参阅管理 [Microsoft AD](#) 合规性。

AMS 托管活动目录

AMS 现在提供了一项名为“托管活动目录”（又名托管 AD）的新服务，它允许 AMS 管理您的活动目录 (AD) 基础设施运营，同时让您控制活动目录的管理。

AMS 对托管 AD 的支持与 AMS 对亚马逊关系数据库服务 (Amazon RDS) 的支持类似。在这两种情况下，AWS（包括 AMS）都支持创建和管理运行服务的基础架构，同时您可以执行访问控制和所有管理功能。该模型具有以下优点：

- 限制安全风险：AWS 而且 AMS 不需要您的域名的管理权限。
- 直接集成：您可以使用当前的授权模型并将其与 AD 集成，而无需与 AMS 接口。

备注：

- AMS 和您都无法访问您的托管 AD 域控制器，因此无法在域控制器上安装任何软件。这一点很重要，因为不允许要求在域控制器上安装软件的第三方解决方案。

访问权限的工作原理是这样的：

- AWS Directory Service 团队：有权访问域控制器。
- AMS：有权访问 Directory Service APIs 以对域名执行某些操作。这些操作包括拍摄 AD 快照、更改 AD 架构和其他操作。
- 您：可以访问域 (AD) 以创建用户、群组等。
- 我们建议您在迁移企业 AD 之前对托管 AD 进行概念验证，因为并非传统 AD 环境中的所有功能都可以在托管 AD 环境中使用。
- AMS 不会管理您的广告管理或提供有关您的广告管理的指导。例如，AMS 不会就组织单位结构、组策略结构、AD 用户命名约定等提供指导。

它的工作原理是这样的：

1. AMS AWS 账户 为您安装了一个新的，与您的 AMS 账户分开并添加到您的 AMS 账户之外，并通过 Directory Service 配置活动目录 (AD) 环境（另请参阅[什么是 AWS AWS Directory Service](#)？）。

以下是系统集成商需要从您那里收集的信息，以便让 AMS 加入托管 AD：

- 账户信息
 - 为您的 AMS 管理 AWS 账户 的广告创建的账户 ID：数字 AWS 账户
 - 要将托管广告加载到的区域：AWS 区域
- 托管活动目录信息：
 - 微软 AD 版：标准版/企业版。AWS Microsoft AD（标准版）包括 1 GB 的目录对象存储空间。此容量最多可支持 5,000 个用户或 30,000 个目录对象，包括用户、群组和计算机。AWS

Microsoft AD (企业版) 包含 17 GB 的目录对象存储空间，最多可支持 100,000 个用户或 500,000 个对象。

有关更多信息，请参阅 [AWS Directory Service FAQs](#)。

- 域名 FQDN：您的 AMS 托管 AD 域名的 FQDN。
- 域 NetBIOS 名称：您的 AMS 托管 AD 域的 NetBIOS 名称。
- 您希望与托管 AD 集成的 AMS 标准账户的账号（AMS 配置从 AMS 标准账户的 AD 到托管 AD 的单向信任）
- 是否需要修改活动目录架构？如果需要，需要进行哪些修改？
- 默认情况下，会配置两个域控制器。你还需要更多吗？如果是，你需要多少？出于什么原因？
- 托管活动目录的联网信息：
 - 域控制器的托管 AD VPC CIDR（托管 AD 域控制器的私有子网范围内的 CIDR）：
 - 域控制器的子网 CIDR 1：[您的 CIDR，必须是 AMS 托管 AD VPC CIDR 的一部分]
 - 域控制器的子网 CIDR 2：[您的 CIDR，必须是 AMS 托管 AD VPC CIDR 的一部分]

例如：

- 托管 AD VPC CIDR：192.168.0.0/16
- 域控制器的 CIDR 1：192.168.1.0/24
- 适用于域控制器的 CIDR 2：192.168.2.0/24

为避免 IP 地址冲突，请确保您指定的托管 AD VPC CIDR 与您在公司网络中使用的任何其他私有子网 CIDR 不冲突。

- VPN 技术（可选）：[Direc Connect/Direct t Connect 和 VPN]
 - 您的网关的 BGP 自治系统编号 (ASN)：[客户提供的 ASN]
 - 网关外部接口的互联网可路由的 IP 地址，该地址必须是静态的：[客户提供的 IP 地址]
 - 您的 VPN 连接是否需要静态路由：[是/否]
2. AMS 为您提供 AD 环境的管理员账户密码，并要求您重置密码，这样 AMS 工程师就无法再访问您的 AD 环境了。
 3. 要重置管理员帐户密码，请使用 Active Directory 用户和计算机 (ADUC) 连接到您的 Active Directory 环境。ADUC 和其他远程服务器管理工具 (RSAT) 应在您在非 AMS 基础架构上配置的管理主机上安装和运行。Microsoft 有保护此类管理主机的最佳实践。有关信息，请参阅[实现安全的管理主机](#)。您可以使用这些管理主机来管理 Active Directory 环境。

4. 在日常操作中，AMS 会管理 AWS 账户直到 AWS Directory Service 方面的事情；例如 VPC 配置、AD 备份、AD 信任的创建和删除等。您使用和管理您的 AD 环境；例如，用户创建、群组创建、群组策略创建等。

有关最新的 RACI 表，请参阅“查看[服务说明](#)”中的“角色和职责”部分。

AMS 应用程序部署

AMS 应用程序开发者指南提供了以下部署的详细描述和演练：

- AMS 工作负载采集 CT 允许您和 AMS 云迁移合作伙伴轻松地将现有工作负载迁移到 AMS 管理的 VPC 中。使用 AMS 工作负载摄取，您可以通过提交 RFC 创建 AMS AMI，其中包含来自迁移合作伙伴迁移的实例 | 创建 CT (ct-257p9zjk14ija) 的部署 | Ingestion | Stack。您必须让迁移伙伴将实例从本地迁移 AWS 到您的本地环境，以及要将该实例提取到的目标 AMS VPC 和子网。

有关详细信息，请参阅 Workload [Ingest](#) 上的 AMS 应用程序开发人员指南。

- CloudFormation 采集更改类型 (ct-36cn2avfrj9v) 功能允许您轻松使用现有模板 CloudFormation 在 AMS 管理的 VPC 中部署自定义堆栈。

有关详细信息，请参阅“[CloudFormation 模板收录](#)”上的 AMS 应用程序开发人员指南。

- 您可以将本地数据库导入新数据库，并将其导入 AMS 管理的 Amazon S3 存储桶或 Amazon RDS 实例。您可以使用部署 | 高级堆栈组件 | 数据库迁移服务 (DMS) 更改类型来执行此操作，包括创建复制实例 (ct-27aplkhqr0ol)、创建复制子网组 (ct-2q5azjd8p1ag5)、创建复制任务 (ct-1d2fml15b9eth)、创建源端点 (ct-0attesnjqy2cx)、创建源端点 (ct-0attesnjqy2cx) 或者创建源端点 (S3) (ct-2oxl37nphsrjz)，然后创建目标端点 (ct-3gf8dolbo8x9p) 或创建目标端点 (S3) (ct-05muqzievnxk5)。

有关详细信息，请参阅 [Database Migration Service](#) 上的 AMS 应用程序开发人员指南。

- 您可以将本地 MS SQL 数据库导入到 AMS 托管的 RDS SQL 实例上的新数据库中。您可以使用各种 AMS 变更类型、Amazon RDS API 以及 AWS 控制台来执行此操作。

有关详细信息，请参阅 AMS 应用程序指南中的[数据库 \(DB\) 导入到 MS SQL RDS](#)。

AWS Managed Services 中的服务管理

主题

- [AWS Managed Services 中的账户管理](#)
- [在 AWS Managed Services 中开始提供服务](#)
- [客户关系管理 \(CRM\)](#)
- [AWS Managed Services 中的成本优化](#)
- [AWS Managed Services 中的服务时间](#)
- [在 AWS Managed Services 中获取帮助](#)

AMS 服务如何为您服务。

AWS Managed Services 中的账户管理

本节介绍 AMS 账户管理。

您被指定为云服务交付经理 (CSDM)，负责在整个 AMS 中提供咨询帮助，并详细了解托管环境的用例和技术架构。CSDMs 与客户经理、技术客户经理、AWS Managed Services 云架构师 (SAs) 和 AWS 解决方案架构师 () 合作（如适用），以帮助启动新项目，并在整个软件开发和运营过程中提供最佳实践建议。CAsCSDM 是 AMS 的主要联系点。您的 CSDM 的主要职责是：

- 组织并主持与客户的月度服务审查会议。
- 提供有关安全性、环境软件更新和优化机会的详细信息。
- 支持您的要求，包括 AMS 的功能请求。
- 回应并解决账单和服务报告请求。
- 为财务和容量优化建议提供见解。

在 AWS Managed Services 中开始提供服务

服务开始：AWS Managed Services 账户的服务开始日期是第一个日历月的第一天，在此之后，AWS 会通知您该 AWS Managed Services 账户的入职要求中规定的活动已经完成；前提是，如果 AWS 在某个日历月的第 20 天之后发出此类通知，则服务开始日期为该通知之日后第二个日历月的第一天。

服务开始

- R 代表负责任的一方，负责完成任务。
- 我代表知情；一个通报进展情况的当事方，通常只有在任务或可交付成果完成后才会被告知。

服务开始

步骤 #	步骤标题	说明	Custome	AMS
1.	移交客户 AWS 账户	客户创建一个新的 AWS 账户并将其移交给 AWS Managed Services	R	我
2.	AWS Managed Services 账户-设计	完成 AWS Managed Services 账户的设计	我	R
3.	AWS Managed Services 账户-构建	AWS Managed Services 账户是按照步骤 2 中的设计创建的	我	R

客户关系管理 (CRM)

AWS Managed Services (AMS) 提供了客户关系管理 (CRM) 流程，以确保与您建立和维持明确的关系。这种关系的基础是AMS对您的业务需求的洞察。CRM 流程有助于准确、全面地理解：

- 您的业务需求以及如何满足这些需求
- 你的能力和限制
- AMS 和您的不同责任和义务

CRM 流程允许 AMS 使用一致的方法向您提供服务，并管理您与 AMS 的关系。CRM 流程包括：

- 确定您的主要利益相关者
- 组建治理团队
- 与您举行和记录服务审查会议
- 提供带有上报程序的正式服务投诉程序
- 实施和监控您的满意度和反馈流程

- 管理您的合同

CRM 流程

CRM 流程包括以下活动：

- 识别和了解您的业务流程和需求。您与 AMS 的协议确定了您的利益相关者。
- 定义要提供的服务以满足您的需求和要求。
- 在服务审查会议上与您会面，讨论 AMS 服务范围、SLA、合同和您的业务需求的任何变化。可能会与您举行临时会议，讨论绩效、成就、问题和行动计划。
- 使用我们的客户满意度调查和会议反馈来监控您的满意度。
- 在内部衡量的月度绩效报告中报告绩效。
- 与您一起审查服务，以确定改进的机会。这包括就所提供的 AMS 服务的水平和质量与您进行频繁沟通。

CRM 会议

AMS 云服务交付经理 (CSDMs) 定期与您开会，讨论服务轨道（运营、安全 and 产品创新）和高管方向（SLA 报告、满意度衡量标准和业务需求的变化）。

会议	用途	Mode	参与者
每周状态回顾 (可选)	未解决的问题或事件、补丁、安全事件、问题记录 12 周运营趋势 (+/-6) 应用程序操作员关注的问题 周末日程安排	现场客户 location/ Telecom/Chime	AMS：CSDM 和云架构师 (CA) 客户分配的团队成员（例如：云/基础架构、Application Support、架构团队等）
每月业务回顾	查看服务级别性能（报告、分析和趋势） 财务分析	现场客户 location/ Telecom/Chime	AMS：CSDM、云架构师 (CA)、AMS 客户

会议	用途	Mode	参与者
	产品路线图 CSAT		团队、AMS 技术 产品经理 (TPM) (可选)、AMS 运营经理 (可 选) 您：应用程序运 营商代表
季度业务回顾	记分卡和服务级别协议 (SLA) 绩效和 趋势 (6 个月) 即将到来的 12 年 3 月 6 日/9 月计划/ 迁移 风险和风险缓解 关键改进举措 产品路线图项目 未来方向一致的机会 金融 成本节约举措 业务优化	现场客户位置	AMS：CSDM、 云架构师、AMS 客户团队、AMS 服务总监、AMS 运营经理 您：应用程序运 营商代表、服务 代表、服务主管

CRM 会议安排

AMS CSDM 负责记录会议，包括：

- 创建议程，包括行动项目、议题和与会者名单。
- 创建每次会议上审查的措施项目列表，以确保项目按计划完成和解决。
- 在会议结束后的一个工作日内通过电子邮件向与会者分发会议纪要和行动项目列表。
- 将会议记录存储在相应的文档存储库中。

在CSDM缺席的情况下，主持会议的AMS代表编写和分发会议记录。

Note

您的 CSDM 会与您合作建立您的账户管理。

CRM 月度报告

您的 AMS CSDM 准备并发送每月服务绩效演示文稿。演讲包括以下方面的信息：

- 举报日期
- 摘要和见解：
 - Key Call Outs：堆栈总数和活跃堆栈数、堆栈补丁状态、账户入职状态（仅限入职期间）、客户特定问题摘要
 - 性能：事件解决、警报、修补、变更请求 (RFCs)、服务请求以及控制台和 API 可用性的统计信息
 - 问题、挑战、疑虑和风险：客户特定的问题状态
 - 即将推出的项目：客户特定的入职培训或事件解决计划
- 托管资源：堆栈的图表和饼图
- AMS 指标：监控和事件指标、事件指标、AMS SLA 遵守指标、服务请求指标、变更管理指标、存储指标、连续性指标、Trusted Advisor 指标和成本摘要（以多种方式呈现）。功能请求。联系信息。

Note

除了上述信息外，您的 CSDM 还会告知您范围或条款的任何重大变化，包括AMS使用分包商进行运营活动。

AMS 会生成有关修补和备份的报告，您的 CSDM 将这些报告包含在您的月度报告中。作为报告生成系统的一部分，AMS 会为您的账户添加一些您无法访问的基础设施：

- 一个 S3 存储桶，报告了原始数据
- 一个 Athena 实例，带有用于查询数据的查询定义
- 用于从 S3 存储桶读取原始数据的 Glue 爬行器

AWS Managed Services 中的成本优化

AWS Managed Services 每月都会在您的每月业务评估中向您提供详细的成本利用率和节省报告 (MBRs)。

AMS 遵循一套标准的流程和机制来确定您的托管账户中的成本节约途径，并帮助您规划和推出变更以优化 AWS 支出。

Note

AMS 正在开发一段有助于成本优化的视频。第一步是为您提供一份包含成本优化最佳实践的 PDF 和 Excel 电子表格。要访问这些资源，请打开[成本优化快速指南](#) ZIP 文件。

成本优化框架

AMS 采用三阶段方法来优化您的 AWS 成本：

1. 确定托管环境中的成本优化途径
2. 向您提交成本优化计划
3. 以可衡量的方式协助实现成本优化

确定托管环境中的成本优化途径

AMS 利用成本资源管理器和 Trusted Advisor 等 AWS 原生工具，同时利用架构优化、EC2 实例和以 AWS 客户为中心的优化中的 20 多种成本节省模式，为您制定量身定制的成本节约建议。

一些优化建议包括以下内容。

架构优化建议：

- S3 存储类的最佳使用：Amazon S3 提供了一系列存储类别，以满足基于数据访问权限、弹性和成本的各种工作负载要求。基于工作负载需求的 S3 智能分层和 S3 存储类分析使您能够高效地管理 S3 成本。
- 使用缓存架构：在适用的情况下，利用缓存实例可以帮助您替换某些数据库实例，同时满足 IOPS 要求。
- EBS 升级节省开支：将 EBS 卷从 gp2 迁移到 gp3 可节省高达 20% 的成本，无论卷大小如何，您都可以利用可预测的 3,000 IOPS 基准性能和 125 MiB/s。

- 使用弹性：AWS 提供的自动缩放功能允许有效的资源利用率和成本优化的途径。根据需要定期审查和更新实例扩展策略，可以进一步节省成本。

EC2 以实例为重点的建议

- 调整实例大小：建议侧重于根据使用情况调整实例大小和优化配置。建议还包括使用 Amazon A EC2 uto Scaling 功能，在适用的情况下将 EC2 实例替换为 Amazon S3 上的静态网页内容等。AWS Lambda
- 实例调度：使用 AMS 资源调度器根据时间表自动启动和停止实例有助于控制成本，特别是对于非工作时间未使用的非生产实例。
- 订阅储蓄计划：储蓄计划是节省 AWS 使用量的最简单方法。与按需定价相比，Instance Savings Plans 可为您的亚马逊 EC2 实例使用量节省高达 72% 的费用。EC2 Amazon SageMaker AI Savings Plans 可为您的亚马逊 A SageMaker I 服务使用量节省高达 64% 的费用。AMS 会根据您的 AWS 资源使用情况提供相应的储蓄计划建议。
- 预留实例 (RI) 使用和消费指南：与按需定价相比，Amazon EC2 Reserved Instances (RI) 可提供大幅折扣（高达 75%），并且在特定可用区域中使用时会提供容量预留。
- 竞价型实例使用率：容错工作负载可以利用竞价型实例并将价格降低多达 90%。
- 空闲实例终止：识别并报告处于空闲状态或利用率低且可以终止的实例。

以账户为中心的推荐

- 账户清理：在账户层面，AMS 还会识别未使用的 EBS 卷、重复的 CloudTrail 跟踪、带有未使用资源的空账户等，并提供清理建议。
- SLA 建议：此外，AMS 会定期审查您的高级版和高级版账户，并建议为这些账户选择正确的 SLA 级别。
- AMS 自动化优化：AMS 不断优化用于提供 AMS 服务的 AMS 自动化和基础设施。

向客户演示并协助规划

AMS 每月与主要的客户利益相关者进行业务审查 (MBRs)，并介绍已确定的成本节约途径、机制和建议以及潜在的成本节约。我们将进一步与您合作，计划所需的更改。

协助实施建议并衡量成本影响

AMS 有助于实现和衡量成本影响和优化变更。

您可以评估所建议更改的应用程序影响、风险和成功标准，并通过 AMS 控制台提出相应的更改请求 (RFCs)。AMS 与您合作，在您的托管账户中实施与成本优化相关的变更。AMS 衡量成本影响，并在月度业务评估中包括实现的节省 (MBRs)。

成本优化责任矩阵

AMS 成本优化方面的职责。

成本优化 RACI

活动	Customer	AMS
编制节省成本的建议并准备报告	我	R
提交成本节约报告	C	R
与成本节约相关的计划变更	R	C
评估变更的影响和风险	R	C
RFCs 为实施变更筹款	R	C
审查 RFCs 并实施变更	C	R
测试应用程序并验证变更实施	R	C

活动	Customer	AMS
衡量变更后的成本影响并提交给客户	我	R

AWS Managed Services 中的服务时间

功能	AMS 高级版
	高级等级
服务请求	全天候
事件管理 (P2-P3)	全天候
备份和恢复	全天候
补丁管理	全天候
监控和提醒	全天候
自动申请变更 (RFC)	全天候
非自动变更请求 (RFC)	全天候
云服务交付管理器 (CSDM)	周一至周五：08:00 — 17:00，当地工作时间

在 AWS Managed Services 中获取帮助

AMS 全年 365 天、每周 7 天、每天 24 小时为您提供事件管理、服务请求管理和变更管理方面的支持（根据适用于该账户的 AMS 服务等级协议）。

要报告影响您的托管环境的 AWS 或 AMS 服务性能问题，请使用 AMS 控制台并提交事件报告。有关详细信息，请参阅[报告事件](#)。有关 AMS 事件管理的一般信息，请参阅[事件响应](#)。

要向 AMS 询问信息或建议，或请求其他服务，请使用 AMS 控制台并提交服务请求。有关详细信息，请参阅[创建服务请求](#)。有关 AMS 服务请求的一般信息，请参阅[服务请求管理](#)。

AWS Managed Services 中的计划活动管理

AWS Managed Services (AMS) 计划活动管理 (PEM) 是一项 AMS 服务。PEM 使用 AMS 服务在客户活动和项目期间参与、协调和协助。PEM 协助协调一组 RFCs 与 PEM 活动或项目的商定范围和时间表一致的相关活动。

AMS PEM 标准

计划中的活动是一个有范围限制和有时限的项目。AMS 使用您提供的详细信息（包括计划和范围、预期结果以及 AMS 运营部门预计要执行的变更）来在 PEM 活动期间为您提供有效支持。然后，您的云架构师 (CAs) 审查和评估 PEM 活动的完整性、技术实施和 AMS 运营参与度。CA 审查后，AMS 运营部门会审查计划，并与您的云服务交付经理 (CSDM) 协调运营团队的参与。

PEM 的类型

以下是可用的 PEM 类型：

- 比赛日
 - O@@ perational Gameday：一种基于场景的游戏操作响应方法，旨在验证流程、人员和系统的集成。
 - Sec@@ urity Gameday：一种安全事件响应策略，它采用基于场景的游戏方法来评估系统、流程和人员的集成。
- BYOEPS：使用 AMS “自带终端安全” (BYOEPS) 功能，将默认的 AWS 趋势科技趋势科技服务器深度安全防护系统代理替换为您首选的端点安全解决方案或自定义的趋势科技许可证。有关更多信息，请参阅 [AMS 自备 EPS](#)。
- 灾难恢复：灾难恢复事件涉及 AMS 在您计划的灾难恢复活动中为您提供协助。有关更多信息，请参阅 [灾难恢复计划](#)。
- 客户安全事件：计划中的安全事件。例如，root 用户活动和渗透测试。
- 迁移支持：为计划的入职和迁移活动提供支持。

此工作流程促进了与 AMS 的合作，以协调与 AMS 支持相关的计划活动和迁移活动。要优先执行 RFCs，最佳做法是使用按需运营 (OOD) 项目。有关更多信息，请参阅 [按需运营](#)。

AMS PEM 流程

PEM 流程包括以下阶段：

- **PEM 启动**：您与 CSDM 合作，为计划中的活动定义目标，并确定 AMS 运营部门需要什么。AMS CAs 审查 PEM 计划的技术方面。他们 CAs 与 AMS Security and Operations 合作进行合规、执行优化和自动化，并定义 PEM 前的执行任务和可交付成果。然后，您的 CSDM 会创建 PEM 工单，并向 AMS 提供项目信息和技术细节。AMS 需要 14 个日历日的准备时间，让 AMS 运营团队有时间进行规划、提供技术审查和分配资源。
- **PEM 审查**：AMS 运营团队审查 PEM 申请，并与您的 CSDM 合作，验证 PEM 计划中的信息是否正确和完整。
- **PEM 接受**：AMS 会审查所提供的信息，并向 CSDM 通报 PEM 活动期间的支持级别。如果 PEM 包含完整的信息，并且您的 CSDM 同意工作范围，则 PEM 就会获得批准。
- **准备和执行**：AMS 确保在 PEM 开始之前完成所需的任务，并促进内部和客户沟通。AMS 确保 PEM 计划正确运行，并提供状态和进度报告。

PEM FAQs

在 PEM 活动期间，如何让 AMS 参与 RFC/Service 请求 (SR)？

- 在格式的 RFC/SR 主题行中使用您的 CSDM 共享的 PEM ID。 *PEM-ID*
- 您也可以创建服务请求 (SR) 来讨论您的用例或询问有关您计划中的活动的问题。如果你使用 SR，那么 PEM 不一定是有效的。

提交与 PEM 相关的 RFC 时会进行哪些验证？

- 验证账户 ID 是否已在 PEM 上列出。
- 验证 PEM 状态是否在提供的开始日期和结束日期之间获得批准且处于活动状态。

是否有 SLAs 或 SLOs 适用于 PEM 请求？

- PEMs 与 SLAs 或无关 SLOs。
- SLAs SLOs 对于与 PEM 相关的工作项目（RFC/服务请求），则由 AMS 定义。SLOs

有关更多信息，请参阅 [AMS 服务级别目标 \(SLOs\)](#)。

我们可以通过服务请求 (SR) 创建 PEM 吗？

- 不，PEM 的创建必须由云服务交付管理器 (CSDM) 管理。

网络架构

AWS Managed Services (AMS) 提供两种网络架构：

- Multi-account landing zone (MALZ)：通过共享账户为部署在不同成员账户中的工作负载提供常见服务，例如访问、端点安全、联网。
- 单账户 landing zone (SALZ)：提供独立账户，其中接入、端点安全、网络等常见服务与工作负载部署在同一个账户中。建议将其用于需要高度隔离的工作负载，因为它会产生更高的 AWS 成本。

MALZ 网络架构

关于多账号 landing zone 网络架构

在开始登录 AWS Managed Services (AMS) 多账户着陆区 (MALZ) 之前，请务必了解 AMS 代表您创建的基准架构或着陆区、其组件和功能。

AMS multi-account landing zone 是一种多账户架构，预先配置了基础设施，以促进身份验证、安全、联网和日志记录。

Note

有关成本估算，请参阅 [AMS 多账户 landing zone 环境基本组件](#)。

主题

- [服务区域](#)
- [组织部门](#)
- [服务控制策略和 AWS 组织](#)

下图概述了账户结构以及如何将基础设施划分到每个账户中：

服务区域

由于 Active Directory 和 Transit Gateway 当前的跨区域限制，AMS 多账户着陆区内的所有资源都部署在您选择的单个 AWS 区域内。

组织部门

典型的 AMS 多账户登陆区由四个顶级组织单位 (OUs) 组成：

- 核心组织单位 (OU) (用于将账户组合在一起，作为一个单元进行管理)
- 应用程序 OU
- 客户管理的 OU
- 加速 OU

AMS 管理的多账户 landing zone 还允许您创建 OUs 用于分组和组织 AWS 账户的自定义账户，并将自定义账户 SCPs 与之关联；有关执行此操作的示例，请分别参阅[管理账户 | 创建自定义账户 OUs](#)和[管理账户 | 创建自定义 SCP \(需要审核 \)](#)。AMS 提供了四个现有账户，可以在这些账户 OUs 下申请新的 OUs 和账户：加速、应用程序 > 托管、应用程序 > 开发和客户管理。

- 加速 OU：

这是 AMS 多账户着陆区 (MALZ) 中的顶级组织单位。此 OU 下的账户由 AMS 提供 RFC (部署 | 托管着陆区 | 管理账户 | 创建加速账户，更改类型 ID：ct-2p93tyd5angmi)。在这些加速应用程序帐户中，您可以受益于加速运营服务，例如监控和警报、事件管理、安全管理和备份管理。有关更多详细信息，请参阅[AMS 加速账户](#)。

- 应用程序 > 托管 OU：

在应用程序 OU 的这个子组织单元中，账户完全由 AMS 管理，包括所有操作任务。运营任务包括服务请求管理、事件管理、安全管理、连续性管理、补丁管理、成本优化、监控和事件管理。这些任务是为了管理您的基础架构而执行的。在达到 AWS 组织的最大嵌套 OUs 限制之前，OUs 可以根据需要创建多个子项目。有关详细信息，请参阅[AWS Organizations 的配额](#)。

- 应用程序 > 开发 OU:

在 AMS 管理的 landing zone 中应用程序 OU 的子组织单位下，账户是[开发者模式](#)账户，可为您提供在 AMS 变更管理流程之外配置和更新 AWS 资源的高级权限。此 OU 还支持根据需要创建新的子项 OU。

- 客户管理的 OU：

这是 AMS 多账号 landing zone 中的顶级 OU。此 OU 下的账户由 AMS 提供 RFC。在这些账户中，工作负载和 AWS 资源的操作由您负责。此 OU 还支持根据需要创建新的子项 OU。

作为最佳实践，我们建议根据其功能 OUs 和政策对这些账户和自定义请求的子账号 OUs 进行分组。

服务控制策略和 AWS 组织

AWS 为 AWS 组织中的权限管理提供服务控制策略 (SCPs)。SCPs 用于为用户在哪些操作中可以执行的操作定义额外的护栏。OUs默认情况下，AMS 提供一组 SCPs 部署在管理账户中的账户，这些账户在不同的默认 OU 级别提供保护。如需了解 SCP 限制，请联系您的 CSDM。

您也可以创建自定义 SCPs 并将它们附加到特定的 OUs。可以使用变更类型 `ct-33ste5yc7hprs` 向您的管理账户申请它们。然后，AMS 会审核所 SCPs 请求的自定义，然后再将其应用于目标 OUs。有关示例，请参阅[管理账户 | 创建自定义账户 OUs](#)和[管理账户 | 创建自定义 SCP \(需要审阅\)](#)。

选择单个 MALZ 或多个 MALZs

下表提供了在单个多账户着陆区 (MALZ) 与多个多账户着陆区 (例如，两个多账户着陆区-Prod 和 non-Prod) 之间做出决定时的一些高级注意事项。通常，选择取决于个人需求、法律要求和运营实践。

单个多账户着陆区与多个多账户着陆区

实体	单个 AMS 着陆区	多个 (两个或更多) 着陆区
基础成本	较低，经过优化，每月约为3,000美元。	更高，每个环境的额外成本约为 3,000 美元。
计费	单一账单，由于单一账单/管理账户。	每个多账号 landing zone 均需单独计费。目前，AWS Org 不支持使用单一账单的多管理账户。
现有预留实例的可移植性 () RIs	低。AWS RIs 目前无法在多个账单账户之间进行转换。你可以将现有资源重新 RIs 用于多账户 landing zone。	更低。您将重新调整用途并在 RIs 所有多账号 landing zone 上进行分发。
产品分层折扣	高。参见 批量折扣 。	低。参见 批量折扣 。
初始设置开销 (按 project/migration 时间表计算)	低。Active Directory、联网和单点登录 (SSO) 集成仅限一次。	高。您将为每个着陆区执行 Active Directory、网络集成和 SSO 集成。这可能会导致任何迁移项目出现延迟。
常用服务可配置性	不费吹灰之力。您可以配置 DNS、备份、监控、日志记录等 common/shared 服务。	付出高昂的努力。需要进行额外的规划，以解决公共基础设施或服务的发展方向。在每个着陆区 (landing

实体	单个 AMS 着陆区	多个 (两个或更多) 着陆区
		zoneTGWs) 中穿越多个公交网关 () 的流量可能会导致额外费用。
可扩展性	中等。AMS 目前的实际限制为每个多账号着陆区 150 个账户。在同一个账户中运行应用程序的多个团队或供应商可以访问不同团队拥有的堆栈。可以通过控制 ServiceNow 层对特定应用程序堆栈的访问来缓解这种限制 (通过集成 AMS Conn ServiceNow ector 应用程序并使用标签)。询问 AMS 技术交付经理 (TDMs) 或云架构师 (CAs) 如何实现这一点。	高。能够利用多个多账户 landing zone 来分配账户，同时实现账户或应用程序的隔离级别。管理大量账户可能会导致运营或成本开销。
运营风险	(视情况而定) 低。操作整合和准备就绪仅一次。流程漂移的可能性更小。	(视情况而定) 低。多种整合和运营活动。在此期间，在多个着陆区漂移可能会导致操作风险。
多 AWS 区域	单个 AWS 区域。AMS 多账户 landing zone 仅限于单个 AWS 区域。要跨越多个 AWS 区域，请使用多个多账户 landing zone。	多 AWS 区域。借助多个多账户着陆区，您可以将每个 MALZ 部署在一个区域中，并使用公交网关 (TGW) 对等互连将它们互连。
账户迁移或可移植性	是。在同一 AWS 组织内将账户从一个 OU 转移到另一个 OU 是可能的。	不是。AMS 不支持跨着陆区 (即 AWS Organizations) 迁移账户。工作负载可以通过传输网关 (TGW) 或 VPC 对等互连跨着陆区域传输。
变更管理	中等。对 TGW、Active Directory (AD) 或出站 (出口) 等常见组件进行破坏性更改可能会影响多账户着陆区中的所有工作负载。但是，对 AMS 管理的组件所做的更改需要在内部进行测试，并以滚动更新形式推送。	低。对 TGW、AD 或出站 (出口) 等常见组件进行破坏性更改只能影响该特定多账户 landing zone 中的工作负载。

实体	单个 AMS 着陆区	多个（两个或更多）着陆区
数据和访问控制	（视情况而定）如果您想连接不同的本地 ADs 和网络来处理生产和非生产工作负载，则控制不足。SAML 联合、TGW 域和安全组 (SGs) 也可以帮助实现所需的控制。	（视情况而定）如果您想连接不同的本地 ADs 和网络以处理生产和非生产工作负载，则可以进行高度控制。使用单独的着陆区以满足严格的合规要求。
合规与安全	（视情况而定）如果有严格的合规要求将材料和非物质工作负荷完全分开，则为低。AMS 标准的预防和侦查控制措施已到位。	（视情况而定）High as multi-account landing zone可以通过将材料和非物质工作量完全隔离来帮助实现严格的合规要求。AMS 标准的预防和侦查控制措施已到位。

建议：如果没有严格的合规或多区域需求，从单个 AMS 多账户 landing zone 开始，就可以在成本、安全、卓越运营和迁移复杂性之间取得良好的平衡。如果遇到任何账户或业务限制，你可以随时设置额外的 landing zone。

单个多账户着陆区与多个多账户着陆区 FAQs

选择设置单个多账户着陆区或多个多账户着陆区时的一些常见问题：

问题 1：如果遇到任何账户限制或业务限制，我能否从单个多账户着陆区开始，然后转移到多个多账户着陆区？

答：是的。您可以选择在任何给定时间设置另一个多账号着陆区：

- 需要设置新的账单付款人账户（目前 AWS 不支持单个 AWS 组织中的多付款人账户）。
- 填写多账户 landing zone 问卷后，多账户 Landing Zone 基础建设最多需要 2 周的交货时间。
- 每个多账户 landing zone 意味着每月增加约 3K 美元的运营成本。
- 新的 MALZ 需要集成 N/W、AD、DNS 和 SSO。
- 需要为新的多账户 landing zone 设置任何预留实例 (RIs)、成本节省计划（RIs 不可转让）。
- AMS 多账户着陆区不支持跨多账户着陆区账户迁移账户；例如，跨AWS Orgs。但是，使用标准迁移方法可以将应用程序从一个帐户转移到另一个帐户。

问题 2：AMS 对 MALZ updates/changes 的 underlying/shared 基础设施和量化客户风险的方法是什么？请详细说明流程中包含哪些保证。客户如何放心 MALZ updates/changes 不会影响客户？客户需要采取任何措施来防止中断吗？

答：AMS 采用严格的变更方法，使用内部工具，使我们能够定义、审查、安排和执行对客户环境的更改。

发布更新的过程强制执行代码审查、集成测试、在 gamma 和 beta 环境中部署，以及在 beta 和 gamma 环境中进行额外的烘焙时间和测试，然后再发布给客户环境。所有版本都包含回滚程序，并受到发布团队以及创建和请求变更的团队的密切监控。版本的范围仅限于 AMS 拥有和提供的堆栈。平均而言，我们每周至少执行一个版本。

此外：

- AMS 服务等级协议适用。根据AMS服务描述，在共享基础设施维护活动后提出的任何事件都将遵守相应的服务等级协议，以获得解决方案或积分。
- 客户无需采取特殊的预防措施来防止公共基础设施中断。客户对 AWS Org 或核心 OU 账户拥有只读权限，因此客户无法对 MALZ 核心环境进行任何破坏性更改。客户对核心基础设施的所有请求都需要 AMS 的审查和批准。
- SCPs/Roles 在应用程序 OU 级别传播更改之前，客户可以测试某些组织级别的更改，例如在个人非生产账户级别进行更改。AMS路线图上允许使用多个应用程序 OUs（2020年第二季度），这将进一步降低进行某些ORG级别更改的风险。MALZ 团队已经为“构建模式”账户发布了单独的 OU，以确保明确区分客户所有权和单独的控制措施。
- 其中大多数变更使AMS能够以有效和高效的方式操作工作负载，并且不一定会影响客户的工作量。如果 AMS 认为共享基础设施变更会对客户的工作负载产生影响，那么他们就会与客户的变更窗口保持一致。

高级建议，如果出现以下情况，则从多个多账户着陆区域开始：

- 它是否可以帮助您实现任何特定的合规性。
- 如果您需要使用多区域。
- 如果您的本地 ADs 和网络 Prod/Material 与非工作负载不同Prod/Non-Material workloads, to clearly segregate b/w。

多账号着陆区账号

主题

- [管理账户](#)
- [社交账号](#)
- [共享服务账户](#)
- [日志存档账户](#)
- [安全账户](#)
- [应用程序账户类型](#)
- [AMS 工具账户 \(迁移工作负载 \)](#)

管理账户

管理账户是您开始使用 AMS 时的初始 AWS 账户。它使用 AWS Organizations 作为管理账户 (也称为支付所有成员账户费用的付款人账户)，这使该账户能够创建成员账户并对其进行财务管理。它包含 AWS landing zone (ALZ) 框架、账户配置堆栈集、AWS 组织服务控制策略 (SCPs) 等。

有关使用管理账户的更多信息，请参阅[管理账户的最佳实践](#)。

下图简要概述了管理账户中包含的资源。

管理账户中的资源

除上述标准服务外，在入职期间不会在管理账户中创建额外的 AWS 资源。在加入 AMS 期间，需要输入以下内容：

- 管理账户 ID：最初由您创建的 AWS 账户 ID。
- 核心账户电子邮件：提供要与每个核心账户关联的电子邮件：网络、共享服务、日志和安全账户。
- 服务区域：提供您的 AMS landing zone 的所有资源都将部署到的 AWS 区域。

社交账号

Networking 账户充当 AMS 多账户 landing zone 账户、本地网络和传出 Internet 的出口流量之间进行网络路由的中心枢纽。此外，该账户还包含公共 DMZ 堡垒，这些堡垒是 AMS 工程师访问 AMS 环境中主机的入口点。有关详细信息，请参阅以下网络帐户的高级示意图。

网络账户架构

下图描绘了 AMS 多账户 landing zone 环境，显示了账户间的网络流量，并且是高可用性设置的示例。

AMS 根据我们的标准模板和您在入职期间提供的选择选项为您配置网络的各个方面。标准的 AWS 网络设计适用于您的 AWS 账户，然后为您创建一个 VPC，并通过 VPN 或 Direct Connect 连接到 AMS。有关 Direct Connect 的更多信息，请参阅 [AWS Direct Connect](#)。标准 VPCs 包括 DMZ、共享服务和应用程序子网。在入职过程中，VPCs 可能会要求并创建其他内容以满足您的需求（例如，客户部门、合作伙伴）。入门后，您将获得一张网络图：一份环境文档，说明您的网络是如何设置的。

Note

有关所有活动服务的默认服务限制和限制的信息，请参阅 [AWS 服务限制](#) 文档。

我们的网络设计围绕 Amazon 的“[最低权限原则](#)”构建。为了实现这一目标，除了来自可信网络的流量外，我们会通过 DMZ 路由所有流量（入口和出口）。唯一可信的网络是通过使用 VPN 和 AWS Direct Connect (DX) 在您的本地环境和 VP and/or C 之间配置的网络。通过使用堡垒实例授予访问权限，从而防止直接访问任何生产资源。您的所有应用程序和资源都位于可通过公共负载均衡器访问的私有子网中。公共出口流量通过出口 VPC（在网络账户中）中的 NAT 网关流向 Internet Gateway，然后流向互联网。或者，流量可以通过您的 VPN 或 Direct Connect 流向您的本地环境。

与 AMS 多账户 landing zone 环境的专用网络连接

AWS 通过虚拟专用网络 (VPN) 连接或使用 AWS Direct Connect 的专用线路提供私有连接。在您的多账户环境中，私有连接是使用下述方法之一设置的：

- 使用 Transit Gateway 实现集中边缘
- 将 Direct Connect (DX) and/or VPN 连接到账户虚拟私有云 (VPCs)

使用公交网关实现集中边缘连接

AWS Transit Gateway 是一项服务，可让您 VPCs 和您的本地网络连接到单个网关。Transit Gateway (TGW) 可用于整合您现有的边缘连接并通过单个 ingress/egress 点进行路由。Transit 网关是在您的 AMS 多账户环境的网络账户中创建的。有关公交网关的更多详细信息，请参阅 [AWS Transit Gateway](#)。

AWS Direct Connect (DX) 网关用于通过中转虚拟接口将您的 DX 连接连接到 VPCs 或 VPNs 连接到您的传输网关。将 Direct Connect 网关与中转网关关联。然后，为您与 Direct Connect 网关的 AWS

Direct Connect 连接创建一个传输虚拟接口。有关 DX 虚拟接口的信息，请参阅 [AWS Direct Connect 虚拟接口](#)。

此配置提供以下好处。您可以：

- 管理同一 AWS 区域中的多个 VPCs 或 VPNs 多个连接的单个连接。
- 将前缀从本地发布到 AWS，从 AWS 发布到本地。

Note

有关在 AWS 服务中使用 DX 的信息，请参阅弹性工具包部分 [Classic](#)。有关更多信息，请参阅 [Transit Gateway 关联](#)。

为了提高连接的弹性，我们建议您将来自不同的 AWS Direct Connect 位置的至少两个传输虚拟接口连接到 Direct Connect 网关。有关更多信息，请参阅 [AWS Direct Connect 弹性建议](#)。

将 DX 或 VPN 连接到账户 VPCs

使用此选项，您的 VPCs AMS 多账户着陆区环境将直接连接到 Direct Connect 或 VPN。流量直接从流向 Direct Connect 或 VPN，无需通过传输网关。VPCs

社交账户中的资源

如网络账户图所示，以下组件是在该账户中创建的，需要您输入。

网络账户包含两个 VPCs：出口 VPC 和隔离区 VPC（也称为外围 VPC）。

AWS 网络管理器

AWS Network Manager 是一项服务，可让您可视化您的传输网关 (TGW) 网络，而无需向 AMS 支付额外费用。它提供对 AWS 资源和本地网络的集中式网络监控，在拓扑图和地理地图中提供其专用网络的单一全局视图，以及利用率指标，例如字节 in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down 连接状态。有关信息，请参阅 [AWS Network Manager](#)。

使用以下角色之一访问此资源：

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole

- AWSManagedServicesChangeManagementRole

出口 VPC

出口 VPC 主要用于向 Internet 的出口流量，由位于最多三个可用区的 public/private 子网组成 ()。AZs 网络地址转换 (NAT) 网关在公有子网中配置，传输网关 (TGW) VPC 附件在私有子网中创建。来自所有网络的出站或出站互联网流量通过 TGW 通过私有子网进入，然后通过 VPC 路由表路由到 NAT。

对于在公有子网中 VPCs 包含面向公众的应用程序的用户，源自 Internet 的流量包含在该 VPC 中。返回流量不会路由到 TGW 或出口 VPC，而是通过 VPC 中的互联网网关 (IGW) 路由回来。

Note

网络 VPC CIDR 范围：创建 VPC 时，必须以无类域间路由 (CIDR) 块的形式为 VPC 指定 IPv4 地址范围；例如 10.0.16.0/24。这是您的 VPC 的主要 CIDR 块。

AMS 多账户 landing zone 团队建议范围为 24 (具有更多 IP 地址)，以便在将来部署其他资源/设备时提供一些缓冲。

托管的帕洛阿尔托出口防火墙

AMS 提供托管 Palo Alto 出口防火墙解决方案，该解决方案支持对多账户着陆区环境中的所有网络 (不包括面向公众的服务) 中的所有网络进行互联网绑定出站流量过滤。该解决方案将业界领先的防火墙技术 (Palo Alto VM-300) 与 AMS 的基础设施管理功能相结合，可在合规的操作环境中部署、监控、管理、扩展和恢复基础架构。包括 Palo Alto Networks 在内的第三方无法访问防火墙；它们完全由 AMS 工程师管理。

交通管制

托管出站防火墙解决方案管理一个域允许列表，该列表由 AMS 必需的域组成，用于备份和补丁等服务，以及您定义的域。当出站 Internet 流量路由到防火墙时，将打开会话，评估流量，如果流量与允许的域相匹配，则将流量转发到目的地。

架构

托管出口防火墙解决方案遵循高可用性模式，即根据可用区域的数量部署两到三个防火墙 ()。AZs 该解决方案利用了默认出口 VPC 中的部分 IP 空间，但还预配置 VPC 扩展 (/24)，用于管理防火墙所需的额外资源。

网络流

总体而言，公共出口流量路由保持不变，但流量从出口 VPC 路由到 Internet 的方式除外：

1. 发往互联网的出口流量通过 VPC 路由表发送到 Transit Gateway (TGW)
2. TGW 通过 TGW 路由表将流量路由到出口 VPC
3. VPC 通过私有子网路由表将流量路由到互联网
 - a. 在默认的多账户着陆区环境中，互联网流量直接发送到网络地址转换 (NAT) 网关。托管防火墙解决方案重新配置私有子网路由表，改为将默认路由 (0.0.0.0/0) 指向防火墙接口。

防火墙本身包含三个接口：

1. 可信接口：用于接收待处理的流量的私有接口。
2. 不可信接口：用于向互联网发送流量的公共接口。由于防火墙执行 NAT，因此外部服务器接受来自这些公有 IP 地址的请求。
3. 管理接口：用于防火墙 API、更新、控制台等的私有接口。

在所有路由中，流量都保持在同一个可用区 (AZ) 内，以减少跨可用区的流量。只有在发生故障转移 AZs 时，流量才会交叉。

修改允许名单

入职后，将创建一个名为的默认允许列表，其中包含 AMS 所需的公共端点以及用于修补 Windows 和 Linux `ams-allowlist` 主机的公共端点。操作完成后，您可以在 AMS 控制台的“管理 | 托管防火墙 | 出站 (Palo Alto)”类别下创建 RFC，以创建或删除允许列表或修改域。请注意，这是 `ams-allowlist` 无法修改的。RFC 是完全自动化处理的（它们不是手动的）。

自定义安全策略

安全策略根据流量属性（例如源和目标安全区域、源和目标 IP 地址以及服务）来确定是阻止还是允许会话。全自动支持自定义安全策略 RFCs。CTs 创建或删除安全策略可以在管理 | 托管防火墙 | 出站（帕洛阿尔托）类别下找到，编辑现有安全策略的 CT 可以在部署 | 托管防火墙 | 出站（帕洛阿尔托）类别下找到。您将能够创建新的安全策略、修改安全策略或删除安全策略。

 Note

ams-allowlist无法修改默认安全策略

CloudWatch PA 出口仪表板

在中可以找到两个仪表板 CloudWatch 来提供帕洛阿尔托（宾夕法尼亚州）的汇总视图。AMS-MF-PA-egress-config-Dashboard 提供了 PA 配置概述、许可名单链接以及包括其属性在内的所有安全策略的列表。可以自定义 AMS-MF-PA-egress-Dashboard 以过滤流量日志。例如，要为安全策略创建控制面板，您可以使用以下筛选器创建 RFC：

[illegible]

故障转移模型

防火墙解决方案包括两三台帕洛阿尔托 (PA) 主机 (每个可用区一台)。健康检查加那利群岛按固定时间表运行, 以评估宿主的健康状况。如果主机被识别为运行状况不佳, 则会通知 AMS, 并通过更改路由表将该 AZ 的流量自动转移到另一可用区中的健康主机。由于运行状况检查工作流程持续运行, 因此如果主机由于暂时性问题或手动修复而恢复正常, 则流量将转移回主机的正确可用区。

扩展

AMS 监控防火墙的吞吐量和扩展限制。当吞吐量限制超过较低的水位线阈值（CPU/网络）时，AMS 会收到警报。低水机阈值表示资源已接近饱和，达到了 AMS 将随着时间的推移评估指标并伸出援手提出扩展解决方案的地步。

备份与还原

备份是在初始启动期间、任何配置更改后按固定时间间隔创建的。初始启动备份是以每台主机为单位创建的，但是调用备份工作流程时，将在所有防火墙主机上进行配置更改和定期间隔备份。AMS 工程师可以在这些窗口之外创建其他备份，或者根据要求提供备份详细信息。

如果需要，AMS 工程师可以恢复配置备份。如果需要恢复，则将在所有主机上进行恢复，以使主机之间的配置保持同步。

当主机需要完全回收实例时，也可以进行恢复。配置新 EC2 实例时，会自动恢复最新的备份。通常，主机不会定期回收，而是预留用于严重故障或必需的 AMI 交换。主机回收是手动启动的，并且在进行回收之前会通知您。

除了防火墙配置备份外，您的特定允许列表规则会单独备份。修改您定义的允许列表规则后，系统会自动创建备份。如果需要，可以由 AMS 工程师恢复允许名单备份。

更新

AMS 托管防火墙解决方案需要随着时间的推移进行各种更新，以增加系统的改进、其他功能或对防火墙操作系统 (OS) 或软件的更新。

大多数更改不会影响运行环境，例如更新自动化基础架构，但其他更改（例如防火墙实例轮换或操作系统更新）可能会导致中断。在评估更新可能导致的服务中断时，AMS 将与您协调以适应维护时段。

操作员访问权限

AMS 操作员使用其 ActiveDirectory 凭据登录帕洛阿尔托设备执行操作（例如，修补、响应事件等）。该解决方案保留了标准的 AMS 操作员身份验证和配置更改日志，以跟踪在 Palo Alto 主机上执行的操作。

默认日志

默认情况下，防火墙生成的日志存储在每个防火墙的本地存储中。随着时间的推移，将根据存储利用率删除本地日志。AMS 解决方案可将日志从计算机实时传送到 CloudWatch 日志；有关更多信息，请参阅[CloudWatch 日志集成](#)。

如果需要，AMS 工程师仍然可以直接从计算机上查询和导出日志。此外，还可以将日志发送到客户拥有的 Panorama；有关更多信息，请参阅[Panorama 集成](#)。

该解决方案收集的日志如下：

RFC 状态码

日志类型	说明
流量	显示每个会话开始和结束的条目。每个条目都包括日期和时间、源和目标区域、地址和端口、应用程序名称、应用于流的安全规则名称、规则操作（允许、拒绝或丢弃）、入口和出口接口、字节数以及会话结束原因。 “类型”列指示该条目是针对会话的开始还是结束，或者会话是被拒绝还是被删除。“丢弃”表示阻止流量的安全规则指定了“任何”应用程序，而“拒绝”表示该规则标识了特定的应用程序。 如果在识别应用程序之前丢弃了流量，例如规则丢弃了特定服务的所有流量，则该应用程序将显示为“不适用”。
威胁	显示防火墙生成的每个安全警报的条目。每个条目都包括日期和时间、威胁名称或 URL、源和目标区域、地址和端口、应用程序名称以及警报操作（允许或阻止）和严重性。 类型列表示威胁的类型，例如“病毒”或“间谍软件”；“名称”列是威胁描述或 URL；“类别”列是威胁类别（例如“键盘记录器”）或 URL 类别。
网址过滤	显示 URL 过滤器的日志，这些过滤器控制对网站的访问以及用户是否可以向网站提交凭据。
配置	显示每项配置更改的条目。每个条目都包括日期和时间、管理员用户名、进行更改的 IP 地址、客户机类型（Web 界面或 CLI）、命令运行的类型、命令成功还是失败、配置路径以及更改前后的值。
系统	显示每个系统事件的条目。每个条目都包括日期和时间、事件严重性以及事件描述。
警报	警报日志记录有关系统生成的警报的详细信息。此日志中的信息也会在警报中报告。请参阅“定义警报设置”。
身份验证	显示有关最终用户尝试访问由身份验证策略规则控制访问权限的网络资源时发生的身份验证事件的信息。用户可以使用这些信息来帮助解决访问问题，并根据需要调整用户身份验证策略。结合关联对象，用户还可以使用身份验证日志来识别用户网络上的可疑活动，例如暴力攻击。

日志类型	说明
	或者，用户可以将身份验证规则配置为记录身份验证超时。这些超时与用户只需要对资源进行一次身份验证但可以重复访问该资源的时间段有关。查看有关超时的信息可以帮助用户决定是否以及如何调整超时。
统一	在单个视图中显示最新的流量、威胁、URL 过滤、WildFire 提交和数据筛选日志条目。集体日志视图使用户能够一起调查和筛选这些不同类型的日志（而不是单独搜索每个日志集）。或者，用户可以选择要显示的日志类型：单击筛选字段左侧的箭头，然后选择流量、威胁、网址、数据、wildfire，以仅显示选定的日志类型。

活动管理

AMS 持续监控防火墙的容量、运行状况和可用性。防火墙生成的指标以及 AWS/AMS 生成的指标用于创建警报，AMS 运营工程师将收到这些警报，他们将调查并解决问题。当前警报涵盖以下情况：

事件警报：

- 防火墙数据平面 CPU 利用率
 - CPU 利用率-数据平面 CPU（处理流量）
- 防火墙数据平面数据包利用率高于 80%
 - 数据包利用率-数据平面（处理流量）
- 防火墙数据平面会话利用率
- 防火墙数据平面会话处于活动状态
- 聚合防火墙 CPU 利用率
 - 所有的 CPU 利用率 CPUs
- 按可用区进行故障转移
 - 可用区发生故障转移时发出警报
- 不健康的 Syslog 主机
 - Syslog 主机未通过运行状况检查

管理警报：

- Health Check 监控器故障警报

- 当运行状况检查工作流程意外失败时
- 这适用于工作流程本身，而不是防火墙运行状况检查失败的情况
- 密码轮换失败警报
 - 当密码轮换失败时
 - API/服务用户密码每 90 天轮换一次

指标

所有指标都被捕获并存储 CloudWatch 在网络账户中。可以通过获得网络帐户的控制台访问权限并导航到控制 CloudWatch 台来查看这些内容。可以在指标选项卡下查看单个指标，也可以通过导航到“控制面板”选项卡并选择 AMS-MF-PA-egress-Dashboard 来查看所选指标的单窗格仪表板视图和汇总指标。

自定义指标：

- 运行状况检查
 - 命名空间: AMS/MF/PA/Egress
 - PARouteTableConnectionsByAZ
 - PAUnhealthyByInstance
 - PAUnhealthyAggregatedByAZ
 - PAHealthCheckLockState
- 已生成防火墙
 - 命名空间：AMS/MF/PA/Egress/<instance-id>
 - DataPlaneCPUUtilizationPct
 - DataPlanePacketBufferUtilization
 - 平底锅 GPGateway UtilizationPct
 - panSessionActive
 - panSessionUtilization

CloudWatch 日志集成

CloudWatch 日志集成可将日志从防火墙转发到 CloudWatch 日志中，从而降低由于本地存储利用率而丢失日志的风险。日志会在防火墙生成时实时填充，并且可以通过控制台或 API 按需查看。

可以为日志分析构建复杂查询，也可以使用 CloudWatch Insights 导出到 CSV。此外，自定义 AMS Managed Firewall CloudWatch 控制面板还将显示特定流量日志查询的快速视图以及一段时间内流量和策略命中率的图表可视化。利用 CloudWatch 日志还可以实现与其他 AWS 服务（例如 AWS Kinesis）的本机集成。

Note

PA 日志无法直接转发到现有的本地或第三方 Syslog 收集器。AMS 托管防火墙解决方案可将日志从 PA 计算机实时传输到 AWS CloudWatch 日志。您可以使用 CloudWatch Logs Insight 功能来运行临时查询。此外，日志可以发送到您的帕洛阿尔托的 Panorama 管理解决方案。CloudWatch 也可以使用 CloudWatch 订阅过滤器将日志转发到其他目的地。在下一节中了解有关 Panorama 的更多信息。要了解有关 Splunk 的更多信息，请参阅[与 Splunk 集成](#)。

Panorama 集成

AMS 托管防火墙可以选择与您现有的 Panorama 集成。这使您可以从 Panorama 查看防火墙配置或将日志从防火墙转发到 Panorama。Panorama 与 AMS 托管防火墙的集成是只读的，不允许从 Panorama 更改防火墙的配置。Panorama 完全由您管理和配置，AMS 仅负责配置与其通信的防火墙。

许可

AMS 托管防火墙的价格取决于所使用的许可证类型、每小时许可证或自带许可证 (BYOL)，以及设备运行的实例大小。您需要通过 AWS Marketplace 订购您喜欢的帕洛阿尔托防火墙的实例大小和许可证。

- Marketplace 许可：接受 MALZ 网络账户中虚拟机系列下一代防火墙捆绑包 1 的条款和条件。
- BYOL 许可证：接受 MALZ 网络账户中虚拟机系列下一代防火墙 (BYOL) 的条款和条件，并将购买许可证后获得的“BYOL 身份验证码”共享给 AMS。

限制

目前，AMS 支持 VM-300 系列或 VM-500 系列防火墙。可以在此处找到配置：[AWS EC2 实例上的 VM 系列模型](#)，

Note

AMS 解决方案在 Active-Active 模式下运行，因为其可用区中的每个 PA 实例都会处理其相应可用区的出口流量。因此，如果有两个 PA 实例 AZs，则每个 PA 实例可处理高达 5 Gbps 的出口流量，并有效地在两个实例之间提供 10 Gbps 的总吞吐量。AZs 每个可用区中的所有限制也是如此。如果 AMS 运行状况检查失败，我们会将流量从 PA 不佳的可用区转移到另一个可用区，在实例替换期间，容量将减少到剩余 AZs 限制。

AMS 目前不支持 AWS Marketplace 上提供的其他 Palo Alto 捆绑包；例如，您不能索取“VM 系列下一代防火墙捆绑包 2”。请注意，使用 Palo Alto 的 AMS 托管防火墙解决方案目前仅提供出口流量过滤服务，因此使用高级 VM 系列捆绑包不会提供任何其他功能或优势。

入职要求

- 您必须在 AWS Marketplace 中查看并接受帕洛阿尔托推出的虚拟机系列下一代防火墙的条款和条件。
- 您必须根据您的预期工作负载确认要使用的实例大小。
- 您必须提供与多账户着陆区环境或本地网络不冲突的 /24 CIDR 区块。它必须与出口 VPC 属于同一类别（解决方案为出口 VPC 预配置 /24 VPC 扩展）。

定价

AMS 托管防火墙基础架构成本分为三个主要驱动因素：托管 Palo Alto 防火墙的 EC2 实例、软件许可证 Palo Alto VM 系列许可证和集成。CloudWatch

以下定价基于 VM-300 系列防火墙。

- EC2 实例：Palo Alto 防火墙在 2-3 个 EC2 实例的高可用性模型中运行，其中实例基于预期的工作负载。实例的成本取决于地区和数量 AZs
 - 例如 us-east-1、m5.xlarge、3 AZs
 - $0.192 * 24 * 30 * 3 = 414.72$ 美元
 - <https://aws.amazon.com/ec2/定价/按需定价/>
- 帕洛阿尔托许可证：Palo Alto VM-300 下一代防火墙的软件许可成本取决于可用区的数量和实例类型。
 - 例如 us-east-1、m5.xlarge、3 AZs
 - $0.87 * 24 * 30 * 3 = 1879.20$ 美元

- https://aws.amazon.com/marketplace/pp/b083m7jpkb?ref_=srh_res_product_title#pdp-pricing
- CloudWatch 日志集成：CloudWatch 日志集成使用 SysLog 服务器 (EC2 -t3.medium)、NLB 和日志。CloudWatch 服务器的成本取决于区域和数量 AZs，NLB/CloudWatch 日志的成本因流量利用率而异。
 - 例如 us-east-1、t3.medium、3AZ
 - $0.0416 * 24 * 30 * 3 = 89.86$ 美元
 - <https://aws.amazon.com/ec2/定价/按需定价/>
 - <https://aws.amazon.com/cloudwatch/定价/>

周长 (DMZ) VPC

外围或 DMZ、VPC 包含 AMS 运营工程师访问 AMS 网络所需的必要资源。它包含跨越 2-3 个的公共子网 AZs，在 Auto Scaling 组 (ASG) 中包含 SSH 堡垒主机，AMS 运营工程师可以登录或通过隧道通过。附加到隔离区堡垒的安全组包含来自亚马逊公司网络的端口 22 入站规则。

DMZ VPC CIDR 范围：创建 VPC 时，必须以无类域间路由 (CIDR) 块的形式为 VPC 指定 IPv4 地址范围；例如 10.0.16.0/24。这是您的 VPC 的主要 CIDR 块。

Note

AMS 团队建议将范围设为 24（具有更多 IP 地址），以便在将来部署其他资源（例如防火墙）时提供一些缓冲。

AWS Transit Gateway

AWS Transit Gateway (TGW) 是一项服务，可让您将亚马逊虚拟私有云 (VPCs) 和本地网络连接到单个网关。传输网关是处理 AMS 账户网络和外部网络之间路由的网络主干。有关 Transit Gateway 的信息，请参阅 [AWS Transit Gateway](#)。

提供以下输入以创建此资源：

- Transit Gateway ASN 编号 *：为您的公交网关提供私有自治系统编号 (ASN)。这应该是边界网关协议 (BGP) 会话的 AWS 端的 ASN。16 位的范围为 64512 到 65534。ASNs

共享服务账户

共享服务账户是大多数 AMS 数据平面服务的中心枢纽。该账户包含访问管理 (AD)、端点安全管理 (趋势科技) 所需的基础架构和资源，还包含客户堡垒 (SSH/RDP)。下图显示了共享服务帐户中包含的资源的高级概述。

共享服务 VPC 由三个可用区中的 AD 子网、EPS 子网和客户堡垒子网组成 (AZs)。下面列出了在共享服务 VPC 中创建的资源，需要您输入。

- 共享服务 VPC CIDR 范围：创建 VPC 时，必须以无类域间路由 (CIDR) 块的形式为 VPC 指定 IPv4 地址范围；例如 10.0.1.0/24。这是您的 VPC 的主要 CIDR 块。

Note

AMS 团队建议的射程为 /23。

- A@@@ ctive Directory 详情：Microsoft Active Directory (AD) 用于 user/resource 管理、身份验证/授权 and 所有 AMS 多账户登录区域账户的 DNS。AMS AD 还配置了对您的 Active Directory 的单向信任，以进行基于信任的身份验证。创建 AD 需要以下输入：
 - 域名完全限定域名 (FQDN)：AWS 托管的 Microsoft AD 目录的完全限定域名。该域不应是现有域或网络中现有域的子域。
 - 域 NetBIOS 名称：如果您未指定 NetBIOS 名称，AMS 会将该名称默认为您的目录 DNS 的第一部分。例如，corp 代表目录 DNS corp.example.com。
- 趋势科技-端点保护安全 (EPS)：趋势科技端点保护 (EPS) 是 AMS 中用于操作系统安全的主要组件。该系统由趋势科技服务器深度安全防护系统管理中心 (DSM)、EC2 EC2 实例、中继实例以及存在于所有数据平面和客户 EC2 实例中的代理组成。

您必须使用共享服务帐户，并订阅趋势科技服务器深度安全防护系统 (BYOL) AMI 或趋势科技趋势科技服务器深度安全防护系统 (Marketplace)。EPSMarketplaceSubscriptionRole

创建 EPS 需要以下默认输入 (如果您想更改默认值)：

- 中继实例类型：默认值-m5.large
- DSM 实例类型：默认值-m5.xlarge
- 数据库实例大小：默认值-200 GB
- RDS 实例类型：默认值——db.m5.large

- 客户堡垒：共享服务账户中为您提供 SSH 或 RDP 堡垒（或两者兼而有之），用于访问您的 AMS 环境中的其他主机。为了以用户身份访问 AMS 网络（SSH/RDP），you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/VPN 到传输网关 (TGW)，然后路由到共享服务 VPC。一旦您能够访问堡垒，就可以跳转到 AMS 环境中的其他主机，前提是访问请求已获得批准。
- SSH 堡垒需要以下输入。
 - SSH 堡垒所需实例容量：默认值-2。
 - SSH 堡垒最大实例数：默认值-4。
 - SSH 堡垒最低实例数：默认值 -2。
 - SSH 堡垒实例类型：默认值-m5.large（可以更改以节省成本；例如 t3.medium）。
 - SSH 堡垒入口 CIDRs：您网络中的用户从中访问 SSH 堡垒的 IP 地址范围。
- Windows RDP 堡垒需要以下输入。
 - RDP 堡垒实例类型：默认值-t3.medium。
 - RDP Bastion 所需的最小会话数：默认值-2。
 - RDP 最大会话数：默认值 -10。
 - RDP 堡垒配置类型：您可以选择以下配置之一
 - SecureStandard = 一个用户收到一个堡垒，只有一个用户可以连接到堡垒。
 - SecureHA = 用户在两个不同的可用区收到两个堡垒可供连接，并且只有一个用户可以连接到堡垒。
 - SharedStandard = 一个用户收到一个要连接的堡垒，两个用户可以同时连接到同一个堡垒。
 - SharedHA = 用户在两个不同的 AZ 中收到两个堡垒可供连接，两个用户可以同时连接到同一个堡垒。
 - 客户 RDP 入口 CIDRs：您网络中的用户将从中访问 RDP 堡垒的 IP 地址范围。

共享服务更新：多账户登录区

AMS 每月向托管账户发布数据平面版本，恕不另行通知。

AMS 使用核心 OU 在您的多账户着陆区提供共享服务，例如访问、联网、EPS、日志存储、警报聚合。AMS 负责解决这些共享服务的漏洞、修补和部署。AMS 会定期更新用于提供这些共享服务的资源，以便用户可以访问最新功能和安全更新。更新通常每月进行一次。这些更新中包含的资源有：

- 属于核心 OU 的账户。

管理账户、共享服务账户、网络账户、安全账户和日志存档账户拥有用于 RDP 和 SSH 堡垒、代理、管理主机和端点安全 (EPS) 的资源，这些资源通常每月更新一次。AMS 使用不可变 EC2 部署作为共享服务基础设施的一部分。

- AMIs 包含最新更新的新 AMS。

Note

AMS 操作员在执行数据平面更改时使用内部警报抑制更改类型 (CT)，并且该 CT 的 RFC 会显示在您的 RFC 列表中。这是因为，在部署数据平面版本时，各种基础架构可能会关闭、重新启动、离线，或者部署可能会出现 CPU 峰值或其他影响，从而触发在数据平面部署期间无关的警报。部署完成后，将验证所有基础设施是否正常运行，并重新启用警报。

日志存档账户

日志存档账户是在 AMS 多账户 landing zone 环境中存档日志的中心中心。账户中有一个 S3 存储桶，其中包含每个 AMS 多账户着陆区环境账户的 AWS CloudTrail 和 AWS Config 日志文件的副本。您可以将此账户用于与 AWS Firehose 或 Splunk 等相关的集中式日志解决方案。AMS 仅限少数用户访问此账户；仅限审计师和安全团队进行与账户活动相关的合规和取证调查。

安全账户

安全账户是住房保障相关操作的中心枢纽，也是向 AMS 控制飞机服务发送通知和警报的主要点。此外，安全账户还存放了 Amazon Guard Duty 管理账户和 AWS Config 聚合器。

应用程序账户类型

应用程序账户是您用来托管工作负载的 AMS 管理的 landing zone 架构中的 AWS 账户。AMS 提供三种类型的应用程序账户：

- [AMS 管理的应用程序账户](#)
- [AMS 加速账户](#)
- [客户托管应用程序账户](#)

根据应用程序账户类型，AWS Organizations OUs 中的应用程序账户按不同的分组方式：

- root OU :
 1. 应用程序 OU
 - 托管 OU : AMS 管理的账户
 - 开发 OU : 启用开发者模式的 AMS 管理的账户
 2. 加速 OU : AMS 加速应用程序账户
 3. 客户管理的 OU : 客户管理的应用程序帐户

应用程序账户通过管理账户提交的 RFC 进行配置 :

- 使用 VPC 创建应用程序账户 `ct-1zdas` [mc2ewzrs](#)
- 创建加速账户 [ct-2p93tyd5angmi](#)
- [创建客户管理的应用程序账户](#) `ct-3pwbixz27n3tn`

AMS 管理的应用程序账户

完全由 AMS 管理的应用程序帐户称为 AMS 管理的应用程序帐户，其中部分或全部操作任务，例如服务请求管理、事件管理、安全管理、连续性管理（备份）、补丁管理、成本优化或基础设施的监控和事件管理，由 AMS 执行。

AMS 执行的任务数量取决于您选择的变更管理模式。AMS 管理的账户支持不同的变更管理模式：

- [RFC 模式](#)
- [AMS 中的直接更改模式](#)
- [AMS 和 AWS Service Catalog](#)
- [AMS 高级开发者模式](#)
- [AMS 中的自助服务配置模式](#)

有关变更管理和不同模式的更多信息，请参阅[更改管理模式](#)。

有些 AWS 服务可以在您的 AMS 托管账户中使用，而无需管理 AMS。[自助服务配置](#)部分介绍了这些 AWS 服务的列表以及如何将其添加到您的 AMS 账户。

AMS 加速账户

AMS Accelerate 是 AMS 运营计划，可以运行支持工作负载的 AWS 基础设施。您可以从 AMS Accelerate 运营服务（例如监控和警报、事件管理、安全管理和备份管理）中受益，而无需进行新的迁

移、停机或更改 AWS 的使用方式。AMS Accelerate 还为需要定期修补的 EC2 基于工作负载提供了可选的补丁插件。

借助 AMS Accelerate，您可以自由地在本地或使用首选工具使用、配置和部署所有 AWS 服务。您将使用首选的访问和变更机制，而 AMS 将始终如一地采用久经考验的实践，帮助您扩大团队规模、优化成本、提高安全性和效率并提高弹性。

Note

AMS Advanced 中的 AMS Accelerate 账户没有 AMS 变更管理 (RFCs) 或 AMS 高级控制台。相反，他们有 AMS Accelerate 控制台和功能。

加速账户只能通过您的 AMS 多账户 landing zone 管理账户进行配置。加速提供不同的运营能力。要了解更多信息，请参阅[加速服务说明](#)。

- 您将继续享受多账户着陆区 (MALZ) 核心账户的某些功能，例如集中记录、单一账单、安全账户中的 Config Aggregator 和。 SCPs
- AMS Accelerate 不提供某些 AMS 高级服务，例如 EPS、访问管理、变更管理和配置。我们建议您按照以下步骤获取访问权限并配置传输网关 (TGW)。

有关加速的更多详细信息，请参阅[什么是加速](#)。

创建您的加速账户

要创建加速账户，请按照此处列出的步骤[创建加速账户](#)。

访问您的加速账户

在您的多账户 landing zone (MALZ) 账户中配置 Accelerate 账户
后AccelerateDefaultAdminRole，账户中将有一个具有[管理访问](#)权限的角色供您代入。

要访问新的加速账户，请执行以下操作：

1. 使用该角色登录管理账户的 IAM 控制台。CustomerDefaultAssumeRole
2. 在 IAM 控制台的导航栏上，选择您的用户名。
3. 选择切换角色。如果这是您首次选择该选项，则会显示一个包含更多信息的页面。在阅读该信息后，请选择切换角色。如果清除您的浏览器 Cookie，则此页面会重新再出现。

4. 在“切换角色”页面上，键入加速账户 ID 和要代入的角色名称：`AccelerateDefaultAdminRole`。

现在您可以访问了，可以创建新的 IAM 角色来继续访问您的环境。如果您想将 SAML 联合身份验证用于您的加速账户，请参阅[启用 SAML 2.0 联合用户访问 AWS 管理](#)控制台。

将你的加速账户与 Transit Gateway 关联起来

AMS 不管理加速账户的网络设置。您可以选择使用 AWS APIs（参见[网络解决方案](#)）管理自己的网络，也可以使用 AMS MALZ 中部署的现有 Transit Gateway (TGW) 连接到由 AMS 管理的 MALZ 网络。

 Note

只有当加速账户位于同一 AWS 区域时，您才能将 VPC 关联到 TGW。有关更多信息，请参阅[公网网关](#)。

要将你的 Accelerate 账户添加到 Transit Gateway，请使用[部署 | 托管着陆区 | 网络账户 | 添加静态路线](#) (ct-3r2ckznmt0a59) 更改类型申请新路线，包括以下信息：

- `Blackhole` : `True` 表示路线的目标不可用。当 Transit Gateway 要丢弃静态路由的流量时，请执行此操作。如果将流量路由到指定的 TGW 附件 ID，则为假。默认值为 `false`。
- `DestinationCidrBlock` : 用于目标匹配的 IPV4 CIDR 范围。路由判断是根据最具体的匹配确定的。示例：`10.0.2.0/24`。
- `TransitGatewayAttachmentId` : 将用作路由表目标的 TGW 附件 ID。如果 `Blackhole` 为假，则此参数为必填项，否则将此参数留空。示例：`tgw-attach-04eb40d1e14ec7272`。
- `TransitGatewayRouteTableId`: TGW 路由表的 ID。示例：`tgw-rtb-06ddc751c0c881c`。

在 TGW 路由表中创建路由以连接到此 VPC：

1. 默认情况下，此 VPC 将无法与您的 MALZ 网络 VPCs 中的任何其他 VPC 通信。
2. 与您的解决方案架构师一起决定 VPCs 您希望这个 Accelerate VPC 与什么通信。
3. 提交[部署 | 托管着陆区 | 网络账户 | 添加静态路由](#) (ct-3r2ckznmt0a59) 更改类型，包括以下信息：
 - `Blackhole` : `True` 表示路线的目标不可用。当 Transit Gateway 要丢弃静态路由的流量时，请执行此操作。如果将流量路由到指定的 TGW 附件 ID，则为假。默认值为 `false`。

- DestinationCidrBlock：用于目标匹配的 IPV4 CIDR 范围。路由判断是根据最具体的匹配确定的。示例：10.0.2.0/24。
- TransitGatewayAttachmentId：将用作路由表目标的 TGW 附件 ID。如果 Blackhole 为假，则此参数为必填项，否则将此参数留空。示例：tgw-attach-04eb40d1e14ec7272。
- TransitGatewayRouteTableId：TGW 路由表的 ID。示例：tgw-rtb-06ddc751c0c881c。

将新的加速账户 VPC 连接到 AMS 多账户着陆区网络（创建 TGW VPC 附件）：

1. 在您的多账户 landing zone 网络账户中，打开 [Amazon VPC 控制台](#)。
2. 在导航窗格中，选择 Transit Gateways（中转网关）。记录您看到的公交网关的 TGW ID。
3. 在您的加速账户中，打开 [亚马逊 VPC 控制台](#)。
4. 在导航窗格中，选择 Transit Gateway 附件 > 创建 Transit Gateway 附件。做出以下选择：
 - 对于 Transit Gateway ID，请选择您在步骤 2 中记录的公交网关 ID。
 - 对于 Attachment type（连接类型），选择 VPC。
 - 在 VPC Attachment（VPC 挂载）下，（可选）为 Attachment name tag（挂载名称标签）键入名称。
 - 选择是否启用 DNS Support and Support IPv6。
 - 对于 VPC ID，选择要附加到中转网关的 VPC。此 VPC 必须至少有一个子网与其关联。
 - 对于子网 IDs，为每个可用区选择一个子网，供传输网关用于路由流量。您必须至少选择一个子网。您只能为每个可用区域选择一个子网。
5. 选择 Create attachment（创建挂载）。记录新创建的 TGW 附件的 ID。

将 TGW 附件关联到路由表：

1. 决定您要将 VPC 与哪个 TGW 路由表关联。我们建议 VPCs 使用部署 | 托管着陆区 | 网络账户 | 创建公交网关路由表 (ct-3dscwaeyi6cup) 更改类型为 Accelerate 账户创建新的应用程序路由表。
2. 在网络账户上提交 [管理 | 托管着陆区 | 网络账户 | 关联 TGW 附件](#) (ct-3nmhh0qr338q6) RFC，将 VPC 或 TGW 附件关联到你选择的路由表。

在 TGW 路由表中创建路由以连接到此 VPC：

1. 默认情况下，此 VPC 将无法与您的多账户 landing zone 网络 VPCs 中的任何其他 VPC 通信。
2. 与您的解决方案架构师一起决定 VPCs 您希望这个 Accelerate 账户 VPC 与什么通信。

3. 提交[部署 | 托管着陆区 | 网络账户 | 针对网络账户添加静态路由](#) (ct-3r2ckznmt0a59) RFC 以创建你需要的 TGW 路由。

将您的 VPC 路由表配置为指向 AMS 多账户 landing zone 公交网关：

1. 与您的解决方案架构师一起决定要向 AMS 多账户着陆区公交网关发送哪些流量。
2. 提交[部署 | 托管着陆区 | 网络账户 | 针对网络账户添加静态路由](#) (ct-3r2ckznmt0a59) RFC 以创建你需要的 TGW 路由。

客户托管应用程序账户

您可以创建 AMS 无法以标准方式管理的账户。这些账户被称为客户管理账户，它们使您可以完全控制账户内的基础设施，同时享受由 AMS 管理的集中式架构的好处。

客户托管账户无权访问 AMS 控制台或我们提供的任何服务（补丁、备份等）。

客户管理账户只能通过您的 AMS 多账户 landing zone 管理账户进行配置。

不同的 AMS 模式对应用程序账户的使用方式不同；要了解有关这些模式的更多信息，请参阅 [AWS Managed Services 模式](#)。

要创建您的客户托管应用程序帐户，请参阅[管理账户 | 创建客户管理的应用程序帐户](#)。

要删除客户管理的应用程序帐户，请使用[管理帐户 | Offboard 应用程序帐户](#)。（[确认离职](#) CT 不适用于客户管理的应用程序账户。）

访问您的客户管理账户

在多账户 landing zone 中配置客户管理账户 (CMA) 后，账户中将有一个管理员角色 (MALZ)CustomerDefaultAdminRole，供您通过 SAML 联合代入来配置账户。

要访问 CMA，请执行以下操作：

1. 使用该角色登录管理账户的 IAM 控制台。CustomerDefaultAssumeRole
2. 在 IAM 控制台的导航栏上，选择您的用户名。
3. 选择切换角色。如果这是您首次选择该选项，则会显示一个包含更多信息的页面。在阅读该信息后，请选择切换角色。如果清除您的浏览器 Cookie，则此页面会重新再出现。
4. 在“切换角色”页面上，键入客户管理的账户 ID 和要担任的角色的名称：CustomerDefaultAdminRole。

现在您可以访问了，可以创建新的 IAM 角色来继续访问您的环境。如果您想将 SAML 联合身份验证用于您的 CMA 账户，请参阅[启用 SAML 2.0 联合用户访问 AWS 管理控制台](#)。

将 CMA 与 Transit Gateway 连接起来

AMS 不管理客户管理账户 (CMAs) 的网络设置。您可以选择使用 AWS APIs (参见[联网解决方案](#)) 管理自己的网络，也可以使用 AMS MALZ 中部署的现有 Transit Gateway (TGW) 连接到由 AMS 管理的多账户着陆区网络。

Note

只有当 CMA 位于同一 AWS 区域时，您才能将 VPC 连接到 TGW。有关更多信息，请参阅[公网网关](#)。

要将你的 CMA 添加到 Transit Gateway，请使用[网络账户申请一条新路线 | 添加静态路由 \(ct-3r2ckznm t0a59\)](#) 更改类型并包含以下信息：

- **Blackhole** : True 表示路线的目标不可用。当 Transit Gateway 要丢弃静态路由的流量时，请执行此操作。如果将流量路由到指定的 TGW 附件 ID，则为假。默认值为 false。
- **DestinationCidrBlock** : 用于目标匹配的 IPV4 CIDR 范围。路由判断是根据最具体的匹配确定的。示例：10.0.2.0/24。
- **TransitGatewayAttachmentId** : 将用作路由表目标的 TGW 附件 ID。如果 Blackhole 为假，则此参数为必填项，否则将此参数留空。示例：tgw-attach-04eb40d1e14ec7272。
- **TransitGatewayRouteTableId**: TGW 路由表的 ID。示例：tgw-rtb-06ddc751c0c0c881c。

将新的客户管理的 VPC 连接到 AMS 多账户着陆区域网络 (创建 TGW VPC 附件)：

1. 在您的多账户 landing zone 网络账户中，打开 [Amazon VPC 控制台](#)。
2. 在导航窗格中，选择传输网关。记录您看到的公网网关的 TGW ID。
3. 在您的客户管理账户中，打开 [Amazon VPC 控制台](#)。
4. 在导航窗格中，选择 Transit Gateway 附件 > 创建 Transit Gateway 附件。做出以下选择：
 - a. 对于 Transit Gateway ID，请选择您在步骤 2 中记录的公网网关 ID。
 - b. 对于 Attachment type (连接类型)，选择 VPC。
 - c. 在 VPC Attachment (VPC 挂载) 下，(可选) 为 Attachment name tag (挂载名称标签) 键入名称。

- d. 选择是否启用 DNS Support and S u IPv6 ppor t。
 - e. 对于 VPC ID，选择要附加到中转网关的 VPC。此 VPC 必须至少有一个子网与其关联。
 - f. 对于子网 IDs，为每个可用区选择一个子网，供传输网关用于路由流量。您必须至少选择一个子网。您只能为每个可用区域选择一个子网。
5. 选择 Create attachment (创建挂载)。记录新创建的 TGW 附件的 ID。

将 TGW 附件关联到路由表：

决定您要将 VPC 与哪个 TGW 路由表关联。我们建议提交部署 | 托管 VPCs 着陆区 | 网络账户 | 创建公交网关路由表 (ct-3dscwaeyi6cup) RFC，为客户管理创建新的应用程序路由表。要将 VPC 或 TGW 附件关联到您选择的路由表，请在网络账户上提交部署 | 托管着陆区 | 网络账户 | 关联 TGW 附件 (ct-3nmhh0qr338q6) RFC。

在 TGW 路由表中创建路由以连接到此 VPC：

1. 默认情况下，此 VPC 将无法与您的多账户着陆区网络 VPCs 中的任何其他 VPC 通信。
2. 与您的解决方案架构师一起决定 VPCs 您希望此客户托管的 VPC 与什么通信。提交部署 | 托管着陆区 | 网络账户 | 针对网络账户添加静态路由 (ct-3r2ckznmt0a59) RFC 以创建你需要的 TGW 路由。

 Note

此 CT (ct-3r2ckznmt0a59) 不允许向核心路由表添加静态路由 EgressRouteDomain；如果您的 CMA 需要允许出口流量，请使用 ct-0xdawir96cy7k 提交管理 | 其他 | 其他 (MOO) RFC。

将您的 VPC 路由表配置为指向 AMS 多账户着陆区中转网关：

与您的解决方案架构师一起决定要向 AMS 多账户着陆区公交网关发送哪些流量。更新您的 VPC 路由表以将流量发送到之前创建的 TGW 附件

获取有关客户管理账户的运营帮助

AMS 可以通过将客户托管账户注册到 AMS Accelerate 来帮助您在客户管理账户中部署的工作负载。借助 AMS Accelerate，您可以从监控和警报、事件管理、安全管理和备份管理等运营服务中受益，而无需进行新的迁移、停机或更改使用 AWS 方式。AMS Accelerate 还为需要定期修补的 EC2 基于工作负载提供了可选的补丁插件。使用 AMS Accelerate，您可以继续以本地方式或首选工具使用、配置和部署所有 AWS 服务；就像使用 AMS 高级客户管理账户一样。您使用首选的访问和变更机制，而 AMS 则采用久经考验的实践，帮助您扩大团队规模、优化成本、提高安全性和效率并提高弹性。要了解更多信息，请参阅[加速服务说明](#)。

要将您的客户管理账户注册到 Accelerate，请联系您的 CSDM 并按照 [AMS Accelerate 入门中的步骤](#) 进行操作。

Note

AMS Advanced 中的 AMS Accelerate 账户没有 AMS 变更管理（变更请求或 RFCs）或 AMS 高级控制台。相反，他们有 AMS Accelerate 控制台和功能。

AMS 工具账户（迁移工作负载）

您的多账户着陆区工具账户（使用 VPC）有助于加快迁移工作，提高您的安全地位，降低成本和复杂性，并标准化您的使用模式。

工具账户提供以下内容：

- 为系统集成商在生产工作负载之外访问复制实例提供了明确的边界。
- 允许您创建一个隔离的密室，以检查工作负载中是否存在恶意软件或未知的网络路由，然后再将其存入具有其他工作负载的帐户。
- 作为定义的帐户设置，它可以更快地为工作负载迁移做好准备和准备。
- 隔离的网络路由到来自本地 -> 工具账户 - CloudEndure > AMS 摄取的图像的安全流量。提取图像后，您可以通过 AMS 管理 | 高级堆栈组件 | AMI | 共享 (ct-1eiczxw8ihc18) RFC 将图像共享到目标账户。

高级架构图：

使用部署 | 托管着陆区 | 管理账户 | 创建工具账户 (使用 VPC) 更改类型 (ct-2j7q1hgf26x5c), 在多账户着陆区环境中快速部署工具账户并实例化工作负载摄取流程。参见[管理账户, 工具账户: 创建 \(使用 VPC\)](#)。

Note

我们建议有两个可用区 (AZs), 因为这是一个迁移中心。

默认情况下, AMS 在每个账户中创建以下两个安全组 (SGs)。确认这两个 SGs 都存在。如果他们不在场, 请向 AMS 团队提交新的服务申请, 请求他们。

- SentinelDefaultSecurityGroupPrivateOnlyEgressAll
- InitialGarden-SentinelDefaultSecurityGroupPrivateOnly

确保在私有子网中创建 CloudEndure 复制实例, 那里有返回本地的路由。您可以通过确保私有子网的路由表中包含返回 TGW 的默认路由来确认这一点。但是, 执行 CloudEndure 计算机切换操作应进入“隔离”私有子网, 那里没有返回本地的路由, 只允许 Internet 出站流量。确保在隔离子网中进行切换, 以避免本地资源出现潜在问题, 这一点至关重要。

先决条件:

1. 高级或高级支持级别。
2. 部署的 KMS 密钥 AMIs 的应用程序账户 IDs 。
3. 工具账户, 如前所述。

AWS 应用程序迁移服务 (AWS MGN)

[AWS 应用程序迁移服务](#) (AWS MGN) 可以通过在工具账户配置期间自动创建的 AWSManagedServicesMigrationRole IAM 角色在您的 MALZ Tools 账户中使用。您可以使用 AWS MGN 迁移在支持版本的 Windows 和 Linux [操作系统](#)上运行的应用程序和数据库。

有关 AWS 区域 支持的大部分 up-to-date 信息, 请参阅[AWS 区域服务列表](#)。

如果 AWS MGN AWS 区域 目前不支持您的首选项, 或者 AWS MGN 目前不支持运行应用程序的操作系统, 请考虑改用工具账户中的[CloudEndure 迁移](#)。

正在请求 AWS MGN 初始化

AWS MGN 在首次使用前必须由 AMS 进行[初始化](#)。要申请新的 Tools 账户，请提交 Tools 账户中的管理 | 其他 | 其他 RFC，其中包含以下详细信息：

RFC Subject=Please initialize AWS MGN in this account

RFC Comment=Please click 'Get started' on the MGN welcome page here:

https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using all default values to 'Create template' and complete the initialization process.

AMS 成功完成 RFC 并在您的 Tools 账户中初始化 AWS MGN 后，您可以使用编辑默认模板 `AWSManagedServicesMigrationRole` 以满足您的要求。

启用对新 AMS Tools 账户的访问权限

创建工具账户后，AMS 会为您提供账户 ID。下一步是配置对新账户的访问权限。执行以下步骤。

1. 将相应的 Active Directory 组更新为相应的帐户 IDs。

AMS 创建的新账户将使用 `ReadOnly` 角色策略以及允许用户申报的角色进行配置。RFCs

Tools 账户还有一个额外的 IAM 角色和用户可用：

- IAM 角色：`AWSManagedServicesMigrationRole`
- IAM 用户：`customer_cloud_endure_user`

2. 请求策略和角色以允许服务集成团队成员设置更高级别的工具。

导航到 AMS 控制台并归档以下内容 RFCs：

- a. 创建 KMS 密钥。使用[创建 KMS 密钥 \(auto\)](#) 或[创建 KMS 密钥 \(需要查看\)](#)。

当您使用 KMS 加密提取的资源时，使用与其余多账户着陆区应用程序账户共享的单个 KMS 密钥可以为摄取的图像提供安全保护，这些图像可以在目标账户中解密。

- b. 共享 KMS 密钥。

使用管理 | 高级堆栈组件 | KMS 密钥 | 共享 (需要查看) 更改类型 (ct-05yb337abq3x5) 请求将新的 KMS 密钥共享给已提取的应用程序账户。AMIs

最终账户设置的示例图：

AMS 预先批准的 IAM CloudEndure 政策示例

要查看 AMS 预先批准的 IAM CloudEndure 政策：解压 [WIGS Cloud Endure 着陆区域示例](#) 文件并打开。customer_cloud_endure_policy.json

测试 AMS Tools 账户连接和 end-to-end 设置

1. 首先要在要复制到 AMS 的服务器上配置 CloudEndure 和安装 CloudEndure 代理。
2. 在中创建项目 CloudEndure。
3. 通过 secrets Manager 输入执行先决条件时共享的 AWS 凭据。
4. 在“复制”设置中：
 - a. 选择 AMS “Sentinel” 安全组（仅限私有和 EgressAll），选择“选择要应用于复制服务器的安全组”选项。
 - b. 为计算机（实例）定义转换选项。有关信息，请参阅[步骤 5。切开](#)
 - c. 子网：私有子网。
5. 安全组：
 - a. 同时选择 AMS “Sentinel” 安全组（仅限私有和 EgressAll）。
 - b. 切换实例必须与 AMS 管理的 Active Directory (MAD) 和公共终端节点通信：AWS
 - i. 弹性 IP：无
 - ii. 公有 IP：否
 - iii. IAM 角色：customer-mc-ec 双实例配置文件
 - c. 按照您的内部标签惯例设置标签。
6. 在计算机上安装 CloudEndure 代理，然后在 EC2 控制台中查找要出现在您的 AMS 账户中的复制实例。

AMS 摄取过程：

AMS Tools 账户卫生

在账户中共享了 AMI 并且不再需要复制的实例之后，您需要清理：

- 实例 WIGs 摄取后：
 - 切换实例：至少在工作完成后，通过 AWS 控制台停止或终止此实例
 - 摄取前 AMI 备份：在接入实例且本地实例终止后将其删除

- AMS 摄取的实例：在共享 AMI 后关闭堆栈或终止
- AMS-ingame AMIs 删除：与目标账户共享完成后删除
- 迁移结束清理：记录通过开发人员模式部署的资源，以确保定期进行清理，例如：
 - 安全组
 - 通过云形成创建的资源
 - 网络 ACK
 - 子网
 - VPC
 - 路由表
 - 角色
 - 用户和账户

大规模迁移-迁移工厂

请参阅 [AWS CloudEndure 迁移工厂解决方案简介](#)。

SALZ 网络架构

下图描述了 AWS Managed Services (AMS) 单账户着陆区 (SALZ) VPC 网络布局，是高可用性设置的示例。

AMS 根据我们的标准模板和您在入职期间提供的选择选项为您配置网络的各个方面。标准的 AWS 网络设计适用于您的 AWS 账户，然后为您创建虚拟私有云 (VPC)，并通过 VPN 或 Direct Connect 连接到 AMS。在 [AWS Direct Connect 上详细了解 Direct Connect](#)。标准 VPCs 包括 DMZ、共享服务和应用程序子网。在入职过程中，VPCs 可能会要求并创建其他内容以满足您的需求（例如，客户部门、合作伙伴）。入门后，你会得到一张网络图。这是一份环境文档，说明你的网络是如何设置的。

Note

要了解所有活动服务的默认服务限制和限制，请参阅 [AWS 服务限制](#) 文档。

我们的网络设计围绕 Amazon 的“[最低权限原则](#)”构建。为了实现这一目标，除了来自可信网络的流量外，我们通过网关路由所有流量，包括入站和出站流量。唯一可信的网络是通过使用 VPN 和 AWS

Direct Connect (DX) 在您的本地环境和 VP and/or C 之间配置的网络。通过使用堡垒实例授予访问权限，从而防止直接访问任何生产资源。您的所有应用程序和资源都位于可通过公共负载均衡器访问的私有子网中。公共出口流量通过我们的正向代理流向 Internet Gateway，然后流向互联网。或者，流量可以通过您的 VPN 或 Direct Connect 流向您的本地环境。

AMS 单账号 landing zone 共享服务

共享服务子网包含 AMS 目录服务、自动配置和常见任务的管理主机、防病毒 (TrendMicro) 管理服务器和内部堡垒主机：

- AMS 目录服务 = AD 域控制器

在 AMS 账户中创建 Active Directory，创建 AMS 域，在启动时将托管堆栈加入该域。

- 管理主机 = AMS 管理主机 (自动配置和常见任务)

充当 API 端点 Directory Service，用于修改和与 Directory Service 域控制器交互。

- 安全服务：防病毒 (TrendMicro) 管理服务器 = EPS DSM + EPS Relay

利用趋势科技™ 趋势科技趋势科技服务器深度安全防护系统软件 (DSM)，在客户端服务器模式下运行，并具有后端数据库，包括趋势科技服务器深度安全防护系统管理器、代理和中继。

- 内部堡垒主机 = 客户堡垒

特殊用途的服务器旨在作为互联网的主要接入点，并充当您的其他 Amazon EC2 实例的代理。

设置 AMS

主题

- [了解 AMS 的默认设置](#)
- [使用 AMS 控制台](#)
- [使用 AMS API 和 CLI](#)
- [AMS 自备 EPS](#)
- [接收 AMS 通知](#)
- [设置私有和公有 DNS](#)
- [AMS 出口流量管理](#)
- [在 AMS 高级版中部署 IAM 资源](#)
- [使用 IAM 角色和个人资料在 AMS 中设置权限](#)
- [AD FS 声明规则和 SAML 设置](#)
- [使用网络 ACL 进行限制](#)
- [Outposts 上的 AMS](#)
- [在 AMS 中使用标签](#)
- [AWS Managed Services 资源调度器](#)
- [AWS Systems Manager 在 AMS 高级版中](#)
- [离线 AMS 账户](#)

某些 AMS 设置任务可能会在入门时完成。

有关角色和职责（包括 AMS）的完整描述[支持的 AWS 服务](#)，请参阅[AMS 责任矩阵 \(RACI\)](#)。

Note

要请求 AMS 提供额外 AWS 服务，请提交服务请求。有关如何提出此请求的信息，请参阅[服务请求管理](#)。

了解 AMS 的默认设置

您的 AWS Managed Services (AMS) 网络采用标准化配置，大多数服务均采用默认配置。

本节介绍 AMS 用于访问、监控、记录 and 管理的默认设置。

有关多账户 landing zone 或单账户 landing zone 基础设施成本的示例，请参阅 [AMS 环境基本组件](#)

主题

- [DNS 解析默认值 \(MALZ\)](#)
- [EC2 IAM 实例配置文件](#)
- [来自 AMS 基线监测的警报](#)
- [默认日志保留和轮换](#)

DNS 解析默认值 (MALZ)

AWS Managed Services (AMS) 多账户着陆区：在 AWS 环境中，可以通过配置解析器转发规则来集成 VPC 中 Route 53 解析器和 DNS 解析器之间的域名系统 (DNS) 解析。在使用这些规则转发 DNS 查询之前，需要设置可以将这些查询转发到的入站和出站解析器终端节点。

默认情况下，AMS VPCs 中多账户设置中的应用程序账户内的 DNS 查询会转发到共享服务账户中存在的 AWS Directory for Microsoft Active Directory (也称为托管 AD) 域的条件转发器。AMS (可选) 允许您使用 AmazonProvided DNS；例如，使用 AmazonProvided DNS 将 DNS 查询转发到。这可以帮助您使用 VPC 终端节点，这些终端节点目前仅支持亚马逊通过 Amazon Route 53 提供的 DNS。相应地，还会自动为共享服务账户中默认部署的常见 VPC 终端节点设置解析器规则。有关这些常用 VPC 终端节点的更多信息，请参阅[AMS VPC 终端节点](#)。

要在您的所有应用程序账户中配置动态主机配置协议 (DHCP) 选项集 VPCs 以使用亚马逊提供的 DNS 用于 VPC 终端节点，并让 Route53 解析器规则指向共享服务账户中的通用 VPC 终端节点 (本地域有可选的解析器规则)，请创建管理 | 其他 | 其他 | 创建更改请求 (RFC)，指定共享服务账户，并请求启用应用程序账户 VPC 本地 DNS 和适用于 VPC 终端节点的 Route 53 解析器规则。

EC2 IAM 实例配置文件

实例配置文件是 IAM 角色的容器，您可以使用该容器在 EC2 实例启动时将角色信息传递给实例。

MALZ

有两个 AMS 默认实例配置文件 `customer-mc-ec2-instance-profile` 和 `customer-mc-ec2-instance-profile-s3`。这些实例配置文件提供下表中所述的权限。

政策描述

配置文件	策略
customer-mc-ec2-instance-profile	AmazonSSMManagedInstanceCore : 允许 Ec2 实例使用 SSM 代理。
	AMSInstanceProfileLoggingPolicy : 允许 Ec2 实例将日志推送到 S3 和 CloudWatch。
	AMSInstanceProfileManagementPolicy : 允许 Ec2 实例执行启动操作，例如加入 Active Directory。
	AMSInstanceProfileMonitoringPolicy : 允许 Ec2 实例向 AMS 监控服务报告调查结果。
	AMSInstanceProfilePatchPolicy : 允许 Ec2 实例接收补丁。
customer-mc-ec2-instance-profile-s3	AMSInstanceProfileBYOEPSPolicy : 允许 Ec2 实例使用 AMS 自带 EPS 。
	AMSInstanceProfileLoggingPolicy : 允许 Ec2 实例将日志推送到 S3 和 CloudWatch。
	AMSInstanceProfileManagementPolicy : 允许 Ec2 实例执行启动操作，例如加入 Active Directory。
	AMSInstanceProfileMonitoringPolicy : 允许 Ec2 实例向 AMS 监控服务报告调查结果。
	AMSInstanceProfilePatchPolicy : 允许 Ec2 实例接收补丁。
	AMSInstanceProfileS3WritePolicy : 允许 Ec2 实例 read/write 访问客户的 S3 存储桶。

SALZ

有一个 AMS 默认实例配置文件customer-mc-ec2-instance-profile，用于授予 IAM 实例策略中的权限customer_ec2_instance_profile_policy。此实例配置文件提供下表中所述的权限。该配置文件向在实例上运行的应用程序授予权限，而不是向登录实例的用户授予权限。

策略通常包含多个语句，其中每个语句授予对不同资源集的权限或在特定条件下授予权限。

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符（任意）。

EC2 默认 IAM 实例配置文件权限

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符（任意）。			
策略声明	效果	操作	描述和资源 (ARN)
亚马逊弹性计算云（亚马逊 EC2）			
EC2 消息操作	允许	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages, SendReply	允许在你的账户中执行 S EC2 ystems Manager 的消息传送操作。
Ec2 描述	允许	* (全部)	允许控制台显示您账户 EC2 中的配置详细信息。
我正在获取角色 ID	允许	GetRole	EC2 允许从aws:iam::*:role/ customer-* 和获取您的 IAM ID aws:iam::*:role/cu stomer_*。
上传日志事件的实例	允许	创建日志组	允许在以下位置创建日志：aws:logs::*:log-group:i-*

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符 (任意) 。			
策略声明	效果	操作	描述和资源 (ARN)
CW for MMS	允许	创建日志流	允许将日志流式传输到 : aws:logs:*:*:log-group:i-*
		DescribeAlarms, PutMetricAlarm, PutMetricData	CloudWatch 允许在您的账户中检索警报。 允许 CW 创建或更新警报并将其与指定指标关联。 允许 CW 向您的账户发布指标数据点。
Ec2 标签	允许	CreateTags, DescribeTags,	允许在您账户中的指定实例上添加、覆盖和描述标签。
明确拒绝 CW 日志	拒绝	DescribeLogStreams, FilterLogEvents, GetLogEvents	不允许列出、筛选或获取以下内容的日志流 : aws:logs:*:*:log-group:/mc/*
亚马逊 S EC2 imple Systems Manager (SSM)			
SSM 操作	允许	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	允许在您的账户中使用各种 SSM 功能。

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符 (任意) 。

策略声明	效果	操作	描述和资源 (ARN)
S3 中的 SSM 访问权限	允许	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadParts, ListBucketMultipartUploads	允许上的 SSM 获取和更新中的对象，中止向中多部分上传的多部分对象，并列出可供多部分上传的端口和存储桶。EC2 <code>aws:s3:::mc-*-internal-*/aws/ssm*</code>

亚马逊 EC2 简单存储服务 (S3) Simple Storage Service

在 S3 中获取对象	允许	获取 列表	允许 EC2 应用程序检索和列出您账户中 S3 存储桶中的对象。
客户加密日志 S3 访问权限	允许	PutObject	允许 EC2 应用程序更新中的对象 <code>aws:s3:::mc-*-logs-*/encrypted/app/*</code>
修补数据放置对象 S3	允许	PutObject	允许 EC2 应用程序将修补数据上传到您的 S3 存储桶，网址为 <code>aws:s3:::awsms-a*-patch-data-*</code>
将自己的日志上传到 S3	允许	PutObject	允许 EC2 应用程序将自定义日志上传到： <code>aws:s3:::mc-a*-logs-*/aws/instances/*/\${aws:userid}/*</code>

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符 (任意)。

策略声明	效果	操作	描述和资源 (ARN)
明确拒绝 MC 命名空间 S3 日志	拒绝	GetObject* 看跌*	不允许 EC2 应用程序从以下位置获取或放置任何对象： aws:s3:::mc-* -logs-*/encrypted/mc* , aws:s3:::mc-* -logs-*/mc/*, aws:s3:::mc-a* -logs-* -audit/*
明确拒绝 S3 删除	拒绝	* (全部)	不允许 EC2 应用程序对以下对象执行任何操作： aws:s3:::mc-a* -logs-*/* , aws:s3:::mc-a* -internal-*/* ,
明确拒绝 S3 CFN 存储桶	拒绝	Delete*	不允许 EC2 应用程序从以下位置删除任何对象：aws:s3:::cf-templates-*
明确拒绝列出存储桶 S3	拒绝	ListBucket	不允许您列出来自以下内容的任何加密、审核日志或保留 (mc) 对象：aws:s3:::mc-* -logs-*

AWS Secrets Manager 在亚马逊 EC2

顺时针 = CloudWatch。ARN = 亚马逊资源名称。* = 通配符 (任意) 。			
策略声明	效果	操作	描述和资源 (ARN)
趋势云一号秘密访问权限	允许	GetSecretValue	EC2 允许亚马逊访问 Trend Cloud One 迁移的机密： aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-tenant-id* , arn:aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-activation-token* , aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-tenant-id* , aws:secretsmanager::*:secret:/ams/eps/cloud-one-agent-tenant-guid*
AWS Key Management Service 在亚马逊 EC2			
Trend Cloud One 解密密钥	允许	Decrypt	EC2 允许亚马逊使用别名/-migration解 AWS KMS 密密钥 ams/eps/cloudone arn:aws:kms::*:alias/ams/eps/cloudone-migration

如果您不熟悉 Amazon IAM 政策，请参阅 [IAM 政策概述](#) 了解重要信息。

Note

策略通常包含多个语句，其中每个语句授予对不同资源集的权限或在特定条件下授予权限。

来自 AMS 基线监测的警报

了解 AMS 监控默认设置。有关更多信息，请参阅 [AMS 中的监控和事件管理](#)。

下表显示了监控的内容以及默认的警报阈值。在确定要进行哪些更改并订阅相关的 Amazon SNS 主题后，您可以使用管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC 更改提醒阈值。CloudWatch 有关创建和订阅主题的信息，请参阅[订阅主题](#)。有关一般信息，请参阅 [Amazon SNS FAQs](#)。除了 AMS 的标准警报流程外，要在警报超过阈值时直接收到通知，请按照以下有关如何覆盖警报配置的说明进行操作。[接收 AMS 生成的警报](#)

Amazon CloudWatch 提供了更长的指标保留期。有关更多信息，请参阅[CloudWatch 限制](#)。

Note

AMS 定期校准其基线监测。新账户始终使用最新的基准监控，该表描述了新加入账户的基准监控。AMS 会定期更新现有账户的基准监控，在更新到位之前，您可能会遇到一段时间延迟。有关更多信息，请参阅 [查看 AMS 账户的监控配置](#)。

Note

默认情况下，EC2 实例警报Non-root volume usage处于禁用状态。[如果您需要根据此警报生成警报，则必须使用 RFC Change Type ct-0erkoad6uyvvg 将其启用](#)

来自基线监控的警报

服务	安全警报	警报名称和触发条件	备注

对于已加星标的 (*) 警报，AMS 会主动评估影响并在可能的情况下进行补救；如果无法进行补救，AMS 就会造成事故。如果自动化无法纠正问题，AMS 会通知您事故案例，并让 AMS 工程师参与。此外，这些提醒可以直接发送到您的电子邮件中（如果您已选择加入 Direct-Customer-Alerts SNS 主题）。

服务	安全 警报	警报名称和触发条件	备注
Application Load Balancer (ALB) 实例	否	RejectedConnectionCount 总和 > 0，持续 1 分钟，连续 5 次。	CloudWatch 如果因为负载均衡器达到最大值而被拒绝的连接数就会发出警报。
Application Load Balancer (ALB) 目标	否	TargetConnectionErrorCount 总和 > 0，持续 1 分钟，连续 5 次。	CloudWatch 如果负载均衡器和注册实例之间未成功建立连接数，则发出警报。
亚马逊 EC2 实例 — Windows	否	SecureChannelFailure 在最后 15 个数据点中，有 10 个数据点大于 0.0。	CloudWatch 在 Windows 实例上发出警报，以便在安全通道连接失败时发出警报。
Aurora 实例	否	CPUUtilization 大于 85%，持续 5 分钟，连续 2 次。	CloudWatch 警报。
AWS Backup	是	DeleteRecoveryPoint 意外的 IAM 角色委托人或 IAM 用户委托人删除了 AWS Backup 恢复点。	CloudWatch 事件。删除备份恢复点时发出。
AWS Outposts	是	AMSOupostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% 持续 5 分钟，连续 12 次。	CloudWatch 对 AWS Outposts 资源的实例系列容量可用性发出警报。
		AMSOupostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% 持续 5 分钟，连续 12 次。	CloudWatch 对 AWS Outposts 资源的实例类型容量可用性发出警报。

服务	安全 警报	警报名称和触发条件	备注
EC2 实例-全 部 OSs	否	AMSOutpostsConnectedStatusC onnectedStatus < 1，持续 5 分钟，连续 1 次。	CloudWatch AWS Outposts 服务 链路连接时发出警报，少于 1 个 计数受损。
		AMSOutpostsCapacityExceptio nCapacityExceptions 0 表示 5 分钟，连续 1 次。	CloudWatch 为资源启动实例 时出现容量不足错误时 AWS Outposts发出警报 .
		CPUUtilization* 大于 95%，持续 5 分钟，连续 6 次。	CloudWatch 警报。CPU 利用 率高表明应用程序状态发生了变 化，例如死锁、无限循环、恶意 攻击和其他异常。
		StatusCheckFailed > 0，持续 5 分钟，连续 3 次。 根卷使用情况 大于 95%，持续 5 分钟，连续 6 次。	CloudWatch 警报。

服务	安全 警报	警报名称和触发条件	备注
亚马逊 EC2 实例-Linux		非 root 卷使用情况 大于 85%，持续 5 分钟，连续 2 次。 默认情况下处于禁用状态；有关更多信息，请参阅 https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info 。 内存可用 * MemoryFree 小于 5%，持续 5 分钟，连续 6 次。	
	是	EPS恶意软件 在实例中发现了恶意软件。	CloudWatch 事件。
	否	根卷索引节点使用情况 连续 6 次，5 分钟内平均值大于 95%。 免费交换 * 内存交换 < 5%，持续 5 分钟，连续 6 次。	CloudWatch 警报。仅适用于 Linux 实例。

服务	安全 警报	警报名称和触发条件	备注
ElastiCache 集群	否	CurrConnections = 65000	此警报通知 AMS ElastiCache 主机的最大连接限制。 CloudWatch 警报。如果您想更新此阈值，请联系 AMS 支持人员。
ElastiCache 节点	否	CPUUtilization 平均值 > 预定义值，持续 2 次，持续 15 分钟。	CloudWatch 警报。默认值为 90。如果是 Redis，则根据实例类型使用以下值之一： • cache.t1.micro : 90% • cache.m1.small : 90% • cache.m1.medium : 90% • cache.m1.large : 45% • cache.m1.xlarge : 22.5% • cache.m2.xlarge : 45% • cache.m2.4xlarge : 11.25% • cache.c1.xlarge : 11.25% • cache.t2.micro : 90% • cache.t2.small : 90% • cache.t2.medium : 45% • cache.m3.medium : 90% • cache.m3.large : 45% • cache.m3.xlarge : 22.5% • cache.m3.2xlarge : 11.25% • cache.r3.large : 45% • cache.r3.xlarge : 22.5% • cache.r3.2xlarge : 11.25% • cache.r3.4xlarge : 5.625% • cache.r3.8xlarge : 2.8125%

服务	安全 警报	警报名称和触发条件	备注
ElastiCache 节点-内存缓存	否	SwapUsage 连续 5 次，5 分钟内最大值大于 50,000,000 字节。	CloudWatch 警报。仅适用于内存缓存。
OpenSearch 集群	否	ClusterStatus.red 最大值为 >= 1，持续 1 分钟，连续 1 次。 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	CloudWatch 警报。至少有一个主分片其及副本未分配给节点。要了解更多信息，请参阅 Red Cluster 状态 。
OpenSearch 域	否	KMSKey错误 >= 1 持续 1 分钟，连续 1 次。	CloudWatch 警报。用于在您的域中加密静态数据的 KMS 加密密钥已禁用。重新启用它可恢复正常操作。要了解更多信息，请参阅 OpenSearch 服务服务的静态数据加密 。
		ClusterStatus. 黄色 最大值为 >= 1，持续 1 分钟，连续 1 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	至少有一个副本分片未分配给节点。要了解更多信息，请参阅 黄色群集状态 。
		FreeStorageSpace 最小值为 <= 20480，持续 1 分钟，连续 1 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	您的集群中的节点已降至 20GiB 的可用存储空间。要了解更多信息，请参阅 可用存储空间不足 。

服务	安全 警报	警报名称和触发条件	备注
		ClusterIndexWritesBlocked ≥ 1 持续 5 分钟，连续 1 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	集群正在阻止写入请求。要了解更多信息，请参阅 ClusterBlockException。
		节点 最小值为 $< x$，持续 1 天 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	x 是您的集群中的节点数。此警报表示您的群集中至少有一个节点无法访问的时间已达到一天。要了解更多信息，请参阅集群节点故障。
		CPUUtilization 连续 3 次，15 分钟内平均值大于 80% 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	100% 的 CPU 利用率很常见，但是持续的高平均利用率是有问题的。考虑使用更大的实例类型或添加实例。
		JVMMemory压力 最大值为 $\geq 80\%$，持续 5 分钟，连续 3 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	如果使用量增加，群集可能会遇到内存不足错误。请考虑垂直扩展。Amazon ES 将实例内存的一半用于 Java 堆，堆大小不超过 32 GiB。您最多可以将实例的 RAM 垂直扩展至 64GiB，此时可以通过添加实例水平扩展。
		大师 CPUUtilization 15 分钟内平均值大于 50%，连续 3 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	考虑为您的专用主节点使用更大的实例类型。由于专用主节点在集群稳定性和blue/green 部署中的作用，因此其平均 CPU 使用率应低于数据节点。

服务	安全 警报	警报名称和触发条件	备注
		主JVMMemory压力 最大 >= 80%，持续 15 分钟，连续 1 次 触发此警报后，AMS 会采取积极措施以减少对运营的影响。	考虑为您的 专用主节点 使用更大的实例类型。由于专用主节点在集群稳定性和 blue/green 部署 中的作用，因此其平均 CPU 使用率应低于数据节点。
OpenSearch 实例	否	AutomatedSnapshotFailure 最大值为 >= 1，持续 1 分钟，连续 1 次。	CloudWatch 警报。自动快照失败。此故障通常由红色群集运行状况导致。参见 红色集群状态 。
		SurgeQueueLength 大于 100，持续 1 分钟，连续 15 次。	CloudWatch 如果有多余的请求等待路由，则发出警报。
Elastic Load Balancing	否	HTTPCode_elb_5xx_count 总和 > 0，持续 5 分钟，连续 3 次。	CloudWatch 如果来自负载均衡器的 HTTP 5XX 响应代码数量过多，则发出警报。
		SpilloverCount > 1，持续 1 分钟，连续 15 次。	CloudWatch 如果由于激增队列已满而被拒绝的请求数量过多，则发出警报。
GuardDuty 服务	是	不适用；所有发现（威胁目的）都受到监控。每个发现都对应一个警报。 GuardDuty 调查结果的变化。这些变化包括新生成的发现或后续出现的现有发现。	支持的 GuardDuty 查找类型列表位于“ GuardDuty 活动查找类型 ”上。

服务	安全 警报	警报名称和触发条件	备注
Health	变化	AWS Health Dashboard	与 AMS 支持的基准服务相关的 AWS Health Dashboard (AWS Health) 事件状态发生变化时，系统会发送通知。有关更多信息，请参阅 支持的服务 。
AWS Managed Microsoft AD	否	活动目录状态 AWS Managed Microsoft AD 实例发送活动状态事件。	服务事件。在事件发生后目录正常运行时发出。
		受损的目录状态 AWS Managed Microsoft AD 实例发送受损的目录状态事件。	服务事件。当目录以降级状态运行时发出。检测到一个或多个问题，可能有的目录操作未在完全有效地工作。
		无法操作的目录状态 AWS Managed Microsoft AD 实例发送无法操作的状态事件。	服务事件。当目录不起作用时发出。所有目录终端节点都报告有问题。
		正在删除目录状态 AWS Managed Microsoft AD 实例发送删除目录状态事件。	服务事件。当前正在删除目录时发出。
		失败的目录状态 AWS Managed Microsoft AD 实例发送失败状态事件。	服务事件。无法创建目录时发出。
		RestoreFailed 目录状态 AWS Managed Microsoft AD 实例发送恢复失败的目录状态事件。	服务事件。从快照恢复目录失败时发出。

服务	安全 警报	警报名称和触发条件	备注
亚马逊 RDS 实例	否	当为数据库实例分配的存储空间用完时，将触发存储空间不足警报。	RDS-EVENT-0007，详情请参阅 使用亚马逊 RDS 事件通知 。
		数据库实例失败 由于某个不兼容配置或底层存储问题，数据库实例已失败。从 point-in-time-restore数据库实例开始。	服务事件。RDS-EVENT-003 1、 Amazon RDS 事件类别和事件消息 。
		未尝试故障切换 Amazon RDS 不会因为数据库实例上最近出现故障转移而尝试请求故障转移。	服务事件。RDS-EVENT-003 4、 Amazon RDS 事件类别和事件消息 。
		数据库实例参数无效 例如，由于该实例类的内存相关参数设置得太高，MySQL 无法启动，因此客户需要修改内存参数并重启数据库实例。	服务事件。RDS-EVENT-003 5、 Amazon RDS 事件类别和事件消息 。
		子网 IDs 数据库实例无效 数据库实例处于不兼容的网络中。某些指定的子网 IDs 无效或不存在。	服务事件。RDS-EVENT-003 6、 Amazon RDS 事件类别和事件消息 。
		数据库实例只读副本错误 在读取复制过程中出错。有关详细信息，请参阅事件消息。有关排查只读副本错误的信息，请参阅 MySQL 只读副本问题疑难解答 。	服务事件。RDS-EVENT-004 5、 Amazon RDS 事件类别和事件消息 。
		数据库实例读取复制已结束 只读副本上的复制已结束。	服务事件。RDS-EVENT-005 7、 Amazon RDS 事件类别和事件消息 。

服务	安全 警报	警报名称和触发条件	备注
		创建 statspack 用户账户时出错 创建 Statspack 用户账户 PERFSTAT 时出错。在添加 Statspack 选项之前，请先删除账 户。	服务事件。RDS-EVENT-005 8、 Amazon RDS 事件类别和事件消息 。
		数据库实例恢复开始 SQL Server 数据库实例正在重新建立其镜像。在镜像重新建立之前，性能将下降。发现具有非 FULL 恢复模式的数据库。恢复模式已更改回完整模式并开始镜像恢复。(<dbname>: <recovery model found>[,...])。	服务事件。RDS-EVENT-006 6、 Amazon RDS 事件类别和事件消息 。
		数据库群集的故障转移已失败。	RDS-EVENT-0069，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		权限恢复无效 S3 存储桶 用于访问您的 Amazon S3 存储桶以执行 SQL Server 本机备份和恢复的 IAM 角色配置不正确。有关更多信息，请参阅 设置本机 Backup 和还原 。	服务事件。RDS-EVENT-008 1、 Amazon RDS 事件类别和事件消息 。
		Aurora 无法从 Amazon S3 存储桶复制备份数据。	RDS-EVENT-0082，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		当数据库实例消耗了其分配的存储空间 的 90% 以上时，会发出存储空间 不足警报	RDS-EVENT-0089，请在 Amazon RDS 事件类别和事件消息 中查看详情。

服务	安全 警报	警报名称和触发条件	备注
		Aurora 无服务器数据库集群扩展失败时的通知服务。	RDS-EVENT-0143，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		数据库实例处于无效状态。无需采取操作。弹性伸缩稍后将重试。	RDS-EVENT-0219，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		数据库实例已达到存储已满阈值，并且数据库已关闭。	RDS-EVENT-0221，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		此事件表示 RDS 实例存储无法自动扩展，自动扩缩失败的原因可能有多种。	RDS-EVENT-0223，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		存储弹性伸缩已触发待处理的扩展存储任务，该任务将达到最大存储阈值。	RDS-EVENT-0224，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		数据库实例的存储类型目前在可用区中不可用。弹性伸缩稍后将重试。	RDS-EVENT-0237，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		RDS 无法为代理预调配容量，因为您的子网中没有足够的 IP 地址可用。	RDS-EVENT-0243，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		您的 AWS 账户的存储空间已超过允许的存储配额。	RDS-EVENT-0254，请在 Amazon RDS 事件类别和事件消息 中查看详情。
		CPUUtilization 连续 2 次，15 分钟内 CPU 平均利用率大于 90%。	CloudWatch 警报。

服务	安全 警报	警报名称和触发条件	备注
		DiskQueueDepth 总和大于 75，持续 1 分钟，连续 15 次。	
		FreeStorageSpace 连续 2 次，5 分钟内平均值小于 1,073,741,824 字节。	
		SwapUsage 连续 2 次，5 分钟内平均值 >= 104,857,600 字节。	
Amazon Redshift 集群	否	RedshiftClusterStatus 未处于维护模式时集群的生命值 < 1，持续 5 分钟。	1 表示集群运行状况良好。
Amazon Macie	是	新生成的警报和对现有警报的更新。 Macie 发现调查结果有任何变化。这些变化包括新生成的发现或后续出现的现有发现。	亚马逊 Macie 提醒。有关支持的 Macie 警报类型的列表，请参阅 分析亚马逊 Macie 调查结果 。请注意，并非所有账户都启用 Macie。

触发此警报后，AMS 会采取主动行动（扩展集群）。

有关补救工作的信息，请参阅[AMS 自动修复警报](#)。

[观看安德鲁的视频以了解更多信息 \(7:03\)](#)

默认日志保留和轮换

本节介绍 AMS 日志管理默认值；有关更多信息，请参阅[日志管理](#)。

- 轮换 = 实例内部的日志周转

- 保留期 = 我们在亚马逊日志和亚马逊简单存储服务 (S3) Simple Service 中保存 CloudWatch 日志的时间段

日志会根据需要保留在 CloudWatch 日志中（您可以对此进行配置），并保留在 S3 中。它们不会过期或被删除，并且受服务持久性的限制。有关 S3 持久性的详细信息，请参阅 [Amazon S3 中的数据保护](#)。

您可以请求更改所有日志的日志保留期，但 AWS CloudTrail 日志除外，出于审计和安全考虑，这些日志会无限期保存。

日志轮换是在实例内部配置的。默认情况下，如果操作系统和安全日志的容量超过 100MB，则每小时轮换一次，这样做是为了确保您在实例中不会出现磁盘不足的情况。

实例内部的日志代理将在线日志上传到 Amazon CloudWatch Logs，日志从那里存档到 S3。

日志以生成的原始格式存储在 CloudWatch Logs 和 S3 中，没有预处理。

使用 AMS 控制台

AWS 管理控制台中的 AMS 控制台可供您与 AMS 交互并操作您的 AMS Advanced 管理资源和 AMS Accelerate 资源。AMS 控制台的行为通常与任何 AWS 主机类似；但是，由于 AMS 是私人组织，因此只有启用 AMS 的账户才能访问控制台。在您的账户中启用 AMS 后，您可以通过在统一搜索栏中搜索“Managed Services”来访问控制台。

Note

根据您的账户角色，您可以访问 AMS 高级控制台或 AMS Accelerate 控制台。

使用 AMS 主机时，请注意以下注意事项：

- AMS 控制台是特定于账户的。因此，如果您使用的是组织的“测试”帐户，则无法在该组织的“Prod”帐户中查看资源。同样，您必须拥有 AMS 高级角色才能访问 AMS 高级控制台。
- 在您进行身份验证时，AMS 控制台会应用 IAM 策略，该策略决定了您可以访问哪个控制台以及可以在那里做什么。您的管理员可以对默认 AMS 策略应用其他策略，以限制您在控制台中可以看到和执行的的操作。

AMS 高级控制台具有以下功能：

- 打开页面：开头页面包含信息框和链接，便于您访问现有信息 RFCs、事件、服务请求和报告。
- 专题页面，左侧导航窗格中的链接：
 - 控制面板：概述您的账户当前状态，包括：
 - 更改请求：查看 RFCs 有多少人正在等待您的回复，然后跳转到该过滤器处于活动状态的 RFC 列表页面。查看 RFCs 有多少人正在等待您的批准，然后跳转到该筛选器处于活动状态的 RFC 列表页面。查看 RFCs 有多少处于打开状态，然后跳转到该过滤器处于活动状态的 RFC 列表页面。单击“查看全部”链接打开列表页面。RFCs
 - 事件：查看有多少事件案例正在等待您的回复，然后在过滤器处于活动状态的情况下跳转到事件列表页面。查看以及有多少已打开，然后在过滤器处于活动状态的情况下跳转到事件列表页面。单击“查看全部”链接，打开事件列表页面。
 - 服务请求：查看有多少服务请求正在等待您的响应，然后跳转到该过滤器处于活动状态的服务请求列表页面。查看以及有多少已打开，然后跳转到该过滤器处于活动状态的服务请求列表页面。单击“查看全部”链接，打开服务请求列表页面。
 - 最近更新 RFCs：日期、RFC 详情链接和状态
 - 最近创建的事件和服务请求：日期、案例详情链接和类型（事件或服务请求）
- RFCs: 打开账户现有账户 RFCs 的列表
- 事件：打开账户的未解决事件列表
- 服务请求：打开账户的未处理服务请求列表
- 报告：打开“报告”页面和默认报告、“每日备份”、“每日补丁”和“每月账单”
- 资源：
 - VPCs: 打开账户现有账户 VPCs 的列表
 - 堆栈：打开账户现有堆栈列表
 - AMIs: 打开可用 AMS 列表 AMIs
- 功能聚焦：有关主机最新更新的信息
- 开发者资源：一页可下载文件，包括 AMS Advanced 变更管理 SDK 等
- 文档：AWS Managed Services 文档登录页面

使用 AMS API 和 CLI

AWS Managed Services (AMS) API 与其他 AWS 服务类似。APIs 您可以在 AMS API [参考中阅读有关 AMS API](#) 的信息。

用于 REST 调用的 AMS API HTTP

除此之外 SDKs，AMS 还提供 CLI；您还可以针对 AMS 端点调用 REST API 调用。

有两个 AMS APIs（两者的终端节点都位于 us-east-1 中）：

- 变更管理：使用此 API 请求访问或更改您的基础架构，包括创建和更新 RFCs、部署新实例、更新和删除实例、获取相关信息以及创建 AMIs。CTsHTTP 终端节点是：

`https://amscm.us-east-1.amazonaws.com`

- SKMS：使用此 API 获取有关您的基础架构的信息，包括 VPCs 堆栈、子网和。AMIsHTTP 终端节点是：

`https://amsskms.us-east-1.amazonaws.com`

安装或升级 AMS CLI

AMS CLI 是一种与 AMS API 交互的简便方法，本节的示例中使用了该工具。有关 AWS CLI 和 AMS CLI 的使用惯例，请参阅[使用 AWS 命令行界面](#)。

有关安装 SAML 的信息，请参阅[AD FS 声明规则和 SAML 设置](#)。

要安装或升级 AMS CLI，请按照以下说明进行操作：

Note

您必须具有管理员凭据才能执行此过程。

AWS CLI 是使用 AWS Managed Services (AMS) CLIs（变更管理和 SKMS）的先决条件。

1. 要安装 AWS CLI，请参阅[安装 AWS 命令行界面](#)，然后按照相应的说明进行操作。请注意，该页面底部有使用不同安装程序（[Linux](#)、[MS Windows](#)、[mac OS](#)、[虚拟环境](#)、[捆绑安装程序（Linux、macOS 或 Unix）](#)）的说明。

安装完成后，运行 `aws help` 以验证安装。

2. 安装 AWS CLI 后，要安装或升级 AMS CLI，请下载 AMS CLI 或 AMS SDK 可分发文件 zip 文件并解压缩。您可以通过 AMS 控制台左侧导航栏中的[开发者资源](#)链接访问 AMS CLI 发行版。
3. README 文件提供了任何安装的说明。

打开任一选项：

- CLI zip：仅提供 AMS CLI。
- 软件开发工具包压缩包：提供所有 AMS APIs 和 AMS CLI。

对于 Windows，请运行相应的安装程序（仅限 32 位或 64 位系统）：

- 32 位：ManagedCloudAPI_x86.msi
- 64 位：ManagedCloudAPI_x64.msi

对于 Mac/Linux，请运行以下命令运行名为:AWSManagedServices_InstallCLI.sh 的文件：。sh AWSManagedServices_InstallCLI.sh 请注意，amscm 和 amsskms 目录及其内容必须与.sh 文件位于同一个目录中。AWSManagedServices_InstallCLI

4. 如果您的公司证书是通过与 AWS 的联合身份验证（AMS 默认配置）使用的，则必须安装可以访问您的联合身份验证服务的凭证管理工具。例如，您可以使用此 AWS 安全博客[如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问](#)来帮助配置您的凭证管理工具。
5. 安装完成后，运行aws amscm helpaws amsskms help并查看命令和选项。

Note

必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用户指南》中的“AMS 信息资源”部分。您可能需要添加身份验证--profile选项；例如，aws amsskms *ams-cli-command* --profile SAML。您可能还需要添加该--region选项，因为所有 AMS 命令都将使用 us-east-1；例如。aws amscm *ams-cli-command* --region=us-east-1

在 CLI、Ruby、Python 和 Java 中使用 AMS API

以下是 AMS API ListChangeTypeClassificationSummaries 操作的所有可用语言的代码片段列表。

有关 Python、Ruby 和 Java SDKs 的信息，[请参阅亚马逊 Web Services 工具](#)，然后向下滚动到该 SDKs 部分。每个 SDK 安装程序都包含一个带有其他代码片段的自述文件。

AMS API 到 CLI 示例

安装 AMS CLI (需要 CL AWS I; 请参阅[安装或升级 AMS CLI](#)) 后, 您可以运行任何 AMS API 操作, 方法是重新调整调用, 指定哪个 AMS API `aws amscm` 或 `aws amsskms`, 然后使用连字符代替驼峰大小写。最后, 提供证书, 例如 SAML。

要了解更多信息, 请参阅[使用 AWS 命令行界面](#)。

示例:

- API: `'ChangeTypeClassificationSummaries[].
[Category,Subcategory,Item,Operation,ChangeTypeId]'`
- CLI: `amscm list-change-type-classification-summaries
--query "ChangeTypeClassificationSummaries[*].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

Note

如果您使用 SAML 进行身份验证, 请 `aws --profile saml` 添加到命令的开头。例如,

```
aws --profile saml amscm list-change-type-classification-  
summaries --query "ChangeTypeClassificationSummaries[*].  
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

AMS API 到 Python 示例

要在 Python 中使用 AMS API, 请安装 AMS CLI 并安装 boto3。按照以下步骤进行操作:

1. 安装 AMS CLI。请参阅[安装或升级 AMS CLI](#)。
2. 安装适用于 Python 的 AWS 软件开发工具包 boto3。欲了解更多信息, 请参阅这篇博客文章[现已推出 — 适用于 Python 的 AWS SDK \(Boto3\)](#)。

```
import boto3
```

3. 获取 AMS 变更管理客户端:

```
cm = boto3.client('amscm')
```

4. 获取 AMS CTs:


```
cts = cm.list_change_type_classification_summaries()

print(cts)
```

Python 示例

以下是一些在 AMS 中使用 Python、要创建 EC2 实例、 and/or 使用 Lambda 的示例。

创建一个 Python 示例 EC2

此示例展示了如何在 Python 代码中使用 amscm RESTFul API 来归档和执行 RFC 流程。

1. 将 AMS CLI 安装在您可以访问的地方；您需要它提供的文件。
2. 调用 Python 库并创建 EC2 实例：

```
import boto3
import json
import time

# Create the amscm client
cm = boto3.client('amscm')

# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)
```

```
# Extract the RFC ID from the response
NewRfcID = cts['RfcId']

# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
    if RFC_Status_Code == "PendingApproval":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "InProgress":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "Failure":
        print(RFC_Status_Code)
        break
    else:
        print(RFC_Status_Code)

RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

使用 Lambda 的 Python 示例

此示例说明如何将 AMS 模型与您的代码捆绑在一起，以便您可以将其与 Lambda 一起使用，或者 EC2; 您不会或无法安装的地方。amsccli

Note

AMS 不提供可导入的 AMS 专用的 Python SDK。amsccli 安装脚本在 CLI 的正常路径中安装 AMS 服务数据模型。对于 CLI 的使用和系统 Python 的使用，这没问题，因为两者都从相同的默认位置 boto3 读取它们的服务模型（~/.aws/models）。但是，当您想在 Lambda（或任何其他非本地运行时）中通过 boto3 使用 AMS 服务时，它会中断，因为您不再拥有数据模型。以下是通过将数据模型与函数打包来解决此问题的方法。

您可以采取一些简单的步骤在 Lambda 或其他运行时（例如 EC2 Fargate 等）中运行集成了 AMS 的 Python 代码。以下工作流程显示了集成 AMS 的 Lambda 函数所需的步骤。

通过将数据模型添加到代码的部署包并更新 SDK 搜索路径，您可以模拟 SDK 体验。

Important

此示例和显示的所有非 python 命令均在 Mac 计算机上进行了测试。

工作流程示例：

1. 安装 `amsccli`。这将在您的计算机 (Mac) `~/ .aws/models` 上创建一个文件夹。
2. 将模型复制到本地目录：`cp ~/ .aws/models ./models`。
3. 将模型包含在代码的部署包中。
4. 更新您的函数代码，将新模型添加到 SDK 路径中。请注意，此代码必须在导入 `boto3` 或 `botocore` 之前运行！

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

由于示例模型位于名为的目录中 `models`，因此我们添加 `./models` 到 `AWS_DATA_PATH`。如果目录已命名 `/ams/boto3models`，我们将添加以下代码：

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

您的代码应该可以成功找到 AMS 模型。以下是关于：打包的更具体的示例，以下是 Lambda 的特定工作流程。

AMS Lambda 工作流程示例：

这些步骤将前面的通用示例应用于创建 AWS Lambda 函数。

1. 安装 amscli。这将在您的计算机 (Mac) `~/ .aws/models` 上创建一个文件夹。
2. 将模型复制到本地目录：

```
cp ~/.aws/models ./models
```

3. 将模型添加到函数的部署 zip 文件中：

```
zip -r9 function.zip ./models
```

Important

更新您的函数代码，将新模型添加到 SDK 路径中。请注意，此代码必须在导入 boto3 或 botocore 之前运行！

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

因为示例模型位于名为的目录中models，所以我们添加./models到 AWS_DATA_PATH。如果目录已命名/ams/boto3models，我们将添加以下代码：

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

现在，部署你的函数：

1. 将您的函数代码添加到部署 zip 文件中（如果您尚未这样做）：

```
zip -g function.zip lambda-amscm-test.py
```

2. 使用您创建的 zip 文件（控制台或 CLI）创建或更新您的函数：

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://function.zip --region us-east-1
```

你的 AMS 集成的 Python Lambda 现在应该可以工作了。

Note

您的函数必须具有 IAM 权限，amscm 否则会出现权限错误。

用于测试 amscm 的 Lambda 函数代码示例（.py 的内容）：lambda-amscm-test

```
import json

# Force lambda to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore

def lambda_handler(event, context):
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
        cts = cm.list_change_type_categories()
        print(cts)
    except botocore.exceptions.UnknownServiceError:
        print("amscm not found")

    return {
        'statusCode': 200,
```

```
'body': json.dumps('Hello from Lambda!')
}
```

测试输出 (成功) :

函数响应 :

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}
```

Request ID:
"1cea13c0-ed46-43b1-b102-a8ea28529c27"

函数日志 :

```
START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: $LATEST
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',
  'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-
bcc2-10cf0aa19ece', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid':
  'e27276a0-e081-408d-bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1',
  'content-length': '89', 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

Ruby 的 AMS API 示例

要在 Ruby 中使用 AMS API , 请安装 Rub AWS y SDK 和 AMS CLI。按照以下步骤进行操作 :

1. 安装 AMS CLI。请参阅[安装或升级 AMS CLI](#)。
2. 安装 AWS Ruby 开发工具包。参见 [Amazon Web Services 工具](#)。
3. 使用以下命令配置 Ruby :

```
require 'aws-sdk'

config = {

  region: 'us-east-1',

  credentials: Aws::Credentials.new('ACCESS_KEY', 'SECRET_KEY')}
```

4. 获取 AMS CTs :

```
ams_cm = Aws::amscm::Client.new(config)

cts = ams_cm.list_change_type_classification_summaries

print(cts)
```

AMS API 转 Java 示例

要在 Java 中使用 AMS API，请安装 Jav AWS a SDK 和 AMS CLI。按照以下步骤进行操作：

1. 安装 AMS CLI。请参阅[安装或升级 AMS CLI](#)。
2. 安装 AWS Java 开发工具包。参见 [Amazon Web Services 工具](#)。
3. 使用以下命令配置 Java：

```
import com.amazonaws.auth.BasicAWSCredentials;

import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesReque

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResul

public static void getChangeTypeClassificationSummaries() {
```

4. 设置凭证。我们建议您不要对此进行硬编码。

```
final BasicAWSCredentials awsCredsCm =

    new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. 创建 AMS 变更管理客户端：

```
final AWSManagedServicesCMClient cmClient =

    new AWSManagedServicesCMClient(awsCredsCm);
```

6. 获取 AMS CTs：

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();
```

```
final ListChangeTypeClassificationSummariesResult listCtsResult =
cmClient.listChangeTypeClassificationSummaries(listCtsRequest);

System.out.println("List of CTs");

listCtsResult.getChangeTypeClassificationSummaries().stream()

.map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" +
x.getItem() + "/" + x.getOperation())

.forEach(System.out::println);

}
```

AMS 自备 EPS

使用 AMS “自带端点安全” (BYOEPS) 功能，将默认的趋势科技趋势科技服务器深度安全防护系统代理替换为您自己的端点安全解决方案或趋势科技许可证。如果您已经拥有除趋势科技趋势科技趋势科技趋势科技服务器深度安全防护系统以外的产品的经济实惠的许可证，或者您想使用特定的 EPS 工具，则在您的实例中使用 BYOEPS。

BYOEPS 在账户层面起作用。您在账户中的实例要么使用 BYOEPS，要么使用 AMS 管理的默认 EPS：

- 多账户 landing zone (MALZ)：您可以指定使用 BYOEPS 或托管 EPS 的应用程序账户。
- 单账户着陆区 (SALZ)：您的 AMS 账户使用 BYOEPS 或托管 EPS。

BYOEPS，通过趋势科技趋势科技服务器深度安全防护系统的成本来减少 AWS 账单。您仍需要支付 EPS 费用，因为仍然需要 AMS 管理的 EPS 来保护 AMS 创建和维护的访问管理所需的 EC2 实例（堡垒和管理主机）。要计算总成本影响，您必须考虑新工具的许可证成本以及按所需服务级别管理 EPS 的成本。

BYOEPS 的使用会改变 AMS 在安全管理方面的角色和职责：

- R 代表负责任的一方，负责完成任务。
- C 代表咨询；征求意见的当事方，通常是作为主题专家征求意见的当事方；并与之进行双边沟通。
- 我代表知情；一个通报进展情况的当事方，通常只有在任务或可交付成果完成后才会被告知。

安全管理	Customer	AWS 托管服务
保持 AMS 共享服务 EC2 实例的托管 EPS 的有效许可证	R	C
为 AMS 共享服务 EC2 实例配置托管 EPS	我	R
更新 AMS 共享服务 EC2 实例的托管 EPS	我	R
监控 AMS 共享服务 EC2 实例上的恶意软件	我	R
维护和更新 AMS 共享服务 EC2 实例的病毒签名	我	R
修复 AMS 共享服务实例中感染恶意软件的 EC2 实例	C	R

当你使用 BYOEPS 时，你会丢失 AMS 提供的其中一个安全控制措施。您仍然可以通过诸如亚马逊 GuardDuty、Amazon Macie 之类的工具以及诸如审查 IAM 配置之类的流程控制来提供安全管理。使用 BYOEPS 不会影响 AMS 合规性认证和认证。但是，许多安全框架和认证都要求防范恶意软件和恶意代码。为了帮助确保您的账户安全和合规，请评估您计划的控制措施，以确保它们符合工作负载合规性认证的安全要求。

为你的账户开启 BYOEPS

开启 BYOEPS 的过程包含三个阶段，并使用多个阶段。RFCs 查看以下信息，了解开启 BYOEPS 所需的三个阶段。然后，与您的 CSDM 协调，为您的账户启用 BYOEPS。

主题

- [第 1 阶段：先决条件](#)
- [第 2 阶段：在您的账户中启用 BYOEPS](#)
- [第 3 阶段：实例迁移](#)

第 1 阶段：先决条件

- 默认的 Amazon EC2 实例配置文件是 `customer-mc-ec2-instance-profile`。如果您除了默认配置文件之外还使用其他的 Amazon EC2 实例配置文件，则允许对您的 EC2 实例配置文件执行 `/ams/end-point-security` 资源 `ssm:GetParameter` 操作。

如果您无法更新 EC2 实例配置文件，请提交一份指定您需要更新的实例配置文件的 RFC。

- 了解此次变更的范围。

通过 AMS 自动更改类型 (CT) 进行部署允许您指定创建时使用的 AMI。

要对使用 AMS 管理的 EPS 的账户使用 BYOEPS，您必须与 AMS 合作从这些 EC2 实例中卸载趋势科技代理，并更新这些实例上的 AMS 代码（例如启动脚本）。这些操作可能需要重新启动，因此最佳做法是将这些操作作为维护时段的一部分来执行。请联系您的 CSDM，确定执行此活动的维护时段，并制定迁移计划。对于迁移计划，请考虑以下问题：

1. 您需要迁移多少实例？将实例总数分成较小的增量批次。
 2. 您将如何分批划分实例？例如，您可以按资源组划分，然后创建一个列表以与 AMS 运营团队共享。
 3. 每批需要多长时间？总共需要多少时间？考虑一下，您可能需要在同一个维护时段内安装首选的 EPS 工具。这需要多长时间？
- 您的 CSDM 与 AMS 运营团队共享迁移计划。如果您的实例队列大于 50，请与您的 CSDM 合作，使用计划事件管理 (PEM) 流程创建计划事件。有关更多信息，请参阅 [AWS Managed Services 中的计划活动管理](#)。

AMS Operations 会与您的 CSDM 进行协调，并根据您账户 RFCs 中的实例数量，建议如何根据您的维护时段进行提交。

- 使用自定义或 AMS 更新 EC2 实例启动自动化或流程，AMIs 以使用 2020 年 12 月之后 AMIs 发布的 AMS。

第 2 阶段：在您的账户中启用 BYOEPS

当您在账户中使用 BYOEPS 时，AMS 对安全管理责任会发生变化。启用 BYOEPS 之前，请咨询您的安全和云平台团队。

要为您的账户申请 BYOEPS，请使用 `ct-0xdawir96cy7k` 提交“MOO”更新 RFC（管理 | 其他 | 其他 | 更新），详细信息如下：

Please enable BYOEPS for this account/these accounts
Account IDs: *IDs for the accounts for BYOEPS.*

AMS 将参数存储更新部署到账户并更新 [EC2 Amazon IAM 实例配置文件](#)。

Note

- 启动新实例且使用最新 AMS 的账户 AMIs 可以跳过趋势科技代理的安装。AMIs 2020 年 12 月之前的版本不支持 BYOEPS 功能。更新使用旧版本的自动化，AMIs 以使用支持 BYOEPS AMIs 功能的最新 AMS。
- 有关现有 EC2 实例处理的信息，请参阅第 3 阶段：实例迁移

第 3 阶段：实例迁移

根据您的用例，使用以下选项之一来迁移您的实例。如果您不确定要选择哪个选项，请联系您的 CA 或 CSDM。

拥有使用 AMS EC2 管理的 EPS 的实例的账户

在维护时段内，为了与第 1 阶段的计划保持一致，将对需要载入 BYOEPS 的每个实例执行以下操作：

- 由 AMS 执行：将 AMS 代码（启动脚本、模块等）更新到最新版本。这是必需的，因为旧的 AMS 启动脚本不支持 BYOEPS 功能，并且每次启动时都要重新安装趋势科技代理。另外，请卸载趋势科技代理。
- 由您执行：安装和配置您的首选 EPS 工具。

Important

趋势科技代理提供恶意软件防护。请务必安装适当的替代品以保护您的实例。

要进行这些更改，请分批提交 RFCs `ct-2iz9nvw8zlhst`，[趋势科技 DSM | 移除趋势科技](#) EPS 代理（需要审阅）。

没有使用 AMS EC2 管理的 EPS 的实例的账户

启动新实例且使用最新 AMS 的账户 AMIs 可以跳过趋势科技代理的安装。AMIs 2020 年 12 月之前的版本不支持 BYOEPS 功能。更新使用旧版本的自动化，AMIs 以使用支持 BYOEPS AMIs 功能的最新 AMS。

在 EC2 实例上添加您的代理

您可以使用 AMS 模式部署工具代理，例如 CrowdStrike 或 Qualys，提交服务请求以寻求帮助。

接收 AMS 通知

您和 AMS 之间进行通信的原因有很多：

- 由 AMS 创建的 RFC，需要您的批准
- 为调查您创建的失败的 RFC 而创建的 AMS 案例
- 通过监控警报创建的事件
- 修补服务通知，通知你即将进行的修补
- 服务请求和事件报告
- 每月的 CRM 报告
- 不定期发布重要的 AWS 公告（如果需要您采取任何行动，您的 CSDM 会与您联系）

所有这些通知都将发送到您在入职时向 AMS 提供的默认联系信息（root 账户电子邮件）。由于很难保持单个电子邮件的更新，因此我们建议您使用可以随时更新的群组电子邮件。AMS 运营部门还会收到发送给您的所有通知，并在做出回复之前对其进行分析。

AMS 通知服务提供了另外两种设置通知联系人的方法：

- 使用联系人标签（标签键值为联系信息）标记您的资源，并将标签密钥名称提供给您的 CSDM。除了在入职时创建的账户联系人外，还将向密钥值中提供的联系人发送有关这些资源的警报。这对于应用程序所有者特别有用。有关更多信息，请参阅 [基于标签的警报通知](#)。
- （入职时必填）将非基于资源的 notification 发送到您的 CSDM 指定联系人列表。例如，您可能有一个名为“SecurityContacts”的列表和另一个名为 OperationsContacts 的列表，依此类推。AMS 会将列表添加到通知服务，适用于该列表上下文的警报会发送给这些联系人。这对于组织事项特别有用。

此高级警报路由功能适用于大多数基本 CloudWatch 警报，例如亚马逊 EC2 实例故障、Amazon Elastic Block Store (Amazon EBS) Elastic Block Store 卷容量利用率-根使用率、亚马逊 NonRoot EBS 使用率、高内存利用率、高交换使用率和亚马逊高 CPU 使用率。EC2

此外，当您提交服务请求或事件报告时，您可以选择添加“抄送电子邮件”（强烈推荐），这些电子邮件地址会收到有关服务请求或事件的通知。

Important

虽然服务请求和事件报告中提供的 CC 电子邮件地址会收到有关通信的电子邮件通知，但其他通知（例如修补通知）会出现在您的服务请求列表中（还会向默认联系人发送电子邮件），而不会明确通知您有通信等待您的关注。因此，我们强烈建议您尽可能添加抄送电子邮件，并将默认联系人电子邮件设置为所有使用 AMS 的用户均加入的群组。

此外，您可以针对新的 AMIs、RFC 状态更改以及 AMS 账户中的配置更改请求特殊通知。接下来将讨论这些可选的通知服务。

带有 SNS 的 AMS AMI 通知

AMS 提供了 AMI 通知服务。您可以使用它订阅亚马逊简单通知服务 (SNS) Simple Notification Service 主题，该主题将在 AMS AMI 更新发布时通知您。您可以选择仅接收 AMIs 您使用的 AMS 的通知，也可以注册接收所有 AMS 的更新通知 AMIs。有关 SNS 主题的更多信息，请参阅[什么是 Amazon 简单通知服务？](#)

每当 AMIs 发布时，我们都会向相应主题的订阅者发送通知；本节介绍如何订阅 AMS AMI 通知。

示例消息

```
{
  "Type" : "Notification",
  "MessageId" : "example messageId",
  "TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
  "Subject" : "New AMS AMIs are Now Available",
  "Message" : "{\"v1\": {\"Message\": \"A new version of the AMS Amazon Machine Images has been released. You are now able to launch new EC2 stacks from these AMIs. Please use this time to update any dependencies such as CloudFormation or Autoscaling groups. Release Notes Windows - Contains latest Windows Patches: Microsoft Windows Server 2008 R2 Datacenter - (KB2819745, KB3018238, KB4507004, KB4507437) Microsoft Windows Server 2016 Datacenter Security Enhancedn - (KB4509091, KB4507459) Microsoft Windows Server 2016 Datacenter - (KB4509091, KB4507459) Microsoft Windows Server 2012 R2 Security Enhancedn - (KB3191564, KB3003057, KB3013172, KB3185319, KB4504418,
```

```
KB4506996, KB4507463) Microsoft Windows Server 2012 R2 Standardn - (KB3003057,
KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Linux - Contains latest Linux
patches -
All AMIs now force domainjoin-cli leave before domainjoin-cli join for better
stability in the domain join process.", "images":
{"images": {"image_name": "customer-ams-windows2019-2021.08-1", "image_id":
"ami-05dfa45396fddaa5e"}}, "region": "us-east-1"}},
"Timestamp" : "2021-09-03T19:05:57.882Z",
"SignatureVersion" : "1",
"Signature" : "example sig",
"SigningCertURL" : "example url",
"UnsubscribeURL" : "example url"
}
```

可能要订阅的 AMS AMI 主题：

- 全部：使用customer-ams-all-amis。当任何 AMS AMIs 更新时，此主题订阅会通知您。
- AMS AWS Linux AMIs：对于亚马逊 Linux，请使用customer-ams-amazon1和customer-ams-amazon1-security-enhanced。对于亚马逊 Linux 2，使用customer-ams-amazon2和customer-ams-amazon2-security-enhanced。
- AMS SUSE Linux AMIs：使用customer-ams-sles12或customer-ams-sles15。
- AMS AWS RedHat AMIs：使用customer-ams-rhel8customer-ams-rhel8-security-enhanced、customer-ams-rhel7、customer-ams-rhel7-security-enhanced。
- AMS AWS CentOS AMIs：使用customer-ams-centos7，customer-ams-centos7-security-enhanced。
- AMS Ubuntu AMIs：使用。customer-ams-ubuntu18
- AMS AWS Windows AMIs：使用customer-ams-windows2019customer-ams-windows2019-security-enhancedcustomer-ams-windows2016、customer-ams-windows2016-security-enhanced、customer-ams-windows2012、customer-ams-windows2012r2、customer-ams-windows2012r2-security-enhanced、customer-ams-windows2022。

要使用亚马逊 SNS 控制台订阅 AMS 新的 AMI 通知，请执行以下操作：

1. 打开 Amazon SNS 控制台以显示[控制面板](#)。
2. 在右上角，切换到您要订阅的 AWS 区域。AMIs
3. 在左侧导航窗格中，选择订阅，然后选择创建订阅。

4. 提供以下信息：

- a. 主题 ARN：`arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}` 其中区域是所选的 AWS 区域（创建 SNS 通知的地方），*AMS_AMI_NAME* 是您想要通知的 AMI。示例：
 - 要订阅 AWS 区域 us-east-1 AMIs 中新 AMS Amazon Linux 的通知，请使用此主题 ARN = `arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`
 - 要订阅 AWS 区域 us-west-2 的新 AMS Window Server 2016 AMIs 的通知，请使用此主题 ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`
 - b. 对于协议，选择电子邮件。
 - c. 对于端点，输入可用来接收通知的电子邮件地址。我们建议使用通讯组列表而不是个人的电子邮件。
5. 选择创建订阅。
6. 当您收到主题为“AWS 通知-订阅确认”的确认电子邮件时，请打开电子邮件并选择确认订阅以完成订阅。

Note

您不仅限于通过电子邮件发送该协议。有关其他可接受协议及其使用方法的信息，请参阅[订阅](#)。

要使用 AWS SNS 控制台取消订阅 AMS 新 AMI 通知，请执行以下操作：

1. 打开 Amazon SNS 控制台以显示[控制面板](#)。
2. 在导航栏中，切换到您选择的 AWS 区域。您必须使用要接收相应通知的 AWS 区域 AMIs。
3. 在导航窗格中，选择“订阅”，选择订阅，然后选择“操作”->“删除订阅”。
4. 当系统提示进行确认时，选择 Delete（删除）。

要使用部署 | Ingestion | Stack from CloudFormation template | Create (ct-36cn2avfrrj9v) 订阅 AMS New AMI 通知，请执行以下操作：

1. 要订阅 AmazonLinuxSubscription，请创建并保存执行参数 JSON 文件；此示例将其命名为 `CreateSubscribeAmiParams.json`：

```
{
```

```
"AWSTemplateFormatVersion": "2010-09-09",
"Resources": {
  "AmazonLinuxSubscription":{
    "Type" : "AWS::SNS::Subscription",
    "Properties": {
      "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
      "Protocol": "email",
      "Endpoint": "username@yourdomain.com"
    }
  }
}
```

2. 创建并保存包含以下内容的 RFC 参数 JSON 文件；此示例将其命名为 CreateSubscribeAmiRfc.json 文件：

```
{
  "ChangeTypeId": "ct-36cn2avfrrj9v",
  "ChangeTypeVersion": "1.0",
  "Title": "cfn-ingest-subscribe-ami"
}
```

3. 创建 RFC，指定 CreateSubscribeAmiRfc 文件和 CreateSubscribeAmiParams 文件：

```
aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json --
execution-parameters file://CreateSubscribeAmiParams.json
```

您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

有关创建的示例 AMIs，请参阅[创建 AMI](#)。

有关 AMIs 以编程方式消费的信息，请参阅[EC2 堆栈：创建](#)。

服务通知

当您需要采取行动或注意可能影响您的账户或资源的事情时，AMS 会发送出站服务请求或服务通知，包括：

- **基础设施影响**：当有底层 AWS 服务影响您的基础设施时，AMS 会发送服务通知，并且您需要在某个日期之前采取行动，否则可能会出现故障。

- EC2 硬件问题：AMS 会针对 EC2 硬件问题发送服务通知，要求您在特定日期之前重启 EC2 实例，或者告知您 AMS 将为您重启实例。这是一个重要的通知，因为重启可能会导致中断，您必须以可接受的日期进行响应，或者使用 `ct-09qbhy7kvtxqw` 创建 RFC，才能自己重启实例。如果您不回复，这样的服务通知将在五天后自动关闭。

RFC 状态变更通知

AMS 通过电子邮件和 CloudWatch 活动提供 RFC 状态变更通知：

- 通过 AMS 控制台发送电子邮件：创建 RFC 向导的第二页上有一个选项，您可以在其中添加最多五个电子邮件地址，以便在 RFC 状态发生变化时收到通知。
- CloudWatch 事件：您可以为 CloudWatch 事件配置不同的规则和目标，以接收每个 RFC 状态更改的通知。

电子邮件通知

您可以添加电子邮件地址，以接收您在 AMS 控制台中创建的 RFC 的 RFC 状态更改，也可以使用 AMS API/CLI。

在 AMS 控制台中，使用“创建 RFC”向导第二页上的“电子邮件通知”选项：

在 AMS API/CLI 中，在 RFC 的 RFC 参数部分添加这样一行（不要将该行添加到运行参数部分）：

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"
```

通知的行为因 RFC 计划类型而异：

- 预定 RFCs 接收以下日期的电子邮件通知：已提交、已计划 InProgress、已完成、已拒绝、已取消、自动拒绝或自动取消。
- 尽快 RFCs 收到以下电子邮件通知：已提交、已完成 InProgress、已拒绝、已取消或自动取消。
AutoRejected

Note

- 电子邮件通知是从这个地址发送的：`no-reply@managementservices.amazonaws.com`。

- 我们发送的电子邮件 URLs 中删除了您的 RFC 标题中的特殊字符。这是一项安全措施。

CloudWatch 活动通知

AMS 通过 CloudWatch 事件提供 RFC 状态变更的推送通知。要获取这些通知，请执行以下操作：

1. 创建将在其中发送通知的主题和订阅。您可以随心所欲地命名主题；有关如何执行此操作的信息，请参阅 [SNS 主题和订阅：创建](#)。
2. 使用“管理 | 其他 | 其他 | 其他 | 创建变更类型”提交 RFC，并在申请 RFC 状态变更通知时包含 SNS 主题和订阅。

当您提交针对此功能的“管理 | 其他 | 其他 RFC”请求时，您可以指定您有兴趣收到通知的 RFC 状态更改以及哪些更改类型，并设置其他筛选条件。例如，您可能希望仅在“管理员访问权限”更改类型 EventType 为 = RfcSubmitted 和 EventType = 时才请求收到通知 RfcUpdated。

这是您可以接收 CloudWatch 的事件通知模板（包含所有可能的值）：

```
{
  "source ": "aws.managedservices",
  "detail-type": "AMS RFC State Change",
  "detail": {
    "ActionState": "null | AwsActionPending | AwsOperatorAssigned | CustomerActionPending | NotApplicable | NoActionPending",
    "ActualExecutionTimeRange": {
      "StartTime": "null | Actual Start Time",
      "EndTime": "null | Actual End Time"
    },
    "AutomationStatus": "Automated | Manual",
    "AwsAccountId": "AWS Account ID",
    "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending | Rejected | Approved",
    "ChangeTypeId": "Change_Type_ID",
    "ChangeTypeVersion": "Change_Type_Version",
    "CreatedTime": "Created_Time",
    "CustomerApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending | Rejected | Approved",
    "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected | RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted | RfcUpdated",
    "LastModifiedTime": "Last_Updated_Time",
```

```

    "LastSubmittedTime": "null | Last_Submitted_Time",
    "RequestedExecutionTimeRange": {
        "StartTime": "null | Expected_Start_Time",
        "EndTime": "null | Expected_End_Time"
    },
    "RfcId": "RFC_ID",
    "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled |
ExecutionLock | InProgress | Success | Failure",
    "Title": "Title"
}
}

```

实际 CloudWatch 事件通知中显示的支持的 RFC 状态更改 (EventType) 是：

- RfcActionStateUpdated (没有 AMS 控制台选项)：处于其中一种状态的 RFC (稍后介绍) 已更改。
- RfcApproved (没有 AMS 控制台选项)：RFC 通过了系统 and/or AMS 操作员验证，并已获准完成。
- RfcAutoRejected (自动拒绝)：RFC 未通过系统验证或 AMS 操作员并已被拒绝。
- RfcCanceled (已取消或自动取消)：RFC 已被提交者或 AMS 操作员取消。
- RfcCompleted (已完成)：RFC 运行参数已完成，包括 UserData。
- RfcCreated (没有 AMS 控制台选项)：RFC 已成功创建 (JSON 和提交的参数有效)。
- RfcInProgress (InProgress): RFC 运行仍在进行中。
- RfcRejected (已拒绝)：RFC 失败的系统或 AMS 操作员验证已被拒绝。
- RfcSubmitted (已提交)：RFC 已提交，正在进行系统验证。
- RfcUpdated (没有 AMS 控制台选项)：AMS 操作员已手动更新 RFC。

此外，您可以向任何支持的目的地发送 CloudWatch 事件 (CWE) 通知，并在这些自动通知的基础上构建自己的系统：

- 亚马逊 EC2 实例
- AWS Lambda 函数
- Amazon Kinesis Data Streams 中的流
- Amazon Data Firehose 中的传送流
- Amazon CloudWatch 日志中的日志组
- Amazon ECS 任务

- Systems Manager 运行命令
- Systems Manager Automation
- AWS Batch 工作
- Step Functions 状态机
- 管道进来 CodePipeline
- CodeBuild 项目
- Amazon Inspector 评估模板
- Amazon SNS 主题
- Amazon SQS 队列
- 内置目标：EC2 CreateSnapshot API 调用、EC2 RebootInstances API 调用、EC2 StopInstances API 调用和 EC2 TerminateInstances API 调用。
- 其他 AWS 账户的默认事件总线

Note

我们会尽力发送有关 RFC 状态更改 CloudWatch 的事件通知。

设置私有和公有 DNS

在入职期间，AMS 会设置私有 DNS 服务，用于您的托管资源与 AMS 之间的通信。

您可以使用 AMS Route 53 管理应用程序资源（Web 服务器、应用程序服务器、数据库等）的内部 DNS 名称，而无需将这些信息暴露给公共 Internet。这增加了额外的安全层，还允许您通过将 DNS 名称映射到不同的 IP 地址来从主资源故障转移到辅助资源（通常称为“翻转”）。

使用部署 | 高级堆栈组件 | DNS（私有）| 创建（ct-0c38gftq56zj6）或部署 | 高级堆栈组件 | DNS（公共）| 创建（ct-0vzsr2nyraedl）创建私有 DNS 资源后，你可以使用管理 | 高级堆栈组件 | DNS（私有）| 更新（ct-1d55pi44ff21u）和管理 | 高级堆栈组件 | DNS（公共）| 更新（ct-1hzofpphabs3i），配置其他记录集或更新现有记录集。CTs 对于多账户 landing zone (MALZ) 账户，VPCs 可以在应用程序账户中创建的 DNS 资源与共享服务账户 VPC 共享，以便使用 AMS AD 维护集中式 DNS。

MALZ

下图说明了多账户着陆区 AMS 可能的 DNS 配置。它说明了 AMS 和典型客户网络之间的混合 DNS 设置。客户网络 DNS 服务器中的规范名称记录 (CNAME) 使用条件转发到共享服务账户中的 AMS AD DNS，条件转发将 AMS FQDN 的别名记录转发到 A 记录。

SALZ

下图说明了单账户着陆区 (SALZ) 可能的 DNS 配置。它显示了 AMS 和典型客户网络之间的混合 DNS 设置。客户网络 DNS 服务器中的别名记录通过条件转发到 AMS AD DNS，条件转发将 AMS FQDN 的别名记录转发到 A 记录。

SALZ Route53 DNS

下图说明了单账户着陆区 (SALZ) 可能的 DNS 配置。它显示了 AMS 和典型客户网络之间的混合 DNS 设置。客户网络 DNS 服务器中的别名记录通过条件转发到 AMS AD DNS，条件转发将 AMS FQDN 的别名记录转发到 A 记录。这还利用 Route53 来处理出站网络流量，这样账户中的任何应用程序都可以在可用性最高的账户中使用 DNS 解析。

已启用 Route53 的解析路径：

- 正在尝试解析 AMS MAD 名称的实例--> VPC +2 (Route53/ AmazonProvided DNS) --> 条件转发器已评估--> Route53 MAD 条件转发器规则匹配--> Route53 出站解析器--> 托管 AD DNS
- 正在尝试解析客户本地名称的实例--> VPC +2 (AmazonProvidedRoute53/ DNS) --> 条件转发器已评估--> Route53 本地条件转发器规则匹配--> Route53 出站解析器--> 客户本地 DNS
- 正在尝试解析互联网名称的实例--> VPC +2 (Route53/ AmazonProvided DNS) --> 已评估条件转发器--> 没有匹配的转发器--> 互联网 DNS 服务

有关更多信息，请参阅在[您的 VPC 中使用 DNS](#) 和[使用私有托管区域](#)。

AMS 出口流量管理

默认情况下，AMS 私有子网和客户应用程序子网的目标 CIDR 为 0.0.0.0/0 的路由将网络地址转换 (NAT) 网关作为目标。AMS TrendMicro 服务和补丁是必须具有互联网出口访问权限的组件，这样 AMS 才能提供其服务，TrendMicro 并且操作系统可以获取更新。

AMS 支持通过客户管理的出口设备将出口流量转移到互联网，前提是：

- 它充当隐式（例如，透明）代理。

以及

- 它允许 AMS HTTP 和 HTTPS 依赖关系（在本节中列出），以便能够持续修补和维护 AMS 托管基础架构。

部分示例包括：

- 公交网关 (TGW) 的默认路由，通过多账户着陆区网络账户中的 AWS Direct Connect 连接指向客户管理的本地防火墙。
- TGW 有一个默认路由，指向利用 AWS 的多账户着陆区出口 VPC 中的 AWS 终端节点，指向另一个 PrivateLink AWS 账户中的客户管理的代理。
- TGW 的默认路由指向另一个 AWS 账户中的客户管理的防火墙，site-to-siteVPN 连接作为多账户着陆区 TGW 的附件。

AMS 已经确定了相应的 AMS HTTP 和 HTTPS 依赖关系，并不断开发和完善这些依赖关系。请参阅 [egressMgmt.zip](#)。除了 JSON 文件外，ZIP 还包含一个自述文件。

Note

- 此信息并不全面，此处未列出一些必需的外部站点。
- 请勿在拒绝列表或屏蔽策略下使用此列表。
- 此列表旨在作为出口过滤规则集的起点，期望使用报告工具来精确确定实际流量与列表的偏离位置。

要询问有关筛选出口流量的信息，请发送电子邮件至 CSDM：ams-csdm@amazon.com。

在 AMS 高级版中部署 IAM 资源

AMS 通过两种方式在您的多账户着陆区 (MALZ) 应用程序和单账户着陆区 (SALZ) 账户中部署 IAM 资源：

- 自动化 IAM 配置：AMS 中的此功能允许您提交创建、更新或删除 IAM 角色或策略配置的变更类型，无需操作员审查，并且自动运行 IAM 和 AMS 验证检查。

必须通过管理 | 托管账户 | 具有读写权限的 AMS 自动 IAM 配置 | 启用 ([需要审查](#)) [更改类型 \(ct-1706xvvk6j9hf\)](#) [明确启用](#) 此功能。要了解更多信息，请参阅 [自动化 IAM 配置 AMS](#)。启用 AMS 自动 IAM 配置后，您可以访问“创建”、“更新”和“删除”更改类型来管理您的 IAM 资源。

- 查看所需的 IAM 变更类型：此变更类型，部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | [创建实体或策略 \(需要审查\)](#) (ct-3dpd8mdd9jn1r)，需要 AMS 操作员审查，如果需要澄清，有时可能需要几天才能完成。

Note

无论使用哪种方法，都会向相关账户配置一个 IAM 角色，在配置该角色后，您必须在联合身份验证解决方案中加入该角色。

自动化 IAM 配置 AMS

AWS Managed Services (AMS) 支持使用 AMS Advanced 变更请求 () 和新变更类型 (RFCs) 自动验证和配置 IAM 资源 (包括角色和策略 CTs)。以前，这些请求经过半自动流程，有时会导致等待时间很长。现在，您可以使用 AMS 自动 IAM 配置来配置 IAM 资源并更快地获得结果。

AMS 中的自动 IAM 配置的工作原理

自动化 IAM 配置依赖于 IAM 的自动运行时检查来验证 IAM 资源的更改。这些自动检查是在运行“创建”、“更新”或“删除”更改类型时执行的，可防止过度宽松或模式不安全的 IAM 资源部署到您的账户中。这使您可以将 IAM 审核的严格程度与团队的专业知识相匹配。我们建议刚接触云服务且需要手动检查所有 IAM 资源变更的团队使用现有的“需要审阅”的更改类型：部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | [创建实体或策略 \(需要审阅\)](#)，(ct-3dpd8mdd9jn1r)。具有 AWS 专业知识并能控制其环境的团队可以使用自动 IAM 配置来加快部署速度。您可以使用此功能通过自动运行时检查来执行验证，或者在成功验证后对 IAM 资源进行验证和配置。

Important

AWS Managed Services 已主动实施了一系列验证 [运行时检查](#)，以防止创建具有特定权限和条件的 IAM 资源或策略。有关这些权限和条件的描述，请参阅在 [AMS 高级版中部署 IAM 资源](#)。自动变更类型 [ct-1n9gfnog5x7fl](#)、[ct-1e0xmuy1diafq](#) 和 [ct-17cj84y7 632o6](#) 允许精通管理 IAM 资源的用户配置允许超出只读权限的操作的 IAM 角色和策略。

此外，您可以使用通过自动变更类型 [ct-1n9gfnog5x7fl](#)、[ct-1e0xmuy1diafq](#) 和 [ct-17cj84y7632o6](#) 创建的角色来创建新资源。但是，这些资源不能遵循 AMS 命名标准，也不是标准 AMS 堆栈的一部分。AMS 尽最大努力为这些特定资源提供运营和安全支持。虽然手动和自动流程都旨在维护我们的安全标准，但值得注意的是，两者之间的检查存在差异。自动配置允许更灵活地创建和更新角色和策略；因此，它们是不一样的。建议您的组织仔细查看《AMS 用户指南》中列出的验证[运行时检查](#)，以确保它们符合贵组织的期望和要求。

验证流程

验证和配置流程

Note

此功能适用于对 IAM 资源有经验 AWS 的团队，我们不建议刚开始使用该功能的团队使用 AWS。自动验证流程旨在捕捉大多数错误，有助于团队在了解所需的权限后快速查看 IAM 的更改。为了安全有效地使用新的变更类型，我们建议您充分了解 AWS IAM 以及变更类型提供的[运行时检查](#)，以确定它们是否适合您的团队。

登录 AMS 在 AMS 中自动配置 IAM

要使用新的更改类型，请先使用以下更改类型提交 RFC 来启用 AMS 自动 IAM 配置：管理 | 托管账户 | 具有读写权限的 AMS 自动 IAM 配置 | [启用（需要审阅）\(ct-1706xvvk6j9hf\)](#)。AWS 要求您的组织通过客户安全风险管理体系 (CSRM) 流程，以确保这些变更类型的使用符合您的组织政策。作为所需审查的一部分，AWS 运营团队会与您合作，以风险接受的形式获得您的安全团队联系人的明确批准。要了解更多信息，请参阅 [RFC 客户风险管理 \(CSRM\)](#) 流程。

在开启具有读写权限的 AMS 自动 IAM 配置功能的 RFC 成功后，AMS 将在用于提交启用 RFC 的账户中启用 AMS 自动 IAM 配置变更类型。要确认账户是否已开启 AMS 自动 IAM 配置，请在 IAM 控制台中查看该 `AWSManagedServicesIAMProvisionAdminRole` 角色。

在入职过程中，AMS 会在账户的同一 AWS 区域配置 IAM 访问分析器，以利用其访问预览功能。IAM Access Analyzer 可帮助识别您的组织和账户中与外部实体共享的资源，根据策略语法和最佳实践验证 IAM 策略，并根据 AWS CloudTrail 日志中的访问活动生成 IAM 策略。要了解更多信息，请参阅[使用 AWS Identity and Access Management Access Analyzer](#)。

一旦加载，就会部署到AWSManagedServicesIAMProvisionAdminRole已启用的账户。如果您选择通过 SAML 联合使用此角色，则必须将该角色加入您的联合解决方案。

作为入职的一部分，您可以使用请求更新 AWSManaged服务的IAMProvisionAdminRole信任政策，以授予其他 IAM 角色 ARN 代入此角色。AWS Security Token Service

在 AMS 中使用 AMS 自动化 IAM 配置

您可以使用 RFCs 以下 AMS 自动 IAM 配置更改类型进行创建。

Note

- 仅支持对角色和策略进行置备。

更新角色时，Update CT 将现有的托管策略列表 Amazon 资源名称 (ARNs) 和“代入角色”策略文档替换为提供的托管策略列表 ARNs 和“代入角色”策略文档。在部分更新中；例如，在现有托管策略列表中添加或删除 ARN ARNs，不允许在“代入角色”策略文档中添加或删除单个策略声明。同样，在更新策略时，Update CT 会取代现有的策略文档，并且不允许在现有政策文档中添加或删除单个政策声明。

- 选择“仅验证”选项后，将在不预配置任何 IAM 实体或策略的情况下执行运行时检查。不管有什么发现，RFC 的状态都是“成功”。“成功”状态表示已成功对所提供的 IAM 实体或策略进行验证。

- 部署 | 高级堆栈组件 | 身份和访问管理 (IAM) Management | [创建实体或策略 \(读写权限\)](#) (ct-1n9gfnog5x7fl)：自动验证和配置新的 IAM 实体或策略。
- 管理 | 高级堆栈组件 | 身份和访问管理 (IAM) Management | [更新实体或策略 \(读写权限\)](#) (ct-1e0xmuy1diafq)：现有 IAM 实体或策略会自动更新和验证。
- 管理 | 高级堆栈组件 | 身份和访问管理 (IAM) Management | [删除实体或策略 \(读写权限\)](#) (ct-17cj84y7632o6)：使用自动创建实体或策略更改类型配置的现有 IAM 实体或策略已删除。

您只能 CTs 使用专用 IAM 角色调用前三个角色:AWSManagedServicesIAMProvisionAdminRole. 此角色仅适用于使用管理 | 托管账户 | AMS 自动 IAM 配置读写权限 | [启用 \(需要审核\)](#) (ct-1706xvvk6j9hf) 加入该功能的账户。

Important

创建、更新和删除更改类型在您的账户中始终可见，但默认情况下它们并未开启。如果您在未先启用 AMS 自动 IAM 配置功能的情况下尝试使用其中一种更改类型提交 RFC，则会显示“未授权”错误。

限制:

- 创建 CT 可能允许您创建具有创建 AWS 资源权限的 IAM 角色或策略。但是，由这些角色和策略创建的 AWS 资源不由 AMS 管理。最佳做法是遵守组织控制以限制此类角色或策略的创建。
- Update CT 无法修改通过 CFN Ingest、直接更改模式、开发者模式创建的 IAM 角色和策略，在某些情况下，也无法修改通过现有 AMS Advanced 手动或自动模式创建的 IAM 角色和策略。CTs
- 删除 CT 无法删除不是使用 AMS 自动 IAM 配置创建 CT 创建的现有角色或策略。
- 直接更改模式角色不支持具有读写权限的 AMS 自动 IAM 配置功能。这意味着您无法使用这些角色配置或更新具有读写权限的 IAM 角色和策略。
- 具有读写权限的 AMS 自动 IAM 配置创建、更新和删除更改类型与 ServiceNow 连接器不兼容。

在 AMS 中对 AMS 自动 IAM 配置进行运行时检查

自动化 IAM 配置利用来自 AMS 边界策略的检查 AWS Identity and Access Management Access Analyzer，并根据 AMS 边界策略执行额外的检查和验证。AMS 基于 IAM 最佳实践、在云端操作客户工作负载的经验以及 AMS IAM 手动评估的集体经验，定义了额外的检查和验证。

您可以在更改请求 (RFC) 输出中查看策略运行时检查结果。调查结果包括资源标识符、生成调查结果的角色 and/or 策略中的位置，以及一条概述 IAM 实体或资源未能通过检查的消息。这些发现可帮助您制定功能齐全且符合安全最佳实践的策略。

Note

自动 IAM 配置会尝试具体说明未能通过检查的实体或策略定义中的位置。根据类型，该位置可能包括资源名称、ARN 或数组内的索引。例如，一份可帮助您调整实体或政策以取得成功结果的声明。

为了获得流畅的 AMS 自动 IAM 配置体验，最佳做法是使用“仅验证”选项来运行验证检查，直到 RFC 输出中没有报告验证检查的结果。当验证检查未报告任何发现结果时，选择从 AMS 控制台创建副本以

快速创建现有 RFC 的副本。准备好配置后，在“参数”部分中，将“仅验证”值从“是”切换为“否”，然后继续。

以下是 AMS 自动 IAM 配置为确保您的 IAM 资源安全而执行的运行时检查：

-  Note

要配置包含这些自动变更类型拒绝的操作的 IAM 策略，您必须遵循 RFC 客户安全风险管理体系 (CSRM) 流程。使用以下更改类型：部署 | 高级堆栈组件 | 身份和访问管理 (IAM) Management (IAM) | 创建实体或策略 (需要审查) (ct-3dpd8mdd9jn1r)。
- IAM Access Analyzer 策略检查和验证：另请参阅[访问分析器策略检查参考](#)和 [IAM Access Analyzer 策略验证](#)。
 - AMS 权限边界策略检查：对一组默认情况下被拒绝的服务的操作。有关更多信息，请参阅 [IAM 自动配置权限边界检查](#)。
 - 客户定义的权限边界策略检查：对一组被拒绝的服务执行其他受限操作。有关更多信息，请参阅 [IAM 自动配置权限边界检查](#)。
 - AMS 定义的自定义检查：用于识别所请求的 IAM 实体或策略中的各种不安全和过于宽松的策略或访问模式的检查，如果找到则拒绝请求。有关信息，请参阅 [AWS JSON 策略元素：委托人](#)。

调查发现	说明
可以从您信任区域之外的外部账户访问该角色。	此发现指的是角色信任策略中列出的委托人，该委托人位于您的信任区域之外。信任区域定义为创建角色的账户或该账户所属的 AWS 组织。不属于该账户或同一 AWS 组织的实体是外部实体。要解决此问题，请查看委托 ARNs 人中的账户 ID，确保它们属于您并且是 AMS 已注册账户。
该角色可由不属于 AMS 客户所有账户 <i>External_Account_ID</i> 的账户所拥有的外部实体访问。 <i>Account_ID</i>	如果角色信任策略包含一个不属于您的账户 ID 的委托人 ARN 和一个 AMS 已注册账户，则会生成此结果。要解决此问题，请从角色信任策略中删除任何此类委托人。

调查发现	说明
规范用户 ID 不是 IAM 信任策略中支持的委托人。	IAM 信任策略 IDs 不支持规范委托人。要解决此问题，请从角色信任策略中移除任何此类委托人。
您信任区域之外的外部 Web 身份可以访问该角色。	如果角色信任策略允许 SAML IdP 以外的外部 Web 身份提供商 (IdP)，则会生成此结果。要解决此问题，请查看角色信任策略并删除允许该 <code>sts:AssumeRoleWithWebIdentity</code> 操作的声明。
可以通过 SAML 联合访问该角色；但是，所提供的 SAML 身份提供商 (IdP) 不存在。	如果角色信任策略包含您的账户中不存在的 SAML IdP，则会生成此结果。要解决此问题，请确保您的账户中存在所有列出的 SAML IdP。
策略包含等同于管理员或高级用户访问权限的特权操作。考虑将权限范围缩小到特定的服务、操作或资源。如果使用高级策略元素（例如 <code>NotAction</code> 或 <code>NotResource</code>），请确保它们授予的访问权限不会超出您的预期，尤其是在 <code>Allow</code> 语句中。	在 AWS Identity and Access Management 使用 IAM 策略设置权限时，仅授予执行任务所需的权限是最佳安全实践。通过定义在特定条件下可以对特定资源采取的操作（也称为最低权限权限）来实现此目的。当自动化检测到策略授予广泛权限且不符合最小权限原则时，就会生成此发现。要解决调查结果，请查看并减少权限。
语句包含的权限操作 <i>Service_Name</i>。考虑使用 <code>deny</code> 语句排除这些操作。有关特权操作的列表，请参阅 AMS 文档中的边界策略参考。	AMS 认为某项服务的某些行为存在风险，需要客户安全团队进行进一步的风险审查和接受。当自动化检测到授予此类权限的给定策略时，就会生成此结果。要解决此问题，请在您的政策中拒绝这些操作。有关操作列表，请参阅 AMS 边界策略。有关 AMS 边界策略的详细信息，请参阅 AMS 自动化 IAM 配置权限边界检查。
声明允许访问特权 RFC 变更类型：ct-1n9gfnog5x7fl、ct-1e0xmuy1diafq 和 ct-17cj84y7632o6 进行服务。 <i>Service_Name</i> 考虑将权限范围限定为特定的变更类型，或者使用 <code>deny</code> 语句排除这些变更类型。	如果策略授予使用自动 IAM 配置更改类型 () CTs 执行 RFC 相关操作的权限，则会生成此结果。CTs 它们需要接受风险，并且只能通过已上岗的角色使用。因此，你不能向它们授予权限 CTs。要解决此问题，请拒绝使用这些 CTs 操作的 RFC 操作。

调查发现	说明
语句包含的特权操作，这些操作不限于您的服务 <i>Service_Name</i> 资源。考虑将操作范围限定为特定资源或排除带有 AMS 命名空间前缀的资源。如果使用通配符，请确保它们将范围限制在您的资源范围内。	如果策略授予的权限操作不限于给定服务的资源，则会生成此结果。通配符通常会创建过于宽松的策略，从而将一系列资源或操作纳入权限的范围。要解决此问题，要么缩小您拥有的资源的权限范围，要么排除 AMS 命名空间中的资源。有关 AMS 命名空间前缀的列表，请参阅 AMS 文档中的边界策略。请注意，并非所有前缀都适用于所有服务。有关 AMS 边界策略的详细信息，请参阅AMS 自动化 IAM 配置权限边界检查。
账户 ID 或亚马逊资源名称 (ARN) 无效。	如果策略或角色信任策略中指定的任何 ARN 或账户 ID 无效，则会生成此结果。要查看有效资源 ARN 的服务资源，请参阅服务授权参考。确保账户 ID 为 12 位数字，并且该账户处于活动状态。AWS
在 ARN 中限制使用通配符 (*) 作为账户 ID。	如果在 ARN 的账户 ID 字段中指定了通配符 (*)，则会生成此结果。账户 ID 字段中的通配符与任何账户匹配，并可能授予对资源的非预期权限。要解决此问题，请将通配符替换为特定的账户 ID。
指定的资源账户不属于同一 AMS 客户拥有的账户 <i>Account_ID</i> 。	如果资源 ARN 中指定的账户 ID 不属于您且不由 AMS 管理，则会生成此结果。要解决这个问题，请确保所有资源（如其在策略中的 ARN 中指定）都属于由 AMS 管理的账户。
角色名称位于 AMS 受限命名空间中。	如果您尝试创建名称以 AMS 保留前缀开头的角色，则会生成此结果。要解决此问题，请使用特定于您的用例的角色名称。有关 AMS 保留前缀的列表，请参阅AMS 保留前缀
策略名称位于 AMS 受限命名空间中。	如果您尝试创建名称以 AMS 保留前缀开头的策略，则会生成此结果。要解决此问题，请使用特定于您的用例的策略名称。有关 AMS 保留前缀的列表，请参阅AMS 保留前缀。

调查发现	说明
ARN 中的资源 ID 位于 AMS 受限命名空间中。	如果您尝试创建向 AMS 命名空间中的命名资源授予权限的策略，则会生成此结果。要解决此问题，请确保您限制资源的权限或拒绝对 AMS 命名空间中的资源的权限。有关 AMS 命名空间的更多信息，请参阅 AMS 受限命名空间 。
策略变量大小写无效。将变量更新为 <i>Variable_Names</i> 。	如果在错误的情况下尝试创建包含 IAM 全局策略变量的策略，则会生成此结果。要解决此问题，请在策略中对全局变量使用正确的大小写。有关全局变量的列表，请参阅 AWS 全局条件上下文键 。有关策略变量的更多信息，请参阅 IAM 策略元素：变量和标签
语句包含不限于您的 KMS 密钥的特权操作。考虑将这些权限限定为特定的密钥或排除 AMS 拥有的密钥。	如果策略包含的权限不限于您拥有的特定 KMS 密钥，则会生成此结果。要解决此问题，请将权限范围限定为特定密钥或排除 AMS 拥有的密钥。AMS 拥有的密钥具有特定的别名集。有关 AMS 拥有的密钥别名的列表，请参阅 AMS 自动化 IAM 配置权限边界检查 。
语句包含不限于 KMS 密钥别名的权限操作。考虑将这些权限限定为您的密钥或别名，或者排除 AMS 拥有的密钥别名。	如果策略包含的权限不限于您拥有的特定 KMS 密钥别名，则会生成此结果。要解决此问题，请将权限范围限定为特定密钥或排除 AMS 拥有的密钥。AMS 拥有的密钥具有特定的别名集。有关 AMS 拥有的密钥别名的列表，请参阅 AMS 自动化 IAM 配置权限边界检查 。

调查发现	说明
语句包含的特权操作，这些操作的范围不够大，仅限于使用的 KMS 密钥。kms:ResourceAliases condition 考虑使用特定的别名以及条件键的相应集合运算符。如果在别名中使用通配符，请确保它们将范围限制在有限的 KMS 密钥集内。	如果您使用条件来限定 KMS 密钥的权限范围，而不是使用将范围缩小 kms:ResourceAliases 到 KMS 密钥的别名，则会生成此结果。或者，如果 kms:ResourceAliases 条件密钥的值还包含 AMS 拥有的 KMS 密钥别名。要解决此问题，请更新条件以将权限范围缩小到您的 KMS 密钥的别名或排除 AMS 拥有的 KMS 密钥的别名。有关 AMS 拥有的密钥别名的列表，请参阅AMS 自动化 IAM 配置权限边界检查。
该角色必须附有 customer_deny_policy。将策略 ARN 包含在托管策略列表中。 ARNs	如果您正在创建的角色没有 customer_deny_policy 附加到该角色，则会生成此结果。要解决此问题，请在托管策略 ARNs 列表 customer_deny_policy 中添加。
AWS 托管策略过于宽松或授予受 AMS 边界策略限制的权限。	如果角色的 ManagedPolicyArns 值包含任何提供对相关服务的完全或管理员级别访问权限的 AMS 托管策略，则会生成此结果。要解决这个问题，请查看 AWS 托管策略的使用情况，使用提供范围缩小权限的策略，或者根据最低权限原则定义自己的策略。
客户托管策略位于受限的 AMS 命名空间中。	如果将任何在 AWS 命名空间中以名称为前缀的客户托管策略附加到该角色，则会生成此结果。要解决此问题，请从该角色的 ManagedPolicyArn 列表中删除该策略。
无法将 customer_deny_policy 与角色分离。将策略 ARN 包含在托管策略列表中。 ARNs	如果在更新期间与 customer_deny_policy 角色分离，则会生成此结果。要解决此问题，请将 customer_deny_policy 添加到角色的 ManagedPolicyArns 字段中，然后重试。

调查发现	说明
客户管理的策略是在 AMS 变更管理服务之外配置的，或者未经事先验证。	如果将一个或多个现有的客户托管策略附加到某个角色，并且 ARNs 这些策略不是通过 AMS 变更管理服务（通过 RFC）配置的，则会生成此结果。例如，开发人员模式或直接更改模式允许客户在没有 RFC 的情况下配置 IAM 策略。要解决此问题，请 ARNs 从该角色的 ManagedPolicyArns 列表中删除客户托管策略。
提供的托管策略数量 ARNs 超过每个角色配额的附加策略。	如果附加到角色的托管策略总数超过每个角色的策略配额，则会生成此结果。有关 IAM 配额的更多信息，请参阅 IAM 和 AWS STS 配额、名称要求和字符限制。使用此信息来减少您附加到该角色的策略数量。
信任策略大小 ({trust_policy}) 超过了假设角色策略大小配额 {size}。	如果代入角色策略文档的大小超过策略大小配额，则会生成此结果。有关 IAM 配额的更多信息，请参阅 IAM 和 AWS STS 配额、名称要求和字符限制。
声明包含 Amazon S3 的所有变异操作。考虑将这些权限的范围仅限于必需的操作。如果使用通配符，请确保通配符的作用范围有限的一组突变动作。	如果给定策略授予所有 Amazon Simple Storage Service 变异权限，而不考虑一个或多个资源，则会生成此结果。要解决此问题，请仅对您的存储桶执行必需的 Amazon S3 突变操作。
声明包含不允许对 Amazon S3 中的任何存储桶执行的特权操作。考虑添加一条否认这些操作的声明。	如果策略允许对任何存储桶执行特权操作，则会生成此结果。有关特权操作的列表，请参阅 AMS 自动化 IAM 配置权限边界检查 要解决此问题，请在策略中删除或拒绝这些操作。
声明包含不限于 Amazon S3 中存储桶的特权操作。可以考虑包含您的存储桶或排除带有 AMS 命名空间前缀的存储桶。如果使用通配符，请确保它们与您的命名空间中的存储桶相匹配。	如果策略授予 Amazon S3 操作的范围不限于您的存储桶，则会生成此结果。如果在指定存储桶资源时使用通配符，则通常会发生这种情况。要解决此问题，请指定存储桶名称或您拥有的存储桶名称 ARNs，或者排除带有 AMS 命名空间前缀的存储桶。

调查发现	说明
声明包含不限于 Amazon S3 中存储桶的特权操作。考虑避免使用通配符 (*) 来限定账户中所有存储桶的范围。	如果策略授予 Amazon S3 操作的范围不限于您的存储桶，则会生成此结果。如果在指定存储桶资源时使用通配符，则通常会发生这种情况。要解决此问题，请指定存储桶名称或您拥有的存储桶名称 ARNs，或者排除带有 AMS 命名空间前缀的存储桶。
语句包含一个资源通配符，其作用域为所有 Amazon S3 存储桶，包括不存在的存储桶和您不拥有的存储桶。考虑使用条件和s3:ResourceAccount 条件键来确定权限的范围。	如果策略向使用通配符指定的存储桶授予权限，则会生成此结果。使用通配符通常会将不存在或非所有者的存储桶置于范围内。要解决这个问题，请使用条件和aws:ResourceAccount 条件键将权限范围限定为仅限于当前账户内的存储桶。有关更多详细信息，请参阅限制对特定 AWS 账户拥有的 Amazon S3 存储桶的访问权限。
语句包含一个NotResource 策略元素，该元素的作用域可能包括大量存储桶，包括不存在的存储桶和您不拥有的存储桶。考虑使用条件和s3:ResourceAccount 条件键来确定权限的范围。	如果策略利用NotResources 策略元素来指定存储桶资源，则会生成此结果。使用该NotResource 元素可能会限制大量存储桶，包括不存在的存储桶或非所有者的存储桶。要解决这个问题，请使用条件和aws:ResourceAccount 条件键将权限范围限定为仅限于当前账户内的存储桶。
声明包含 Amazon S3 对不存在、不归账户所有或名称中包含通配符的操作Account_ID，该通配符的范围可能限定为大量存储桶，包括不存在的存储桶和您不拥有的存储桶。Bucket_Name 考虑使用条件和条件键来确定权限的s3:ResourceAccount 范围	如果策略向不存在、不归您所有或存储桶名称中包含通配符覆盖大量存储分区且访问范围不限于当前账户的存储桶授予权限，则会生成此结果。要解决这个问题，请使用条件和aws:ResourceAccount 条件键将权限范围限定为仅限于当前账户内的存储桶。

调查发现	说明
声明包含 Amazon S3 对不存在或不属于账户的存储桶<code>Bucket_Name</code> 的操作<code>Account_ID</code> , 或者名称中包含通配符, 该通配符的作用域可能限定为大量存储桶, 包括不存在的存储桶和您不拥有的存储桶。在条件下使用<code>s3:ResourceAccount</code> 或指定的资源帐户不属于您, 访问不受限制。	如果策略向不存在、不归您所有或存储桶名称中包含通配符覆盖大量存储桶且访问权限仅限于特定账户的存储桶授予权限, 则会生成此结果。但是, <code>aws:ResourceAccount</code> 条件键中指定的账户不属于您, 而是由 AMS 管理。要解决此问题, 请更新<code>aws:ResourceAccount</code> 条件密钥并设置您拥有并由 AMS 管理的相应账户 ID。
声明包含不限于您的 Amazon EC2 实例的特权操作。考虑将操作范围限定为特定实例, ARNs 或者排除名称标签键值在 AMS 命名空间前缀中的实例。如果使用通配符, 请确保它们与您拥有的命名空间相匹配。	如果策略授予对 AMS 拥有的 Amazon EC2 实例的特权操作, 则会生成此发现。AMS 实例使用名称标签键进行标记, 其值在 AMS 命名空间中。要解决这个问题, 请使用<code>StringNot Like</code> 运算符指定您的资源或排除 AMS 实例, 条件为其<code>aws:ResourceTag/Name</code> 密钥排除 AMS 命名空间中的值
语句包含特权操作, 这些操作不限于 AWS Systems Manager 参数存储中的资源。考虑指定 ARNs 您的参数或排除带有 AMS 命名空间前缀的参数。如果使用通配符, 请确保它们仅限于您的参数。	如果策略向不属于您的参数授予权限, 则会生成此结果。这通常是使用通配符或在策略声明的资源下列出带有 AMS 命名空间前缀的参数情况。要解决此问题, 请指定命名空间内的参数或使用 <code>deny</code> 语句排除 AMS 参数。
语句包含针对中的资源的特权操作 AWS Systems Manager。考虑将权限范围限定为只读操作或针对您的资源的操作。	如果策略授予对 Systems Manager 资源的参数存储或只读操作以外的权限, 则会生成此结果。要解决此问题, 请将权限减少为只读操作或仅限参数存储。
语句包含不限于您拥有的 {message} 的特权操作。<code>Service_Name</code> 考虑酌情将这些权限限定为特定的资源类型, 或者排除 AMS 拥有的资源。如果使用通配符, 请确保它们匹配<code>Resources</code> 。	如果策略允许对您的资源 (尤其是命名资源) 进行未授予的特权操作, 则会生成此结果。要解决此问题, 请查看您的资源列表, 看看它们是否仅限于命名空间中的资源。或者, 排除 AMS 命名空间中的资源。

调查发现	说明
语句包含 { <i>Service_Name</i> } 的标记操作，其作用域不限于 Name tag key 的特定值。考虑通过使用命名空间中的值设置aws:RequestTag/Name 条件键来限定这些操作的范围，或者通过使用 AMS 命名空间前缀中的值的StringNot Like 运算符设置aws:RequestTag/Name 条件键来限制这些操作。	如果策略授予给定服务的标记权限，并且该权限不限于特定的标签键/值，则会生成此结果。要缩小标签操作中可以使用的键或值的范围，例如，在请求执行操作时，请使用aws:RequestTag/tag key 条件。因此，要解决此问题，请使用此条件键来限制命名空间中的一个或多个密钥值。或者，拒绝带有 AMS 命名空间中值的Name标签密钥 (aws:RequestTag/Name)。
验证 IAM 角色信任策略时出现内部错误。	当 CT 自动化通过 IAM Access Analyzer 服务对 IAM 角色信任策略执行验证时遇到错误时，就会生成此发现。要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。
验证客户托管策略时出现内部错误。	当 CT 自动化通过 IAM Access Analyzer 服务对客户托管策略执行验证时遇到错误时，就会生成此发现。要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。
在中找不到访问分析器 <i>AWS ##</i> 。无法对角色信任策略执行访问预览检查。	此发现是在中找不到 IAM 访问分析器资源时生成的 AWS 区域。联系 AMS 运营部门在 AWS 区域进行故障排除并创建 IAM 访问分析器资源。
角色的信任策略无效 <i>Role_Name</i>	此发现是在提供的 IAM 角色包含无效的信任策略时生成的。要解决问题，请查看信任策略以验证其是否有效。
IAM 访问分析器遇到了内部错误。无法为角色创建访问预览 <i>Role_Name</i>	当自动化在通过 IAM Access Analyzer 为角色创建访问预览时遇到错误时，就会生成此发现。要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。

调查发现	说明
无法为角色的信任策略创建访问预览 <i>Role_Name</i>	当自动化在通过 IAM Access Analyzer 为角色创建访问预览时遇到错误时，就会生成此发现。要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。
验证列出的 SAML IdP 时出现内部错误。	当自动化在验证角色信任策略中 IdPs 列出的提供的 SAML 时遇到错误时，就会生成此发现。要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。
验证权限时出现内部错误。 AWS Key Management Service	当自动化在验证所提供的策略中的 AWS KMS 密钥权限时遇到错误时，就会生成此结果。要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。
验证列出的托管策略 ARNs 时出现内部错误。	当自动化在验证列出的托管策略 ARNs 时遇到错误时，就会生成此结果。要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。
验证默认 customer_deny_policy 附件时出现内部错误。	当自动化在验证是否已关联到角色时遇到错误时，就会生成此发现。customer_deny_policy 要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。
验证角色的托管策略 ARN 时出现内部错误 <i>Role_Name</i>	当自动化在验证角色的托管策略 ARNs 时遇到错误时，就会生成此结果。要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。
根据客户定义的边界策略 <i>Policy_name</i> 进行验证时出现内部错误 AWSManagedServices IAMProvisionCustomerBoundaryPolicy	当自动化在验证包含您的自定义拒绝列表的策略时遇到错误时，就会生成此结果。要解决这个问题，请重新提交 RFC。如果错误仍然存在，请联系 AMS 运营部门解决错误。

调查发现	说明
账户中AWSManagedServicesIAMProvisionCustomerBoundaryPolicy 存在客户定义的边界策略。但是，该策略包含授予权限的 allow 语句。该策略只能包含拒绝声明。	当包含您的自定义拒绝列表的策略包含授予权限的声明时，就会生成此结果。尽管自定义拒绝列表作为 IAM 托管策略存在于您的账户中，但它不能用于权限管理。该策略必须仅包含拒绝声明，表明您希望 AMS 自动 IAM 配置验证和拒绝 AMS 自动 IAM 配置创建的 IAM 策略中的那些操作。
声明包含您的组织为定义的特权操作Service_Name。考虑使用 deny 语句排除这些操作。有关受限操作列表的参考，请参阅您账户中指定的政策。	当自动化检测到您的策略中您在自定义拒绝列表中定义的任何操作时，就会生成此结果。要解决此问题，请查看您的政策声明并删除自定义拒绝列表中定义的所有操作，或者添加拒绝这些操作的拒绝声明。
角色必须已POLICY_ARN 附加。将策略 ARN 包含在托管策略列表中。 ARNs	如果您正在创建的角色没有POLICY_ARN 附加，则会生成此结果。要解决此问题，请在角色ManagedPolicyArns字段POLICY_ARN 中加入，然后重试。
POLICY_ARN 无法与角色分离。将策略 ARN 包含在托管策略列表中。 ARNs	如果在更新期间与POLICY_ARN 角色分离，则会生成此结果。要解决此问题，请将POLICY_ARN 添加到角色的ManagedPolicyArns字段中，然后重试。

AMS 自动化 IAM 配置权限边界检查

AMS 权限边界检查可帮助您遵守 AMS 提供的默认权限边界政策。此策略列出了 AMS 自动 IAM 配置拒绝的操作。包含这些受限操作的配置策略需要额外的明确风险承受能力。在此处下载政策：[boundary-policy.zip](#)。

使用客户定义的权限边界策略检查来自定义 AMS 权限边界策略默认值之外的拒绝操作。当您使用以下更改类型加入 AMS 自动 IAM 配置时：管理 | 托管账户 | 具有读写权限的 AMS 自动 IAM 配置 | [启用 \(需要审阅\)](#) (ct-1706xvvk6j9hf)，您可以包括指定其他受限操作的自定义拒绝操作列表。

您可以使用更改类型更新拒绝操作列表：管理 | 托管账户 | 具有读写权限的自动 IAM 配置 | [更新自定义拒绝列表](#) (ct-2r9xvd3sdsic0)。您必须使用专用 IAM 角色 `AWSManagedServicesIAMProvisionAdminRole` 才能运行此更改类型。

Note

- 您必须为每次更新提供一份完整的拒绝操作列表。以前的列表被新列表所取代。
- 拒绝操作列表必须仅包含要拒绝的操作。不支持“允许”操作。
- 拒绝操作列表以名为的 IAM 托管策略的形式存在于账户中 `AWSManagedServicesIAMProvisionCustomerBoundaryPolicy`。该策略不得附加到任何角色上。
- 与 IAM 权限边界相比，用于表示 AMS 自动 IAM 配置中被拒绝的操作的术语具有不同的上下文含义。IAM 权限边界设置了策略在运行时可以向 IAM 实体授予的最大权限。有关 IAM 权限边界的更多信息，请参阅 AWS Identity and Access Management 用户指南中的 [策略类型](#)。AMS 自动 IAM 配置中的权限边界会阻止您配置包含特定权限集（例如被拒绝的操作列表）的 IAM 策略。

对 AMS 自动 IAM 配置发现和错误进行故障排除

使用 AMS 自动 IAM 配置时，您可能会遇到三种问题：

- RFC 错误：这些错误可能有多种原因；例如，输入不正确。有关更多信息，请参阅 [对 AMS 中的 RFC 错误进行故障排除](#)。
- SSM 错误：这些错误可能有多种原因；例如，格式不佳。有关更多信息，请参阅 [Systems Manager 自动化故障排除](#)。
- 验证检查结果：当自动 IAM 预配运行的众多验证检查之一发现问题时，就会出现这些结果。有关验证检查的列表以及要修复的建议操作，请参阅 [在 AMS 中对 AMS 自动 IAM 配置进行运行时检查](#)。

使用 IAM 角色和个人资料在 AMS 中设置权限

AMS 使用 AWS Identity and Access Management (IAM) 来管理用户、安全证书（例如访问密钥）以及控制用户和应用程序可以访问哪些 AWS 资源的权限。AMS 提供默认 IAM 用户角色和默认 Amazon EC2 实例配置文件（其中包括允许资源访问默认 IAM 用户角色的声明）。

请求新的 IAM 用户角色或实例配置文件

AMS 使用 IAM 角色通过您的联合身份验证服务设置用户权限，并使用 IAM 实例配置文件作为该 IAM 角色的容器。

您可以使用部署 | 高级堆栈组件 | 身份和访问管理 (IAM) Access Management | 创建实体或策略 (需要审查) 更改类型 (ct-3dpd8mdd9jn1r) 申请自定义 IAM 角色，也可以使用管理 | 应用程序 | IAM 实例配置文件 | 创建 (需要审查) 更改类型 (ct-0ixp4ch2ch2r) 申请自定义 IAM 实例配置文件 tiu04)。请参阅本节中每种方法的描述。

Note

AMS 有一个 IAM 策略，`customer_deny_policy`可以屏蔽危险的命名空间和操作。默认情况下，此政策附加到所有 AMS 客户角色，用户很少会遇到问题。您的 IAM 用户和角色请求不包含此策略，但是在 IAM 角色的请求`customer_deny_policy`中自动包含有助于 AMS 更快地部署新的 IAM 实例配置文件。您可以请求排除该`customer_deny_policy`政策。但是，此请求将经过严格的安全审查，并且出于安全原因很可能被拒绝。

使用 IAM 角色策略声明限制权限

AMS 使用 IAM 角色通过您的联合身份验证服务设置用户权限。

单账户登录区 AMS：请参阅 [SALZ：默认 IAM 用户角色](#)。

多账户登录区 AMS：请参阅 [MALZ：默认 IAM 用户角色](#)。

IAM 角色是一个 IAM 实体，它定义了一组用于提出 AWS 服务请求的权限。IAM 角色未与特定用户或群组关联。相反，可信实体扮演角色，例如 IAM 用户、应用程序或 Amazon 等 AWS 服务 EC2。有关更多信息，请参阅 [IAM 角色](#)。

您可以通过使用 AWS 安全令牌服务 (STS) API 操作 [AssumeRole](#) 在 Policy 请求字段下传递限制性更强的 IAM 策略，缩小担任 AMS IAM 用户角色的用户所需策略范围。

接下来提供了可用于限制 CT 访问的策略声明示例。

使用您配置的 Active Directory (AD) 群组和 AWS Security Token Service (STS) API 操作 [AssumeRole](#)，您可以为某些用户或群组设置权限，包括限制对某些更改类型的访问权限 (CTs)。您可以使用下面显示的政策声明以各种方式限制 CT 的访问权限。

默认 IAM 实例配置文件中的 AMS 更改类型声明允许访问所有 AMS API 调用 (amscm 和 amsskms) 和所有更改类型 :

```
{
  "Sid": "AWSManagedServicesFullAccess",
  "Effect": "Allow",
  "Action": [
    "amscm:*",
    "amsskms:*"
  ],
  "Resource": [
    "*"
  ]
}
```

1. 仅允许访问和指定两个操作的声明 CTs , 其中 “操作” 是 AMS API 操作 (要 amscm 么是 amsskms) , “资源” 代表现有的变更类型 IDs 和版本号 :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "amscm:*",
      "Resource": [
        "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
        "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
      ]
    }
  ]
}
```

2. 仅允许访问 CreateRfc UpdateRfc、和的语句仅指定 SubmitRfc 了两个 CTs :
3. 允许访问 CreateRfc UpdateRfc、和所有可用内容 SubmitRfc 的声明 CTs :
4. 拒绝对受限 CT 的所有操作进行访问并允许对其他操作进行访问的声明 CTs :

使用 EC2 Amazon IAM 实例配置文件限制权限

IAM 实例配置文件是 IAM 角色的容器，您可以使用该容器在 EC2 实例启动时将角色信息传递给 Amazon 实例。

目前有一个 AWS Managed Services (AMS) 默认实例配置文件 `customer-mc-ec2-instance-profile`，它向在实例上运行的应用程序授予权限，而不是向登录该实例的用户授予权限。如果您想在不向其他实例授予访问权限的情况下授予实例访问权限，则可能需要修改默认实例配置文件或创建新的实例配置文件。您可以使用管理 | 应用程序 | IAM 实例配置文件 | 创建更改类型 (ct-0ixp4ch2tiu04) 申请新的 IAM 实例配置文件。提交 RFC 时，您可以创建自己的实例配置文件并将其添加为 `InstanceProfileDescription`，也可以直接通知 AMS（使用相同的字段）您想要进行哪些更改。由于这是手动 CT，因此 AMS 必须批准变更并将就此与您联系。

如果您不熟悉 Amazon IAM 政策，请参阅 [IAM 政策概述](#) 了解重要信息。还有一篇不错的博客文章《[揭开 EC2 亚马逊资源级权限的神秘面纱](#)》。请注意，AMS 目前不支持基于资源的访问控制，但支持使用 IAM 角色策略进行资源级控制（有关区别的解釋，请参阅[与 IAM 配合使用的 AWS 服务](#)）。

单账户着陆区 AMS：

要查看默认 AMS IAM 实例配置文件授予的权限表，请转到 [EC2 IAM 实例配置文件](#)。

AD FS 声明规则和 SAML 设置

ActiveDirectory AWS Managed Services (AMS) 的联合服务 (AD FS) 声明规则和 SAML 设置

有关如何安装和配置 AD FS 的详细 step-by-step 说明，请参阅[使用 Windows Active Directory、ADFS 和 SAML 2.0 启用与 AWS 的联合](#)。

ADFS 声明规则配置

如果您已经有 ADFS 实现，请进行以下配置：

- 依赖方信任
- 索赔规则

信赖方信任和索赔规则的步骤是从“[使用 Windows Active Directory、AD FS 和 SAML 2.0 为 AWS 启用联合身份验证](#)”博客中介绍的

- 索赔规则：
 - Nameid：每篇博客文章的配置

- RoleSessionName: 按如下方式进行配置
 - 声明规则名称：**RoleSessionName**
 - 属性存储：**Active Directory**
 - LDAP 属性：**SAM-Account-Name**
 - 发出的索赔类型：**https://aws.amazon.com/SAML/Attributes/RoleSessionName**
 - 获取 AD 组：[每篇博客文章](#)的配置
 - 角色声明：按如下方式进行配置

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^\d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =  
  RegExReplace(c.Value, "AWS-([^\d]{12})-", "arn:aws:iam::$1:saml-provider/  
  customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Web 控制台

您可以使用以下链接访问 AWS Web 控制台，将其[\[ADFS-FQDN\]](#)替换为 ADFS 实施的 FQDN。

[https://\[ADFS-FQDN\]/adfs/ls/IdpInitiatedSignOn.aspx](https://[ADFS-FQDN]/adfs/ls/IdpInitiatedSignOn.aspx)

您的 IT 部门可以通过组策略将上述链接部署到用户群中。

使用 SAML 访问 API 和 CLI

如何使用 SAML 配置 API 和 CLI 访问权限。

python 软件包来自以下博客文章：

- NTLM：[如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问](#)
- 表单：[如何使用 SAML 2.0 实现联合 API/CLI 访问的通用解决方案](#)
- PowerShell：[如何使用 Windows 设置对 AWS 的联合 API 访问权限 PowerShell](#)

脚本配置

1. 使用 Notepad++ 将默认区域更改为正确的区域

2. 使用 Notepad++，为测试和开发环境禁用 SSL 验证
3. 使用 Notepad++ 配置 idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?  
loginToRp=urn:amazon:webservices
```

Windows 配置

以下说明适用于 python 软件包。生成的证书将在 1 小时内有效。

1. [下载并安装 python \(2.7.11\)](#)
2. [下载并安装 AWS CLI 工具](#)
3. 安装 AMS CLI :
 - a. 下载您的云服务交付经理 (CSDM) 提供的 AMS 可发行文件 zip 文件并解压缩。

提供了几个目录和文件。
 - b. 根据您的操作系统，打开托管云分发文件-> CLI-> Windows 或托管云发行文件-> CLI-> Linux/macOS 目录，然后：

对于 Windows，请执行相应的安装程序（此方法仅适用于 Windows 32 或 64 位系统）：
 - 32 位：ManagedCloudAPI_x86.msi
 - 64 位：ManagedCloudAPI_x64.msi
对于 Mac/Linux，请执行名为 MC_CLI.sh 的文件。你可以通过运行这个命令来做到这一点：sh MC_CLI.sh。请注意，amscm 和 amsskms 目录及其内容必须与 MC_CLI.sh 文件位于同一个目录中。
 - c. 如果您的公司证书是通过与 AWS 的联合身份验证（AMS 默认配置）使用的，则必须安装可以访问您的联合身份验证服务的凭证管理工具。例如，您可以使用此 AWS 安全博客[如何使用 SAML 2.0 和 AD FS 实现联合 API 和 CLI 访问](#)来帮助配置您的凭证管理工具。
 - d. 安装完成后，运行aws amscm helpaws amsskms help并查看命令和选项。
4. 下载所需的 SAML 脚本

下载到 c:\aws\scripts

5. [下载 PIP](#)

下载到 c:\aws\downloads

6. 使用 PowerShell，安装 PIP

```
<pythondir>。 \ python.exe c:\aws\downloads\get-pip.py
```

7. 使用 PowerShell，安装 boto 模块

```
<pythondir\ scripts>pip 安装启动器
```

8. 使用 PowerShell、安装请求模块

```
<pythondir\ scripts>pip 安装请求
```

9. 使用 PowerShell、安装请求安全模块

```
<pythondir\ scripts>pip 安装请求 [安全]
```

10. 使用 PowerShell，安装 beautifulsoup 模块

```
<pythondir\ scripts>pip 安装 beautifulsoup4
```

11. 使用 PowerShell，在用户配置文件中创建一个名为 .aws 的文件夹 (%userprofile%\ .aws)

```
mkdir .aws
```

12. 使用 PowerShell，在 .aws 文件夹中创建凭证文件

新物品凭证类型文件 —force

凭证文件不能有文件扩展名

文件名必须全部为小写并具有名称凭证

13. 使用记事本打开凭证文件并粘贴以下数据，指定正确的区域

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

14. 使用 PowerShell SAML 脚本和登录

```
<pythondir>。 \ python.exe c:\aws\scripts\samlapi.py
```

用户名 : [用户名] @upn

选择你想担任的角色

Linux 配置

生成的证书将在 1 小时内有效。

1. 使用 WinSCP 传输 SAML 脚本
2. 使用 WinSCP 传输根 CA 证书 (对于测试和开发 , 请忽略)
3. 将 ROOT CA 添加到受信任的根证书中 (对于测试和开发 , 请忽略)

```
$ openssl x509-inform der-in [certname] .cer out certificate.pem ( 测试和开发时忽略 )
```

将 certificate.pem 的内容添加到/etc/ssl/certs/ca-bundle.crt 文件的末尾 (对于测试开发人员来说忽略)

4. 在 home/ec2-user 5 中创建.aws 文件夹

```
[default]
output = json
region = us-east-1
aws_access_key_id =
aws_secret_access_key =
```

5. 使用 WinSCP 将证书文件传输到.aws 文件夹
6. 安装 boto 模块

```
$ sudo pip 安装启动程序
```

7. 安装请求模块

```
$ sudo pip 安装请求
```

8. 安装漂亮的汤模块

```
$ sudo pip 安装 beautifulsoup4
```

9. 将脚本复制到 home/ec2-user

设置所需的权限

执行脚本：samlapi.py

使用网络 ACL 进行限制

网络访问控制列表 (NACL) 是您的 VPC 的可选安全层，它充当防火墙，用于控制进入一个或多个子网的流量。您可以使用 ACLs 与您的安全组相似的规则来设置网络，以便为您的 VPC 增加额外的安全层。有关安全组和网络之间差异的更多信息 ACLs，请参阅[安全组和网络 ACLs 的比较](#)。

但是，在 AMS 托管多账户着陆区中，为了让 AMS 有效地管理和监控基础设施，其使用 NACLs 仅限于以下范围：

- NACLs 不支持多账户 Landing Zone 核心账户，即管理账户、联网、共享服务、日志和安全。
- NACLs 支持多账户登录区域应用程序账户，前提是这些账户仅用作“拒绝”列表并具有“全部允许”以允许 AMS 监控和管理操作。

在大规模的多账户环境中，您还可以利用集中式出口防火墙等功能来控制出站流量和/或 AMS 多账户着陆区中的 Tr AWS Transit Gateway 路由表来隔离网络流量。VPCs

Outposts 上的 AMS

[AWS Outposts](#) 是一种托管硬件解决方案，可将 AMS 托管着陆区扩展到客户数据中心。开启 AMS 支持后 AWS Outposts，寻求 AMS 提供的云专业知识、成本节省和标准化平台的客户将不再局限于在内部托管资源 AWS 区域。开启 AMS 后 AWS Outposts，有本地需求的客户现在可以进行现代化改造 AWS，同时享受 AMS 提供的修补、备份、配置、事件管理、业务连续性和成本优化服务。

在您 AWS Outposts 的 AMS 多账户着陆区或单账户着陆区账户中激活后，您就可以按照现有的 AMS 变更管理流程来配置和管理 AWS 资源。可以通过指定您的 AWS Outposts 特定子网来管理 AMS 托管的基础架构。AWS Outposts 生命周期可以直接在 AWS Outposts 控制台使用 AWS Outposts 自行配置服务角色进行管理。

有关该角色的信息，请参阅[AWS Outposts](#)。

AWS Outposts 安装和运营管理

正在进行的 AMS 入职 AWS Outposts 流程包括：

1. Outposts 规划
2. 订单验证

3. Outposts 加入 AMS

4. 生命周期管理

AWS Outposts 规划

在 AWS Outposts 规划期间，您可以根据 AWS Outposts 用例确定 AMS，并与关键利益相关者（包括您的 AMS 客户团队和 AWS Outposts 代表）接触，以协调容量策略。

1. 确定需要开启 AWS Outposts AMS 的用例后，请联系您的 AMS 客户团队讨论容量规划。
2. 确定您的 AWS Outposts 容量要求后，您的 AMS 客户团队会与 AWS Outposts 服务团队接触，讨论 AWS Outposts 入职计划、角色和职责。在此期间，将为您分配 AWS Outposts 单一联系人 (SPOC)。AWS Outposts SPOC 协助最终确定 AWS Outposts 规模要求。

AWS Outposts 订单验证

在订单验证期间，您可以创建一个 AWS Outposts 站点，然后直接在 AWS Outposts 控制台中或通过您的 AWS Outposts 客户代表订购所需的容量。

一旦您（AMS 客户团队）与团队达成一致，您就可以使用更改类型 ID ct-3qe6io8t6jtny 请求 AWS Outposts 自行配置的服务角色来创建您的网站并直接在控制台中订购。AWS Outposts AWS Outposts AWS Outposts

或者，您可以通过 AWS Outposts SPOC 创建前哨基地和订单。在网站和订单验证以及 AWS Outposts 安装期间，您的 AWS Outposts SPOC 仍将向您和 AMS 客户团队提供状态更新。

AWS Outposts 加入 AMS

在 AMS 托管 VPC 中激活 AWS Outposts 设备后，您可以请求创建监控器来跟踪 Outposts 硬件的可用性、容量、异常情况和网络连接。按照下文所述的监控部署步骤进行操作，AMS 会主动监控您的 AWS Outposts 硬件。

1. 安装并激活后，您可以使用“管理 | 其他 | 其他 | 其他 | 创建 (ct AWS Outposts-1e1xtak34nx76)”更改类型提交以下模板和 RFC，请求特定监控。AWS Outposts AMS 操作可确保在 AMS 内部工具中跟踪 AWS Outposts 子网。
 - AWS Outposts 身份证
 - 子网 CIDR
 - 推荐的 AWS Outposts 警报：
 - InstanceFamilyCapacityAvailabilityAlert

- InstanceTypeCapacityAvailabilityAlert
- EBSVolumeTypeCapacityAvailabilityAlert
- CapacityExceptionsAlert
- 直接连接 ConnectionAlert
- 对于上述每个警报，请指定以下参数：
 - 统计数据（建议使用“平均值”。其他选项包括总和、最大值、最小值、样本数和 p90）
 - 时长（建议使用“5 分钟”）。其他选项包括 10 和 30 秒、1、5 和 15 分钟、1 和 6 小时以及 1 天）
 - 阈值类型（建议使用“静态”。“异常”也是选项。）
 - 条件（“每当呼叫计数大于”、“等于”、“小于”也是选项。）
 - 默认情况下，“条件值”（“25%”）已配置。允许使用另一个正整数。）
 - 通知主题（AMS 操作主题是自动分配的。但是，也可以添加任何其他主题或自定义主题。）

2. 监控和运营 Support

- AMS 运营部门监控网络断开连接或组件故障的 AWS Outposts 指标。AMS 运营部门为 AWS Outposts 问题提供第一响应服务，并在需要时升级到高级支持或 EC2 支持。
 - AMS 操作可用于解决与您的 AWS Outposts 设备有关的问题。
3. 当 EC2 实例状态或系统状态检查失败时，AMS 操作会按照现有流程使实例恢复在线状态。如果重启失败或 AWS Outposts 容量不足，AMS 运营团队成员会直接通知您以确定后续步骤。

AWS Outposts 生命周期管理

登录您的 AMS 账户后 AWS Outposts，如果出现任何可用性、容量或网络异常，您就会收到通知。您可以 AWS Outposts 直接通过 AWS Outposts 控制台或 AWS Outposts SPOC 停用。

您可以使用 AWS Outposts 自助配置服务角色或开发人员模式 AWS Outposts 直接在 AWS Outposts 控制台中进行管理。您也可以 AWS Outposts 通过 CSDM 或 AWS Outposts 单一联系人 (SPOC) 提出申请。

通过部署两个或更多 AWS Outposts AWS Outposts 可以实现开启的高可用性。配置两个或更多实例可为您的 Amazon Relational Database Service 实例 AWS Outposts 启用多可用区域选项。

在上配置 AMS 托管资源 AWS Outposts

在 AMS 账户 AWS Outposts（例如亚马逊、亚马逊 EMR EC2、Amazon EMR、Amazon EKS、Amazon ECS、Amazon EBS 和 Amazon S3）（单账户着陆区、多账户着陆区和加速账户）

中托管的 AWS 资源受与中的资源相同的 AMS 支持级别的约束。AWS 区域您可以使用 AMS 变更管理、自助配置服务或开发人员模式来创建和修改在上创建的资源 AWS Outposts。

目前，所有实例类型 (m5/m5d、c5/c5d、r5/r5d、i3en、g4dn)、亚马逊弹性区块存储、亚马逊弹性容器服务、亚马逊弹性容器服务、亚马逊弹性 Kubernetes Service、亚马逊 EMR、亚马逊关系数据库服务、应用程序负载均衡器和 App Mesh Envoy 代理均可直接在上使用。DBs AWS Outposts 这些资源有资格获得与现有地区资源相同的 AMS 运营支持。

AMS 开启的局限性 AWS Outposts

- 对 AWS Outposts 托管资源的运营支持取决于一致的网络连接。AWS Outposts 网络断开会阻止 AMS 操作部门对断开连接的 AWS Outposts 设备上发生的任何事件或问题进行故障排除。有关 AWS Outposts 服务级别突发事件的 AMS，请参阅更新的 [AWS 服务级别协议 \(SLAs\)](#)。
- 亚马逊 Relational Database Service :
 - 默认情况下，创建 RDS 更改类型 (ct-2z60dyvto9g6c) 启用多可用区并且需要数据库子网组。数据库子网组需要两个子网位于两个不同的可用区 (AZ) 中。如果您只有一个 AWS Outposts，那么创建数据库子网组是个问题，AWS Outposts 因为只能分配给单个 AZ。要规避此限制，请按照以下说明进行操作：
 1. 使用管理 | 其他 | 其他 CT 通过 RFC 请求数据库子网组，并在上指定子网。AWS Outposts
 2. 创建用于部署 RDS 的自定义 CFN 模板 AWS Outposts，并指定在上一步中创建的子网组。要了解有关执行此操作的更多信息，请参阅 [自定义资源](#)。
 3. 请求 AMS 通过 AMS CFN 提取 CT (ct-36cn2avfrj9v) 部署包含目标 RDS 实例的 CFN 模板。
 4. 请注意，由于 RDS 服务的限制，RDS for 目前 AWS Outposts 不提供指标和日志。
 - Workload ingest (WIGs) : WIGs 仅当预 WIGs EC2 实例位于非 AWS Outposts 子网上时，Linux 才起作用。原因是因为 Linux 默认使用 m4.larg WIGs e 在第一个 EC2 实例的子网中 WIGs 创建一个节点。由于 AWS Outposts 没有该实例类型，WIGs 因此无法启动其工作节点。解决方法是在非 AWS Outposts 子网中创建初始 EC2 实例，然后可以在上创建目标实例 AWS Outposts。此外，目前仅支持基于 Nitro 的 EC2 实例类型，包括 C5、c5d、M5、m5d、R5、R5d、G4 和 i3en。AWS Outposts
 - 亚马逊 Elastic Block Store (EBS) : 创建 EBS 卷 CT (ct-16xg8qguovg2w) 不起作用，因为卷是在中创建的，而不是因为我们 AWS Outposts 没有提供亚马逊资源编号 (ARN) AWS 作为 CT 的输入参数。AWS Outposts
 - 网络连接：网络连接是每个 AWS Outposts 团队的责任。
 - Brownfield 和账户接管：由于账 AWS Outposts 单的性质和企业支持要求，在非 AMS 账户中 AWS Outposts 激活的账户无法过渡到 AMS。

AMS 关于 AWS Outposts 合规性

AMS 关于 AWS Outposts 合规性认证

AWS Outposts 控制平面已被证明符合HIPAA标准，符合PCI和ISO标准。但是，AWS Outposts 控制飞机上的AMS尚未得到证实。AWS Outposts因此，我们鼓励客户寻求环境合规性认证 AMS。

AWS Outposts

为了控制 Outpost 单元上的资源创建，我们鼓励客户隔离开发者对 Outpost 的访问权限，以防止开发者在标准 AMS 托管账户中获得过多的访问权限。

需要符合 FedRAMP 标准的 AMS 托管工作负载

最重要的是，必须首先对AMS管理账户进行监管合规性评估，因为控制平面数据将流 AWS Outposts 出AMS管理账户。

如果需要 FedRAMP 认证且 AMS 账户结构合规，则建议您选择已获得所需认证并拥有所有服务链路设备（或者已经加密出口数据）的数据中心供应商。

最后，通过与您的客户团队合作部署 SCP，可以将数据限制在托管 Outpost 的账户中，AWS Outposts 并防止在托管 Outpost 的账户中创建任何区域内资源，从而实现额外的数据保护。

对 AMS 账户现有合规性的影响

只要 AWS Outposts 不使用任何受监管的数据并且该账户在逻辑上是分开的，则无需重新测试该账户的合规性。只要跨账户和入口/出口数据流相互隔离，AMS 管理账户就可以管理不受监管 authentication/authorization 和监管的账户。VPCs因此，即使不合规的 Outpost 账户和现有的合规应用程序账户都在同一个组织中（包括共享服务、联网、日志、主账户、安全 AMS 服务），但由于数据在逻辑上是分开的，合规性应用程序账户仍保持合规性。

AMS 开启 AWS Outposts FAQs

哪些用例有资格获得 AMS 支持 AWS Outposts？

需要成熟的云运营模式的企业 AWS Outposts 可以利用 AMS 开启，这些企业的工作负载需要低延迟（例如工厂机器人管理和大型机迁移）、边缘计算（例如远程工作站和边缘数据精简）以及大量数据传输负载。

为什么应该使用此功能？

AMS 提供 AWS Outposts 硬件监控和对任何 AWS Outposts 硬件问题的第一响应。此外，以下功能支持托管的所有托管资源 AWS Outposts：

- 记录、监控、护栏和事件管理
- 连续性管理
- 安全和访问管理
- 补丁管理
- 变更管理
- 自动化和自助式资源调配管理
- 事件和问题管理
- 报告 (AMS 开启后，最初不支持 AWS Outposts 硬件报告 AWS Outposts)
- 服务请求管理
- 开发者模式
- 企业 Support

如何使用此功能？

AWS Outposts 规划：在 AWS Outposts 规划期间，您已经确定了 AWS Outposts 用例中的 AMS，并将与关键利益相关者（包括 AMS 客户团队和 AWS Outposts 代表）接触，以协调容量战略。

订单验证：在订单验证期间，您可以创建一个 AWS Outposts 站点，然后直接在 AWS Outposts 控制台中或通过您的 AWS Outposts 客户代表订购所需的容量。

AWS Outposts 加入 AMS：在 AMS 托管 VPC 中激活您的 AWS Outposts 设备后，您可以使用 AMS 用户指南 () 中的模板提交变更申请 (RFC)，请求将您的设备加入 AMS 账户。AWS Outposts [AWS Outposts](#) 然后，AMS 运营部门使用 RFC 上提供的输入创建子网并监视您的前哨基地。

生命周期管理：登录您的 AMS 账户后 AWS Outposts，您会收到任何可用性、容量或网络异常的通知。您可以 AWS Outposts 直接通过 AWS Outposts 控制台或 AWS Outposts 单点联系人 (SPOC) 停用。

AMS 开启的局限性有哪些 AWS Outposts 些？

AMS 上的数据驻留（例如，特定国家/地区的数据本地化法律等）用例尚未经过验证 AWS Outposts。

AWS Outposts 由于账 AWS Outposts 单的性质和 Enterprise Support 要求，在非 AMS 账户中激活的账户无法过渡到 AMS。

AWS Outposts 控制平面已被证明符合HIPAA标准，符合PCI和ISO标准。但是，AWS Outposts 控制飞机上的AMS尚未得到证实。AWS Outposts因此，我们鼓励客户寻求环境合规性认证 AMS。

AWS Outposts

我可以选择退出此功能吗？

在 AMS 环境 AWS Outposts 中进行配置是可选的。部署到您的 AMS 账户后，如果不再需要，AWS Outposts 可以随时通过 AWS Outposts 控制台取消配置。

AMS 开启 AWS Outposts 将如何计费？

AMS AWS Outposts 费用上调将适用于 B 组等级。

AMS 服务等级协议将如何变更以适应 AWS Outposts？

事件管理将视 AWS Outposts 可用性而定。AWS Outposts 可用性取决于客户的网络可用性，这是客户的责任。AWS Outposts 可用性还取决于 AWS Outposts 硬件的正常运行时间，这取决于 AWS Outposts 服务级别协议。

另请参阅[AWS Outposts FAQs](#)。

在 AMS 中使用标签

主题

- [AMS 基础设施自动标记](#)
- [AMS 推荐的标签](#)
- [标记批量更新注意事项](#)

提供标签可能非常有价值。如需深入了解，请阅读[标记您的 Amazon EC2 资源](#)。

RFCs 创建实例（例如 Amazon S3 存储桶或 El AWS astic Load Balancer (ELB)）的实例通常会提供一个架构，允许您添加多达七个标签（键/值对）；您可以通过提交管理 | 高级堆栈组件 | Amazon S3 存储 | 更新 CT 来向 S3 存储桶添加更多标签。亚马逊 EC2、Amazon EFS、Amazon RDS 和多层（HA 双层和 HA 单层）架构最多允许 50 个标签。标签是在架构的 ExecutionParameters 部分中指定的。

使用 AMS 控制台时，必须启用其他配置视图才能添加标签。

 Tip

许多 CT 架构的架构顶部附近都有一个 Description 和 Name 字段。这些字段用于命名堆栈或堆栈组件，它们不会命名您正在创建的资源。有些架构提供参数来命名您正在创建的资源，有些则没有。例如，Create Amazon EC2 堆栈的 CT 架构不提供用于命名亚马逊 EC2 实例的参数。为此，您必须使用密钥为 “Name” 和您想要的名称的值创建一个标签。如果您未创建此类标签，则您的亚马逊 EC2 实例将显示在亚马逊 EC2 控制台中，但不带名称属性。

有标签限制吗？是：

- 标签区分大小写。
- 最大键长度为 128 个 Unicode 字符。
- 最大值长度为 256 个 Unicode 字符。
- 每个资源的最大标签数是 50。
- 预留前缀为 aws:。
- AWS 生成的标签名称和值将自动被分配 aws: 前缀，这是您无法分配的。用户定义的标签名称在成本分配报告中具有 user: 前缀。
- 每个密钥仅对每个资源使用一次。如果您尝试在同一个资源上使用相同的密钥两次，则您的请求将被拒绝。
- 允许的字符是 Unicode 字母、空格、数字和以下特殊字符：+ - = . _ /

哪些 AWS 资源类型支持标签？[立即查看通过为每个 AWS 资源使用最多 50 个标签来整理资源。](#)

AMS 基础设施自动标记

AMS 可以使用 “部署 | 高级堆栈组件 | 标记 | 创建 (需要审阅) 变更类型 (ct-0176f0n99vcps) 通过变更请求 (RFC) 在您的多账户着陆区 (MALZ) 和单账户着陆区 (SALZ) 账户中为管理目的创建的所有资源进行标记。这可以帮助您识别 AMS 为管理目的创建的资源。

AMS 可以根据命名标准自动识别 AMS 创建的资源，并检查该资源是否具有以下标签键和值-AppName “”、AppId “”、“” 和 AMSResource “” EnvironmentType。如果标签键不存在或值为空，则这些标签键可以由 AMS 自动创建，标签值为 “”。AMSInfrastructure

您可以根据贵组织的标签标准在 AMS 创建的资源上自定义所需的标签。在向 AMS 提交请求时，您可以添加自己的标签键和标签值。遵循以下 AWS 标签命名标准：[标记最佳实践](#)

Note

对于 MALZ 账户，仅应用程序账户支持 AMS 基础设施的自定义标记。目前不支持对核心账户进行自定义标记。

如果您在 RFC 中提供的标签键名称已存在于资源中，则标签值将替换为您在 RFC 中提供的新标签值。

标签键:值对的总长度不得超过 256 个字符。

使用部署 | 高级堆栈组件 | 标记 | 创建 (需要审阅) 更改类型 (ct-0176f0n99vcps) 在 RFC 中包含以下信息，用于标记 AMS 创建的资源。

1. 出于管理目的，您想在其中标记 AMS 创建的资源的多账户着陆区或单账户登录区域账户列表。
2. 必填的标签键名称和标签值 (如果需要)。默认情况下，AMS 可以将标签键名称标记为 “EnvironmentType”，将标签值标记为 “”。AMSInfrastructure[如果您需要自定义标签键名称和标签值，请遵循 AWS 标签命名标准：标记最佳实践](#)

AMS 基础设施标签目前支持这些资源：

```
API Gateway
Amazon CloudFront
Amazon DynamoDB
Amazon EBS
Amazon EC2
Amazon OpenSearch Service
Amazon Quantum Ledger Database (QLDB)
Amazon Redshift
Amazon RDS
Amazon S3 (specific buckets only*)
Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
Amazon VPC AWS Certificate Manager AWS CloudFormation AWS CloudTrail AWS CodeBuild
AWS CodePipeline AWS Elastic Beanstalk AWS Lambda AWS Secrets Manager AWS Service
Catalog AWS Systems Manager AWS WAF Regional
Elastic Load Balancing
```

* “arn: aws: s3:: awsms-a*-patch-data-*”、“arn: aws: s3:: ams-a*-log-management-*”、“arn: aws:: aws: s3:: ams-a*-backup-reports-*”、“arn: aws:: aws: s3:: ams-a*-backup-reports-*”、“arn: aws:: aws:

s3::ams-a*-backup-reports-*”、“arn:aws:s3::ams-a*-”、“arn:aws:s3::ams-a*-”、“arn:aws:s3::ams-a*-”、“arn:aws:s3::ams-a*-release-assets-*”、“arn:aws:s3::ams-a*-”、“arn:aws:s3::ams-a*-release-assets-*”、“arn:aws:s3::ams-a*-” patch-data-customer-reports patch-data-raw patch-data-reporting ams-cfn-drift-remediation ams-reporting-data-a

AMS 推荐的标签

AMS 建议在支持的资源上使用以下标签。强烈建议使用带星标的 (*) 标签。

Note

您可以使用标签来安排修补程序。有关信息，请参阅 [AMS Advanced Patch Orchestrator：基于标签的修补模型](#)。

AMS 保留的前缀

AMS 资源属性必须符合某些模式；例如，IAM 实例配置文件 BackupVault 名称、名称、标签名称等，不得以 AMS 保留前缀开头。这些保留的前缀是：

```
*/aws_reserved/*
ams-*
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
```



```
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

AMS 推荐的标签

标签键	支持的值	备注
AppName*	不受约束。	确定将驻留在资源上或需要访问该资源的应用程序。这便于 AMS 与您之间的跟踪和沟通。
AppId*		
EnvironmentType *		区分作为资源环境的开发、测试和生产基础架构。
OwnerTeamEmail *	通讯组列表电子邮件地址	确定负责该资源的团队的通讯组列表电子邮件地址。电子邮件不应是个人电子邮件；它必须是匿名电子邮件，如通讯组列表。
ComplianceFramework	不受约束	确定应将哪些控制措施和策略应用于该资源。
CostCenter		确定与资源关联的成本中心或业务部门（通常用于成本分配和跟踪）。
Customer		由拥有来自多个客户的资源的 AMS 客户（AMS 子客户）使用。将托管环境

标签键	支持的值	备注
		中的资源分组到他们所服务的特定客户中。确定特定资源或服务组上的特定客户端。
DataClassification		确定资源支持的特定数据机密级别。确定应将哪些控制措施和策略应用于该资源。
HoursOfOperation		确定应启动、停止、删除或轮换资源的日期或时间。
OwnerTeam		确定负责该资源的团队。促进与负责资源的团队的沟通。
Patch Group	您有两种选择： - 您可以使用 AMS Advanced Patch Orchestrator 中概述的信息提交服务请求：基于标签的修补模型，AMS 会在您的指定资源上创建标签，并使用您提供的信息，为您创建Patch Group标签。 - 如果您已经在资源上创建了Patch Group标签，则支持的值不受限制。	在自动修补维护窗口中应包含哪些资源。
ProjectId	不受约束	确定资源支持的项目。

标签键	支持的值	备注
SupportPriority	机密性、完整性或可用性的六种可能缩写词之一；首字母缩略词的顺序是优先级。例如，I.C.A. 意味着该命令是完整性、机密性、可用性。其他可接受的值包括 C.I.A.、C.A.I.、I.A.C.、A.C.I. 和 A.I.C.	确定应优先考虑哪种类型的支持：机密性、完整性或可用性。

标记批量更新注意事项

这些注释适用于[标记 | 批量更新](#)和[标记 | 批量更新（需要查看）](#)更改类型示例演练。

关于批量更新标签的注意事项：

- 支持的服务：
 - 对于[标签 | 批量更新（需要审核）](#)：全部。
 - 对于[标签 | 批量更新](#)：
 - Auto Scaling
 - Amazon EC2
 - Elastic Load Balancing
 - Amazon RDS
 - Amazon S3 存储桶
 - 要生成逗号分隔值 (CSV) 文件，请在 AWS 控制台中登录资源组 > 标签编辑器，找到要标记的资源，然后将其导出到 CSV 文件中。有关更多信息，请参阅[将结果导出到 CSV](#)。
- 注意：我们建议使用 S3 预签名 URL 来提供 CSV 对象位置。
- 必须有标题为“服务”、“类型”和“标识符”的列。这些列是必填的。
 - 将列标识符重命名为 ID。
 - “服务”、“类型”和“标识符”（已更改为 ID）列的值由标签编辑器在“资源组” (Resource Groups) 下提供。

- 如果标签编辑器下没有要标记的资源，请使用该资源的亚马逊资源名称 (ARN) 作为标识符 (更改为 ID) 列，并将“服务”和“类型”留空。
- 要添加或修改的标签的列标题的格式必须为 Tag: **TagKey**。
- 要删除的标签的列标题的格式必须为 Untag: **TagKey**。
- 每行用于对资源进行标记或取消标记。
- 如果要向资源添加标签，请在相应的 Tag: **TagKey** 列下指定该标签的值。
- 如果要从资源中删除标签，请在相应的 U ntag: **TagKey** 列下指定 True。
- 如果 Tag: **TagKey** 或 Untag: **TagKey** 不适用于资源，请在相应的列中添加一个破折号 (-) 或将其留空。

注意：Untag 会覆盖标签-这是因为与标签不同，Untag 需要手动添加到 CSV 文件中，因此我们假设其目的是移除而不是修改标签。

- 任何不符合条件的其他列都将被忽略。

Important

标签编辑器导出会根据所有资源填充所有标签的矩阵，缺失的标签用“未标记”的值填充。重复使用此导出 CSV 作为 RFC 的输入会导致创建所有先前缺失的标签，字面值为“未标记”。

Note

有关将标签导出到 CSV 文件的信息，请参阅[查找要标记的资源-> 将结果导出到 CSV](#)。

AWS Managed Services 资源调度器

使用 AWS Managed Services (AMS) 资源计划程序安排账户中 AutoScaling 群组、Amazon EC2 实例和 RDS 实例的自动启动和停止。在资源本来不打算全天候运行的情况下，这有助于降低基础设施成本。该解决方案建立在[实例调度器之上 AWS](#)，但包含特定于 AMS 需求的其他功能和自定义设置。

Note

默认情况下，AMS 资源调度器不与不属于 AWS CloudFormation 堆栈的资源进行交互。资源必须是以“stack-”、“sc-”或“SC-”开头的堆栈的一部分。要计划不属于 CloudFormation 堆栈的资源，可以将资源调度器堆栈参数更新ScheduleNonStackResources为Yes。

AMS 资源调度器使用周期和计划：

- 周期定义资源调度器运行的时间，例如开始时间、结束时间和当月中几天。
- 计划包含您定义的时间段以及其他配置，例如 SSM 维护窗口、时区、休眠设置等；并根据配置的时间段规则指定资源何时运行。

您可以使用 AMS 资源计划程序的自动更改类型（CTs）来配置这些时间段和计划。

有关 AMS 资源调度器可用设置的完整详细信息，请参阅[解决方案](#)组件中的相应 AWS 实例计划程序文档。有关解决方案的架构视图，请参阅 Architecture [overview.html](#) 上的相应 AWS 实例调度器文档。

部署 AMS 资源调度器

要部署 AMS 资源调度器，请使用自动更改类型 (CT)：部署 | AMS 资源调度器 | 解决方案 | 部署 (ct-0ywnhc8e5k9z5) 提出 RFC，然后在您的账户中部署解决方案。执行 RFC 后，包含默认配置的 AMS 资源调度器资源的 CloudFormation 堆栈将自动配置到您的账户中。有关资源调度器更改类型的更多信息，请参阅 [AMS 资源调度器](#)。

Note

要了解您的账户中是否已部署 AMS 资源调度器，请查看该账户的 Lamb AWS da 控制台并查找计划程序函数AMSResource。

在您的账户中配置 AMS 资源调度器后，我们建议您查看默认配置，并在需要时根据自己的偏好自定义配置，例如标签密钥、时区、计划服务等。有关推荐的自定义项的详细信息[自定义 AMS 资源调度器](#)，请参阅“下一步”。

要进行自定义配置，或者只是确认资源调度器配置，

自定义 AMS 资源调度器

我们建议您使用更新的 AMS 资源计划程序更改类型自定义 AMS 资源调度器的以下属性，请参阅 [AMS 资源调度器](#)。

- **标签名称**：资源调度器将用于将实例计划与资源关联的标签的名称。默认值为“计划”。
- **定时服务**：以逗号分隔的资源调度器可以管理的服务列表。默认值为“ec2、rds、自动缩放”。有效值为“ec2”、“rds”和“自动缩放”。
- **默认时区**：指定资源调度器要使用的默认时区。默认值为 UTC。
- **使用 CMK**：以逗号分隔的 Amazon KMS 客户托管密钥 (CMK) 列表 ARNs，可以向资源计划程序授予权限。
- **使用 LicenseManager**：以逗号分隔的 AWS 许可证管理器列表，可以 ARNs 向该资源调度器授予权限。

Note

AMS 可能会不时发布功能和修复程序，以使您的账户中的 AMS 资源调度器保持最新状态。发生这种情况时，您对 AMS 资源调度器所做的任何自定义都将保留。

使用 AMS 资源调度器

要在解决方案部署后配置 AMS 资源调度器，请使用自动资源调度器 CTs 创建、删除、更新和描述（获取有关）AMS 资源调度器周期（资源调度器运行的时间）和计划（配置的时间段和其他选项）。有关使用 AMS 资源计划程序更改类型的示例，请参阅 [AMS 资源计划程序](#)。

要选择由 AMS 资源调度器管理的资源，在创建部署和计划后，您可以使用 AMS 标签创建 CTs 来标记 Auto Scaling 组、Amazon RDS 堆栈和 Amazon EC2 资源，使用您在部署期间提供的标签密钥和定义的时间表作为标签值。标记资源后，将根据您定义的资源计划程序计划安排资源启动或停止。

使用 AMS 资源调度器不会产生额外费用。但是，该解决方案会使用多个资源，AWS 服务并且您需要为这些资源的使用付费。有关更多详细信息，请参阅[架构概述](#)。

要选择退出 AMS 资源调度器，请执行以下操作：

- 对于临时选择退出或禁用：使用自动管理 | AMS 资源调度器 | 状态 | 禁用更改类型 (ct-14v49adibs4db) 提交 RFC

- 要永久移除：提交管理层 | 其他 | 其他 | 更新 (需要审核) (ct-0xdawir96cy7k) RFC 请求从资源调度器发布自动化系统中删除

AMS 资源调度器成本估算器

为了跟踪成本节省情况，AMS 资源调度器具有一个组件，该组件每小时计算由计划程序管理的 Amazon EC2 和 RDS 资源的估计成本节约。然后，这些成本节省数据将作为 CloudWatch 指标 (AMS/ResourceScheduler) 发布，以帮助您对其进行跟踪。成本节省估算器仅估算实例运行时间节省的时间。它不考虑任何其他成本，例如与资源相关的数据传输成本。

使用资源调度器启用了成本节约估算器。它每小时运行一次，并从中 AWS Cost Explorer 检索成本和使用数据。它根据该数据计算出每种实例类型的平均每小时成本，然后预测在未计划的情况下运行一整天的成本。节省的成本是给定日期的预计成本与 Cost Explorer 的实际报告成本之间的差额。

例如，如果实例 A 的资源调度器配置为从上午 9 点到下午 5 点运行，则在给定一天中运行八个小时。Cost Explorer 将成本报告为 1 美元，使用量报告为 8。因此，每小时的平均成本为 0.125 美元。如果实例未使用资源调度器进行计划，则该实例将在当天运行 24 小时。在这种情况下，成本将为 $24 \times 0.125 = 3$ 美元。资源调度器帮助您节省了 2 美元的成本。

为了使成本节省估算器仅检索由 Cost Explorer 中的资源调度器管理的资源的成本和使用量，需要在账单控制面板中激活资源调度器用于定位资源的标签密钥作为成本分配标签。如果该账户属于某个组织，则需要在该组织的管理账户中激活标签密钥。有关执行此操作的信息，请参阅[激活用户定义的成本分配标签](#)和[用户定义的成本分配标签](#)

将标签密钥激活为成本分配标签后，AWS 计费开始跟踪资源调度器管理的资源的成本和使用情况，在这些数据可用之后，成本节省估算器开始计算节省的成本并将数据发布在中的 AMS/ResourceScheduler 指标命名空间下。CloudWatch

成本估算器提示

Cost Savings Estimator 在计算时不考虑预留实例、储蓄计划等折扣。估算器从 Cost Explorer 中提取使用成本，然后计算资源每小时的平均成本。有关更多详细信息，请参阅[“了解您的 AWS 成本数据集：备忘单”](#)

为了使成本节省估算器仅检索由 Cost Explorer 中的资源调度器管理的资源的成本和使用量，需要在账单控制面板中激活资源调度器用于定位资源的标签密钥作为成本分配标签。如果该账户属于某个组织，则需要在该组织的管理账户中激活标签密钥。有关执行此操作的信息，请参阅[用户定义的成本分配标签](#)。如果未激活成本分配标签，则即使启用了该指标，估算器也无法计算节省的费用并发布该指标。

AMS 资源调度器最佳实践

计划 Amazon EC2 实例

- 实例关闭行为必须设置为 `stop`，而不是设置为 `terminate`。`stop` 对于使用 AMS Amazon Create 自动更改类型 (ct-14027q0sjyt1h) EC2 创建的实例，通过将属性设置为，可以为通过摄取创建的 EC2 亚马逊实例将其设置为。AWS CloudFormation InstanceInitiatedShutdownBehavior `stop` 如果实例的关闭行为设置为 `terminate`，则当资源调度器停止实例并且调度器无法启动它们时，实例就会结束。
- 作为 Auto Scaling 组一部分的 Amazon EC2 实例不会由 AMS 资源计划程序单独处理，即使它们已被标记。
- 如果目标实例根卷使用 KMS 客户主密钥 (CMK) 加密，则需要向您的资源调度器 IAM 角色添加额外的 `kms:CreateGrant` 权限，以便计划程序能够启动此类实例。为了提高安全性，默认情况下不会将此权限添加到角色中。如果您需要此权限，请使用管理 | AMS 资源计划程序 | 解决方案 | 更新更改类型提交 RFC，并指定以逗号分隔的 KMS 列表。ARNs CMKs

安排 Auto Scaling 群组

- AMS 资源调度器启动或停止 Auto Scaling 组的自动扩展，而不是组中的单个实例。也就是说，调度器恢复 Auto Scaling 组的大小（开始）或将大小设置为 0（停止）。
- 使用指定标签标记 AutoScaling 组，而不是该组中的实例。
- 在停止期间，AMS 资源调度器会存储 Auto Scaling 组的最小、所需和最大容量值，并将最小和所需容量设置为 0。在启动期间，调度器会将 Auto Scaling 组的大小恢复为停止时的状态。因此，Auto Scaling 组实例必须使用适当的容量配置，这样实例的终止和重新启动就不会影响在 Auto Scaling 组中运行的任何应用程序。
- 如果在运行期间修改 Auto Scaling 组（最小或最大容量），则计划程序会存储新的 Auto Scaling 组大小，并在停止计划结束时恢复该组时使用该大小。

安排 Amazon RDS 实例

- 调度器可以在停止 RDS 实例之前拍摄快照（不适用于 Aurora 数据库集群）。默认情况下，此功能处于开启状态，创建 RDS 实例快照 CloudFormation 模板参数设置为 `true`。快照将一直保留到下次停止 Amazon RDS 实例并创建新快照为止。

调度器可以是属于集群或 start/stop Amazon RDS Aurora 数据库或多可用区（多可用区）配置的 Amazon RDS 实例。但是，当计划程序无法停止 Amazon RDS 实例（尤其是多可用区实例）时，

请检查 Amazon RDS 限制。要安排 Aurora 集群的启动或停止，请使用安排 Aurora 集群模板参数（默认为 `true`）。Aurora 集群（不是集群中的单个实例）必须使用初始配置期间定义的标签键进行标记，并将计划名称作为标签值来调度该集群。

每个 Amazon RDS 实例都有一个每周维护时段，在此期间会应用任何系统更改。在维护时段内，Amazon RDS 将自动启动已停止超过七天的实例以进行维护。请注意，维护事件完成后，Amazon RDS 不会停止实例。

计划程序允许指定是否将 Amazon RDS 实例的首选维护时段作为运行时段添加到其计划中。如果没有其他运行周期指定实例应运行，并且维护事件已完成，则解决方案将在维护时段开始时启动实例，并在维护时段结束时停止该实例。

如果维护事件在维护时段结束时仍未完成，则该实例将一直运行到维护事件完成后的计划间隔。

Note

调度程序不验证资源是否已启动或停止。它调用 API 并继续前进。如果 API 调用失败，它会记录错误以供调查。

AWS Systems Manager 在 AMS 高级版中

AWS Systems Manager 文档（SSM 文档）定义了 Systems Manager 对您的 AWS 资源执行的操作。Systems Manager 包含十几个预先配置的文档，您可以通过在运行时指定参数来使用这些文档。文档使用 JavaScript 对象表示法（JSON）或 YAML，它们包括您指定的步骤和参数。

AWS Managed Services (AMS) 是值得信赖的 SSM 文档发布商。AMS 拥有的 SSM 文档仅与已注册的 AMS 账户共享，始终以保留的前缀 (AWSManagedServices-*) 开头，并显示在 Systems Manager 控制台中，归其所有。AWS SSM 文档开发和发布的 AMS 流程遵循 AWS 最佳实践，需要在整个文档生命周期中进行多次同行评审。有关共享 SSM 文档 AWS 的最佳做法的更多信息，请参阅[共享 SSM 文档的最佳实践](#)。

可用的 AMS 高级 SSM 文档

AMS Advanced SSM 文档仅向 AMS Advanced 客户提供，用于自动化操作工作流程，从而操作您的账户。

要查看可用的 AMS 高级 SSM 文档，AWS 管理控制台请访问：

1. 在控制台打开系统管理器控制[AWS Systems Manager 台](#)。
2. 选择“与我共享”。
3. 在搜索栏中，按文档名称前缀筛选，然后按“等于”进行筛选，然后将值设置为“AWSManaged服务-”。

有关 AWS CLI 说明，请参阅[使用共享 SSM 文档](#)。

AMS 高级 SSM 文档版本

SSM 文档支持版本控制。AMS Advanced SSM 文档无法从客户的账户中修改，也无法重新共享。它们由 AMS Advanced 集中管理和维护，以便操作账户。

版本号会随着特定 AWS 区域文档的每次更新而递增。随着新区域的推出，两个区域中的相同文档内容可能具有不同的版本号；这是典型的，并不意味着它们的行为会有所不同。如果您想比较两个 AMS 高级 SSM 文档，我们建议将它们的哈希值与 CLI AWS 进行比较：

```
aws ssm describe-document \
  --name AWSManagedServices-DOCUMENTNAME \
  --output text --query "Document.Hash"
```

如果两个 SSM 文档的哈希值匹配，则它们是相同的。

AMS 中的 Systems Manager 定价

AMS 高级 SSM 文档访问不收取任何费用。运行时间成本因 SSM 文档的类型、步骤和运行时长而异。有关更多信息，请参阅[AWS Systems Manager 价](#)。

离线 AMS 账户

AMS 为单账号着陆区和多账号着陆区账户提供登机帮助。

AMS 不会在离职期间取消与您的任何 AMIs 共享信息，以免影响您的任何依赖项。如果您想 AMIs 从您的账户中移除 AMS，则可以使用 `cancel-image-launch-permission` API 隐藏特定内容 AMIs。例如，您可以使用以下脚本来隐藏之前与您的账户共享 AMIs 的所有 AMS：

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
  query 'Images[].ImageId' --output text) ;
```

```
do
aws ec2 cancel-image-launch-permission --image-id $ami ;
done
```

您必须安装 AWS CLI v2，脚本才能毫无错误地执行。有关 AWS CLI 的安装步骤，请参阅[安装或更新最新版本的 AWS CLI](#)。有关该cancel-image-launch-permission命令的详细信息，请参阅[cancel-image-launch-permission](#)。

Note

服务终止日期是必需的 30 天终止通知期结束后的日历月的最后一天。如果必要的终止通知期限在日历月的第20天之后，则服务终止日期为下一个日历月的最后一天。以下是终止日期的示例方案。

- 如果终止通知是在4月12日提供的，则为期30天的通知将于5月12日结束。服务终止日期为5月31日。
- 如果在4月29日发出终止通知，则为期30天的通知将于5月29日结束。服务终止日期为 6 月 30 日。

主题

- [从 AMS 单账户 landing zone 账户中脱颖而出](#)
- [退出 AMS 多账号 landing zone 账号](#)

从 AMS 单账户 landing zone 账户中脱颖而出

AMS 在 AMS 终止前 30 天内提供下机协助。

您必须在提供此类协助前至少 7 天申请下机协助。离职援助可以通过两种形式提供：

- 控制权移交：AMS 将账户控制权以及所有 AMS 管理的应用程序的访问凭证移交给您，或者
- 因账户关闭而终止资源：AMS 会删除 AMS 管理的环境中的所有数据，并取消配置账户中的所有活动资源。提交离职申请时，客户可以要求 AMS：
 - 删除或保留存储在 Amazon S3 存储桶中的数据对象（包括日志）
 - 移除或保留 Amazon S3 存储桶
 - 移除或保留 AWS Backup 还原点

 Important

在初始化离职之前，必须将任何其他具体请求（视合理性而定）传达给 AMS。

可选先决条件（如果需要）：

 Note

在提出离线请求之前，客户可以请求 AMS 协助，使用 AWS Snowball Edge 或与之 AWS 接口的任何其他媒体以现有格式传输您的数据。

除了数据备份外，还可以提供以下客户数据作为离职帮助的一部分：

- 存储在存储服务中的数据，包括日志
- 客户特定的变更类型架构
- CloudFormation 更改类型架构的模板

如果在 AMS 终止后未完成离职活动，我们会移交账户控制权，以便您能够完成任何待处理的活动。

函数	删除了什么	影响	需要采取的行动
监控、记录、警报	AMS 监控已移除 MMS（托管监控系统）已取消订阅 已移除资源标记器和警报管理器 基线 CloudWatch 警报仍保留在现有资源上	AMS 无法再访问或查看您的资源和环境。	已删除和取消订阅服务的意外开支归您所有。

函数	删除了什么	影响	需要采取的行动
	GuardDuty 还有 Macie：所有权归您所有		
备份管理	AMS Backup 自动化功能已移除，但该 AWS Backup 服务仍可供使用。除非请求删除，否则会保留备份存储库和数据。	AMS 不再监控备份任务或在事件发生期间执行恢复操作。警报和警报已禁用。删除 IAM 备份角色和 KMS 密钥会使您的 AMS 备份无法运行。	必须重新配置 AMS Backup 计划。所有监控和补救所有权都归您所有。
用于服务管理的 AMS 自动化	AMS 策划的 AWS SSM 自动化运行手册、亚马逊简单通知服务 (SNS) Simple Notification Service 和 Lambda 函数已不再可用。AWS	没有 AMS 访问您的账户的权限。禁用所有自动化。	如果需要，需要重新创建包括 SSM、SNS 和 Lambda 函数在内的所有自动化功能。
合规	AMS 对所有人的可见性和监视 GuardDuty 以及 AWS Config 规则已删除，但这些规则仍保留在账户上。	Amazon and Ru AWS Config 中的所有监控、报告 GuardDuty 和补救措施都不再由 AMS 管理。	对所有安全和合规性工具进行监控和补救，由您自己掌握。
实例代理	删除了访问资源调度器、资源标记器或自动实例配置以在您的 EC2 实例中安装所需代理的权限。	CloudWatch 而且，实例上的 SSM 代理保留在现有配置中，但是 AMS 不再为这些配置提供帮助。	您可以管理标记、实例 CloudWatch 和 SSM 代理配置。

函数	删除了什么	影响	需要采取的行动
修补和报告基础架构	AMS 不再管理修补前和修补后的活动，对这些服务的访问和可见性也被移除。	AMS 不再在修补之前创建实例的快照，也不再安装和监控补丁安装，也不会再将结果通知您。应您的要求，报告和“审计” S3 存储桶会保留在您的账户中。AMS 不再生成服务指标报告。	您可以保留过去创建的补丁基准和快照。此外，补丁维护窗口的配置保持不变，但是 AMS 不再安装或修复补丁。现在，所有基础设施运营指标的报告均由您负责。
进程管理	所有账户都脱离了为事件提供的服务管理，包括服务请求、问题和变更管理。	AMS 以前通过事故和服务请求、环境变化以及根本原因调查修复的所有服务中断都将由 AMS 管理。	您重新获得所有流程管理的全部所有权。

退出 AMS 多账号 landing zone 账号

您可以从 AMS Advanced 多 AWS 账号登陆区移出两种类型的账户：

- 应用程序账户
- 核心账户

要从 AMS Multi-Account landing zone 中移出所有账户，您必须先关闭所有应用程序账户，然后才能退出核心账户。

要接管并继续操作已离线的应用程序或核心账户中的工作负载，请务必与 AMS 客户团队一起查看此文档。本文档概述了 AMS 在机外流程中执行的更改。

需要完成的任务，才能继续操作已离线账户

要继续操作从 AMS 多账户 landing zone 下线的账户，需要执行以下任务：

- 开启开发者模式：要获得更多账户权限，请在从 AMS 中移除应用程序账户之前开启开发者模式。开启开发者模式后，您可以更轻松地进行必要的更改，为下线做好准备。不要尝试移除或修改 AMS 基

基础设施资源。如果您删除 AMS 基础设施资源，那么 AMS 可能无法成功退出您的账户。有关如何启用开发者模式的信息，请参阅[AMS 高级开发者模式入门](#)。

如果您在开启开发者模式后无法完成必要的更改以准备下线，请联系您的 AMS 客户团队讨论您的要求。

- 选择另一种访问 EC2 堆栈的方法：从 AMS 中移除应用程序帐户后，您将无法使用 RFCs 访问堆栈资源。查看[离职变更](#)，然后选择其他访问方法，这样您就可以保留对堆栈的访问权限。有关更多信息，请参阅[访问替代方案](#)。

离线 AMS 应用程序账户

要将应用程序帐户从您的多账户 landing zone 环境中移除，请为每个账户完成以下步骤：

1. 确认账户 RFCs 中没有未开户。有关更多信息，请参阅[创建、克隆、更新、查找和取消 RFCs](#)。
2. 确认您可以访问该账户的主用户或根用户电子邮件地址。
3. 在申请账户中，使用[申请账户 | 确认离职 \(ct-2wlfo2jxj2rkj\) 变更](#)类型提交 RFC。在 RFC 中，指定要移除的应用程序帐户。
4. 在管理账户中，使用管理账户[Offboard 应用程序账户 \(ct-0vdiy51oyrh\)](#)的变更类型提交 RFC。在 RFC 中，指定要移除的应用程序帐户。此外，请指明您是要删除还是保留与着陆区的公网连接。
5. 要确保 AMS 账单已停止，请通知您的 CSDM 您已注销该账户。

在应用程序帐户注销后，会发生以下情况：

- 所有组件都与 AMS 服务解除关联，但您创建的资源仍保留在账户中。您可以选择保留或关闭 AMS 离线账户。
- 应用程序账户注销后，核心账户和其他剩余的应用程序账户可以正常运行。
- AMS 账单已停止，但在您关闭账户后才会停止 AWS 计费。如[需了解更多信息，请参阅关闭账户前须知事项](#)。
- 如果账户已关闭，则该账户将在 90 天内在该suspended州的组织中可见。90 天后，已关闭的账户将被永久删除，并且在您的组织中不再可见。
- 账户关闭后，您仍然可以登录并在 90 天内提交支持案例或联系方式 支持。
- 90 天后，账户中保留的所有内容都将被永久删除，剩余的 AWS 服务也将终止。

应用程序账户注销常见问题解答

问：我能否使用我的联合 IAM 角色继续访问我从 AMS 多账户登陆区域下线的应用程序账户？

是。AMS 创建的[默认 AWS Identity and Access Management \(IAM\) 角色](#)在 AMS 离职后仍可在账户中使用。但是，这些角色和策略是为与 AMS 访问管理一起使用而设计的。要为您提供必要的访问权限，您可能需要部署自己的 IAM 资源。

问：如何获得从我的 AMS 多账户 landing zone 下线的应用程序账户的完全访问权限？

已移除的应用程序账户将移至账户结构中的已弃用组织单位 (OU)。AWS Organizations 此举解除了之前阻止 root 用户访问的 SCP 访问限制。有关如何重置 root 用户凭证的信息，请参阅[重置丢失或忘记的 root 用户密码](#)。

问：在应用程序账户注销期间进行了哪些更改？

有关 AMS 在服务关闭账户时所采取的操作的信息，请参阅[离职变更](#)。

问：我能否在不将应用程序账户与公网网关断开的情况下将其从中断开连接？

是。使用[管理账户 | Offboard 应用程序账户](#) (ct-0vdiy51oyrh) 更改类型提交 RFC，并将参数指定为 DeleteTransitGatewayAttachment False

问：注销应用程序账户需要多长时间？

当你使用[管理账户 | Offboard 应用程序账户](#) (ct-0vdiy51oyrh) 更改类型时，请在 1 小时内完成 RFCs

问：我是否必须关闭离职账户？

不是。AMS 下线后关闭账户不是强制性的。在离职过程中，AMS 会移除其对您 AWS 账户的访问和管理权限，但您的账户和账户中的资源仍然存在。请务必注意，AMS 离职后，您全权负责管理和维护自己的 AWS 账户和资源。在离职流程完成后，AMS 对您的账户中可能发生的任何问题、事件或服务中断概不负责。如需了解更多信息，请参阅[如何关闭我的 AWS 账户？](#)。

问：如果我提交账户关闭请求，是否会立即删除所有现有资源？

不是。关闭账户不会终止您的资源。账户中的资源将在关闭请求 90 天后自动终止。AMS 账单会停止，但在您关闭账户之前，AWS 资源计费不会停止。如需[了解更多信息，请参阅关闭账户前须知事项](#)。

问：我能否安排应用程序账户的注销？

是。您可以安排 RFCs 在特定时间运行。但是，[申请账户 | 确认离职](#) RFC 必须先完成，然后才能安排[管理账户 | Offboard 应用程序账户](#) RFC。有关更多信息，请参阅[RFC 调度](#)。

应用程序账户离线 RACI

- R：责任方。负责完成所列任务的一方。
- 答：责任方。批准已完成任务的一方。
- C：咨询方。通常以主题专家的身份征求意见的当事方，并与之进行双边沟通。
- 我：知情方。通报进展情况的一方，通常只有在任务或可交付成果完成后才会被告知。

活动	Custome	AWS Managed Services (AMS)
先决条件		
验证将要移除的每个 AWS 账户 ID 的根电子邮件地址的访问权限	R	C
查看 AMS 关于建议客户操作的文档，并为 AMS 离职准备账户	R	C
如有必要，提交 RFC 以启用开发者模式，为 AMS 离职做好账户准备	R	我
如果需要，请选择其他 EC2 堆栈访问方法。	R	我
离职		
提交 RFCs 以确认并申请注销申请账户	R	我
从应用程序帐户中移除 AMS 组件	我	R
通知 AMS CSDM 已离线账户以停止 AMS 计费	R	我
离职后		
重置 root 用户帐户密码并验证已离线账户的 root 访问权限	R	C
关闭账户或按照 AMS 离职文档中有关建议客户操作的指导方针继续操作账户	R	C

Offboard 核心账户

要退出多账户 landing zone Core 账户，请完成以下步骤：

1. 验证 landing zone 中的所有应用程序账户是否已从 AMS 下线。
2. 确认您的账户 RFCs 中没有未平仓。有关更多信息，请参阅 [创建、克隆、更新、查找和取消 RFCs](#)。
3. 确认您可以访问所有 Core 账户的主用户或根用户电子邮件地址。有关更多信息，请参阅 [多账号着陆区账号](#)。
4. 确认您可以访问管理账户的主用户或 root 用户电话号码。使用 IAM 角色 `AWSTrustedAdvisorBillingRole` 更新电话号码。有关更多信息，请参阅 [如何更新与我的 AWS 账户关联的电话号码？](#)。
5. 登录您的 AMS landing zone 管理账户并提交 AMS 服务申请。在服务请求中，指定离开整个着陆区。

核心账户下线后会发生以下情况：

- 所有组件都与 AMS 服务断开关联，但一些 AWS 资源仍保留在账户中。您可以选择保留或关闭 AMS 已离线的 Core 账户。
- AMS 账单已停止，但在您关闭账户后才会停止 AWS 计费。如需了解更多信息，请参阅 [关闭账户前须知事项](#)。
- 如果账户已关闭，则该账户将在 90 天内在该 suspended 州的组织中可见。90 天后，已关闭的成员账户将被永久删除，并且在您的组织中不再可见。
- 账户关闭后，您仍然可以登录并在 90 天内提交支持案例或联系方式支持。
- 账户关闭 90 天后，账户中保留的所有内容都将被永久删除，剩余的 AWS 服务也将终止。

核心账户下线常见问题解答

问：我能否使用我的联合 IAM 角色继续访问已离线的 Core 账户？

是。AMS 创建的 [默认 AWS Identity and Access Management \(IAM\) 角色](#) 在离线账户中仍然可用。但是，这些角色和策略是为与 AMS 访问管理一起使用而设计的。要为您提供必要的访问权限，您可能需要部署自己的 IAM 资源。

问：退出 AMS 多账户登陆区域后，如何获得管理、共享服务、网络或其他非应用程序 [MALZ 账户](#) 的完全访问权限？

下线后，按照[重置丢失或忘记的根用户密码](#)中的说明使用主（根）用户凭据访问管理账户以外的核心账户。与其他账户类型不同，管理账户保留了与根用户关联的无法访问的多因素身份验证 (MFA) 设备，以防止使用。要重新获得根访问权限，您必须按照[丢失的 MFA 设备恢复](#)流程进行操作。

问：在核心账户离线期间进行了哪些更改？

有关 AMS 在服务关闭账户时所采取的操作的信息，请参阅[离职变更](#)。

问：核心账户下线需要多长时间才能完成？

核心账户离职流程通常需要长达 30 天才能完成。但是，为了确保正确完成所有必需的步骤，您必须在离职开始前至少 7 天提出离职申请。为了便于轻松过渡，请提前计划并提前提交离职申请。

问：AMS 下线后如何管理共享组件？

AMS 托管 Active Directory 和其他共享服务基础设施组件专为 AMS 操作员访问而设计。您可能需要更新亚马逊弹性计算云 (Amazon EC2) 安全组、AWS Organizations 服务控制策略 (SCP) 或进行其他更改以保留对这些组件的完全访问权限。

问：我能否关闭已离线的核心账户？

默认情况下，应用程序账户与 MALZ Core 账户有多种依赖关系，例如 AWS Organizations 成员资格、传输网关网络连接以及通过 AMS 托管 Active Directory 进行的 DNS 解析。解决这些依赖关系后，您可以停用并关闭已离线的 Core 账户。有关更多信息，请参阅[多账号着陆区账号](#)。

核心账户退出 RACI

- R：责任方。负责完成所列任务的一方。
- 答：责任方。批准已完成任务的一方。
- C：咨询方。通常以主题专家的身份征求意见的当事方，并与之进行双边沟通。
- 我：知情方。通报进展情况的一方，通常只有在任务或可交付成果完成后才会被告知。

活动	Custom	AWS Managed Services (AMS)
先决条件		
验证对每个将被移除的 AWS 账户 ID 的根电子邮件地址的访问权限	R	C
验证访问权限并更新管理账户的 root 用户电话号码	R	C
查看 AMS 关于建议客户操作的文档，并为 AMS 离职准备账户	R	C
离职		
提交服务请求以请求离开 landing zone	R	我
从核心账户中移除 AMS 组件	我	R
离职后		
重置 root 用户帐户密码并验证已离线账户的 root 访问权限	R	C
关闭账户或按照 AMS 离职文档中有关建议客户操作的指导方针继续操作账户	R	C

离职变更

下表描述了 AMS 在多账户 landing zone 下线时采取的措施、潜在影响和建议的措施。

组件	账户类型	为下船而采取的行动	潜在影响	建议的客户操作
访问权限管理	应用程序账户	下机后，无法再通过 AMS just-in-time 堡垒主机提交 RFCs 对有时间限制的访问堆栈的 EC2 堆栈访问权限	无法通过 RFS 使用 AMS 堡垒访问实例 EC2	使用其他方法访问 EC2 实例 (请参阅 访问替代方案)
			EC2 从提供的非 AMS 启动的实例	从现有 EC2 资源堆栈中移除 AMS 启

组件	账户类型	为下船而采取的行动	潜在影响	建议的客户操作
		AMS 不再管理任何现有 EC2 资源堆栈上与访问相关的组件 (PBIS Open 代理、域加入脚本)	AMIs 未加入托管 Active Directory 域 如果不移除，现有资源堆栈中的 AMS 启动脚本可能会因为缺少 AMS 依赖项而产生错误，并阻止重新加入其他域	动脚本 (请参阅 禁用 AMS EC2 启动脚本)
访问管理 (续)	核心账户	如果您从 PBIS Open 迁移到 PBIS Enterprise (AD Bridge)，那么在核心账户离职后，AMS 将不再续订许可	如果允许 PBIS Enterprise 许可证过期，则 Active Directory 凭据对现有的基于 Linux EC2 的实例堆栈无效	如果您迁移到 PBIS Enterprise (AD Bridge)，请决定是保留许可还是停用 (请参阅) PBIS Open/Enterprise (AD Bridge)
记录、监控、Incident/Event 管理	应用程序和核心账户	要部署来自 AMS 基线监测的警报的 AMS 组件已移除 现有已部署的 Amazon CloudWatch 警报仍然存在，但不会再产生 AMS 事件 AWS Config 来自 AMS 和 MALZ Core 安全账户的聚合授权已删除 AWS Config 规则仍处于部署状态，Amazon GuardDuty 仍处于启用状态，但不再创建 AMS 事件	新创建的资源没有应用 AMS 基准监控和警报 基础设施指标警报和安全事件不再生成 AMS 事件 AWS Config 不再汇总到中央账户中	定义、捕获和分析运营指标，以查看工作负载事件并采取适当的措施。 实施任何必需的警报工作流程，继续对新资源应用所需的操作监控和警报，并接收来自 AWS Config 和 Amazon 的安全警报 GuardDuty。

组件	账户类型	为下船而采取的行动	潜在影响	建议的客户操作
连续性管理 (Backup and Restore)	应用程序账户	AMS 不再监控备份任务或执行备份和恢复请求 AMS 默认备份存储库、备份加密密钥和备份角色保留	可能不会注意到 Backup 操作失败	监控和审查备份计划配置
补丁管理	应用程序和核心账户	AMS 不再监控修补操作是否成功执行，也不再执行手动修补 AMS 不再更新 AMS 基础设施组件 AMS 提供的补丁基准会保留 AMS 提供的 AWS Systems Manager 补丁自动化运行手册是非共享的，不再可供使用	可能不会注意到修补操作失败 依赖于 AMS 提供的 Systems Manager Automation 运行手册的现有补丁配置必须重新配置才能不间断地继续运行	根据需要查看和重新配置修补配置
网络管理	应用程序账户	如果指定，则移除已移除的应用程序账户中的公网网关附件	已移除的应用程序账户无法再使用传输网关访问共享服务，例如托管 Active Directory 或其他应用程序账户	指定DeleteTransitGatewayAttachment 为False以保持中转网关的连接

组件	账户类型	为下船而采取的行动	潜在影响	建议的客户操作
安全管理	应用程序账户	帐户已从中央趋势科技 DSM 控制台中断开。此外，端点代理不再通过 AMS 事件流程转发警报 趋势科技代理仍处于安装状态，但不再由 AMS 管理或更新 AMS 提供的部署趋势科技代理的 AMI 自定义项不再由 AMS 维护或更新	EC2 可能不会注意到实例端点恶意软件检测 趋势科技代理未部署在从非 AMS 提供的 EC2 实例上 AMIs	考虑继续或停止趋势科技的选项 (请参阅 Trend Micro Deep Security)
安全管理 (续)	核心账户	趋势科技 DSM 基础架构保留在共享服务账户中，但不再由 AMS 维护或更新 趋势科技 DSM 不再通过 AMS 事件流程转发警报	EC2 实例端点恶意软件检测可能会被忽视 EC2 如果不维护基础架构 (定义更新、许可等)，则实例端点保护可能会受到影响	决定是继续还是停止趋势科技 (请参阅 Trend Micro Deep Security)
变更管理	应用程序和核心账户	AMS RFC 控制台和 API 已移除 包含账户级访问限制的 AMS 自定义服务控制策略 (SCPs) 将在应用程序账户注销期间分离，并在 Core 账户注销期间删除	您必须使用原生 AWS API 来创建新资源、更改现有资源或更新现有 CloudFormation 堆栈 不再通过提供的 AMS 在账户层面施加访问限制 SCPs	确保用户角色提供足够的访问权限以使用 AWS 服务 创建 SCPs 以提供账户级别的权限限制

组件	账户类型	为下船而采取的行动	潜在影响	建议的客户操作
用于服务管理的 AMS 操作系统映像和自动化	应用程序和核心账户	AMS 不再为所提供的 AMS 中包含的自定义和启动脚本提供支持 EC2 AMIs 所提供的 AMS 在您的离线账户中 EC2 AMIs 仍然可用 AMS 提供的 Systems Manager Automation 运行手册是非共享的，不再可供使用	下线后，FAILURE 由于缺少对 AMS AMIs 组件的依赖关系，AMS 提供了 CloudFormation 发送 cfn 信号 依赖于 AMS 提供的 Systems Manager Automation 运行手册的操作流程可能会失败	审查和更新任何依赖于 AMS 提供的 AMS 或 Systems Manager Automation 运行手册的构建 AMIs 或操作流程
共享服务基础架构	核心账户	AMS 访问权限已移除，AMS 不再管理共享组件，包括 AMS 托管 Active Directory AWS Transit Gateway，以及 AWS Organizations	对共享基础架构的管理丢失	重置管理员对 AMS 托管 Active Directory 的访问权限并假设管理共享服务组件
报告	应用程序和核心账户	AMS 不再收集账户或资源级别的详细信息以进行汇总报告	对运营和业务指标（备份和补丁覆盖范围、变更管理和事件活动）缺乏洞察力	将所有需要的跨账户汇总数据报告替换为他们自己的解决方案
AMS 客户团队和服务台	应用程序和核心账户	AMS 客户小组（加利福尼亚州 CSDM）和 AMS 运营服务台不再支持已离线账户	失去对 AMS 设计的多账户 landing zone 架构和相关组件的专业知识的运营支持	确保有足够的人员并熟悉账户结构和资源，以支持环境中的运营

访问替代方案

以下是在退出 AMS 账户后保留 EC2 堆栈访问权限的替代方法：

- 使用会话管理器以更高的权限访问 EC2 实例，无需堡垒或入站网络访问权限。有关更多信息，请参阅 [AWS Systems Manager Session Manager](#)。
- 使用新的域凭据@@ 将 EC2 实例重新加入到不同的 Active Directory 域。如果您使用 Directory Service，请参阅[将 EC2 实例加入您的 AWS Managed Microsoft AD 目录](#)。
- 使用您通过其他访问方法之一或通过 [AWS Systems Manager Run Command](#) 创建的本地用户帐户。

禁用 AMS EC2 启动脚本

Linux 操作系统：

使用发行版的软件包管理器卸载该ams-modules软件包。例如，对于亚马逊 Linux 2，请使用yum remove ams-modules。

Windows 操作系统

要在 Windows 中禁用 EC2 启动脚本，请完成以下步骤：

1. Windows Server 2008/2012/2012r2/2016/2016/2019：

从“任务计划程序”中禁用或删除 Managed Services 启动计划任务。要列出计划任务，请运行Get-ScheduledTask -TaskName '*Ec2*'命令。

2022 年 Windows 服务器：

移除 [EC2Launch v2 任务](#)。此任务Initialize-AMSBoot在实例上的 C:\Amazon\LaunchProgramData\config\agent-config.yml 中分postReady阶段运行。以下是示例agent-config.yml中的一段片段：

```
{
  "task": "executeScript",
  "inputs": [
    {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
    }
  ]
}
```

2. （可选）删除以下内容：


```
C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*  
C:\Windows\System32\WindowsPowerShell\v1.0\Modules  
\AWSManagedServices.Build.Utilities\*
```

PBIS Open/Enterprise (AD Bridge)

要确定您使用的是 PBIS 开放版还是 PBIS Enterprise (AD Bridge) 版，请在 Linux EC2 托管实例中运行以下命令：

```
yum info | grep pbis
```

以下是显示 PBIS Enterprise (AD Bridge) 的示例输出：

```
Name      : pbis-enterprise  
From repo : pbise  
Name      : pbis-enterprise-devel  
Repo      : pbise  
Description : The pbis-enterprise-devel package includes the development
```

PBIS 公开赛

PBIS Open 是一款已弃用的产品，BeyondTrust 不再支持。有关更多信息，请参阅 [BeyondTrust pbis-open 文档](#)。

AD Bridge (PBIS 企业版)

您可以执行以下操作之一：

- 续订许可并继续运行 AD Bridge。联系我们 BeyondTrust 讨论许可和支持事宜。
- 停止使用 AD Bridge。运行以下命令行管理程序命令从 Linux 托管实例中删除 PBIS-Enterprise 软件包。有关更多信息，请参阅 BeyondTrust 文档[退出域名并卸载 AD Bridge 代理](#)。

```
$ sudo /opt/pbis/bin/uninstall.sh purge
```

在不移除 PBIS 代理的情况下离开 AMS 托管的活动目录域

您可以选择不移除 PBIS 代理的情况下离开 AMS 托管的 Active Directory。根据您的操作系统，使用以下解决方案之一：

Linux operating systems

使用 AMS 托管 AD 中的 PBIS 运行以下 shell 命令来取消加入 Linux EC2 实例。有关更多信息，请参阅 [BeyondTrust pbis-open](#) 或 [BeyondTrust AD Bridge](#) 文档，具体取决于您使用的版本。

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

您可能会看到类似于以下内容的错误消息：

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]
Cannot resolve network address for KDC in requested realm
```

如果出现此错误，请运行以下命令删除 AD 提供商注册表并重新启动 lwsmd 服务：

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin]'
```

使用您从上一个命令（例如 **A123EXAMPLE.AMAZONAWS.COM**）中收到的目录 ID 输出来运行以下命令：

```
$ /opt/pbis/bin/regshell delete_tree \
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin\DIRECTORID]'

$ /etc/pbis/redhat/lwsmd restart

$ /opt/pbis/bin/lwsm restart lwreg
```

Windows operating systems

```
# Collect hostname and domain name using:

Test-ComputerSecureChannel -verbose

# Disjoin computer from the domain:

netdom remove hostname /domain:domain name /force
```

 Note

请务必禁用或删除 Managed Services 启动计划任务，如中所述[禁用 AMS EC2 启动脚本](#)。

Trend Micro Deep Security

使用以下选项之一继续或停止使用趋势科技趋势科技服务器深度安全防护系统：

继续使用

- （如果退出整个 MALZ）核心账户退出后，请将已离线的应用程序帐户重新连接到现有的趋势科技趋势科技趋势科技服务器深度安全防护系统管理中心 (DSM)，并在共享服务帐户中维护许可。有关更多信息，请参阅[添加 AWS 云帐户](#)和[检查您的许可证信息](#)。
 1. 登录共享服务账户并导航到 Secrets Manager 控制台。
 2. 检索存储在 /ams/eps/ 路径中的 DSM 控制台管理员凭据。
 3. 登录 DSM 控制台，[网址为 https://dsm.sentinel.int](https://dsm.sentinel.int)。
 4. 选择“使用跨账户角色”，然后输入 `arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role`。将 ACCOUNTID 替换为已移除的应用程序帐户 ID。
 5. 选择下一步。
 6. 等待几分钟，让 DSM 处理账户发现并显示同步已成功。
- 将已卸载的应用程序帐户重新连接到新的趋势科技 DSM 安装中。有关更多信息，请参阅[激活和保护代理](#)和[激活代理](#)。
- 将已卸载的应用程序帐户重新连接到趋势科技 Cloud One。有关更多信息，请参阅[从趋势科技服务器深度安全防护系统迁移到工作负载安全防护系统和从本地 DSM 迁移](#)。

停止使用

- 从已移除的应用程序帐户中卸载趋势科技服务器深度安全防护系统客户端。有关更多信息，请参阅[卸载趋势科技服务器深度安全防护系统](#)。

更改管理模式

AWS Managed Services (AMS) 使用变更管理模式对 AMS Advanced 中的更改进行防护。变更管理模式可帮助您保持环境的高运营标准，并控制风险和防止不利影响。AMS Advanced 有不同的模式，可提供不同级别的控制和风险。除客户管理模式外，所有模式均由 AMS 管理。以下是可用的变更管理模式：

- RFC 模式（前身为标准 CM 模式）：提供“更改请求”(RFC) 系统和 AMS 自定义更改类型 (CTs)
- 直接更改模式：与 RFC 模式相同，还可使用 AWS APIs 和控制台创建 AMS 管理的资源
- AMS 上的 AWS Service Catalog：与“直接更改”模式类似，但不是使用 AMS 变更管理系统 (RFCs)，而是使用 AWS Service Catalog 来创建由 AMS 管理的资源。
- 开发者模式：与 Direct Change 模式相同，只有您使用 AWS APIs 和控制台创建的资源不受 AMS 管理——您负责管理这些资源
- 自助服务配置 (SSP) 模式：与开发者模式相同，唯一的不同是无法访问 AMS 变更管理系统 (否 RFCs)
- 客户管理模式：AMS 为您提供多账户 landing zone，但所有资源管理均由您负责

AWS Managed Services (AMS) 变更管理系统使用变更管理 (CM) API，为多账户着陆区 (MALZ RFCs) 和单账户着陆区 (SALZ) 账户提供创建和管理变更请求 (RFC) 的操作。

变更请求 (RFC) 是您或 AMS 通过 AMS 接口创建的对托管环境进行更改的请求，包括特定操作的更改类型 (CT) ID。

AMS 变更管理 (CM) API 提供用于创建和管理变更请求 (RFCs) 的操作。您可以创建、更新、提交、批准、拒绝和取消 RFCs。AMS 运营商可以创建、更新、提交、批准、拒绝、取消和标记 RFCs 为已关闭。

有关不得在标签或其他名称中使用的 AMS 保留前缀的列表，请参阅[保留前缀](#)。

有关每种变更类型的信息，包括架构和示例，请参阅[AMS 变更类型参考](#)。

Note

所有变更管理 API 调用都记录在 AWS 中 CloudTrail。有关更多信息，请参阅[访问您的日志](#)。

模式概述

根据您想要的灵活性和规范性监管组合，使用这些信息来帮助您选择合适的 AWS Managed Services (AMS) 模式来托管应用程序，以实现业务成果。

此信息的目标受众是：

- 客户团队负责其 landing zone 的策略和治理。这些信息将帮助该团队为AMS管理的着陆区奠定基础，以及他们希望向内部和外部客户提供的AMS模式。
- 负责将其应用程序迁移到 AMS 的企业和应用程序所有者。这些信息将有助于规划应用程序迁移，并为 migrate/host 其应用程序提供相应的 AMS 模式。请注意，在软件开发生命周期 (SDLC) 生命周期的不同阶段，同一应用程序可以在多个 AMS 模式下托管。
- AMS 合作伙伴的任务是指导客户选择构建和迁移到 AMS 的不同选项。

这些信息在设置 AMS 托管平台的基础阶段最有用，当你从云采用之旅的基础阶段过渡到迁移阶段时，刚刚完成向 AMS 的入职并专注于应用程序治理和运营。

AMS 中的模式和账户类型

AWS Managed Services (AMS) 模式可以定义为在每种模式的特定管理框架下与 AMS 服务进行交互的方式。记录了着陆区的区别、多账户着陆区 (MALZ) 和单账户着陆区 (SALZ) 。

 Note

有关应用程序部署和选择正确的 AMS 模式的详细信息，请参阅 [AMS 模式和应用程序或工作负载](#)。

有关不同模式的真实用例，请参阅 [AMS 模式的真实世界用例](#)

下表描述了每个 AMS 服务的模式。

AMS 功能	RFC 模式 (以前是标准 CM 模式) /OOD *	直接更改模式	AWS Service Catalog	自助服务配置/开发者模式	客户管理
着陆区配置	MALZ 和 SALZ	MALZ 和 SALZ		MALZ 和 SALZ	

AMS 功能	RFC 模式 (以前是标准 CM 模式) /OOD *	直接更改模式	AWS Service Catalog	自助服务配置/开发者模式	客户管理
变更管理	变更计划、查看手动变更和变更记录	与 RFC 模式相同，适用于高风险更改，例如 IAM 或安全组	无		
记录、监控、防护和事件管理	是 (支持的资源)			否	
连续性管理	是 (支持的资源)			不适用/否	否
安全管理	实例级安全控制和账户级别控制			账户级别控制	AWS 组织级别控制
补丁管理	是			不适用/否	否
事件和问题管理	AMS 支持的资源的响应和解决方案 SLA			对由此产生的资源做出响应 SLA	否
报告	是			否	
服务请求管理	是			仅限 Support 请求	否

* Operations On Demand (OOD) 为使用 RFC 模式的客户提供了通过专用资源管理变更的服务。有关更多详细信息，请参阅按[需运营产品目录](#)，并咨询您的云服务交付经理 (CSDM)。

 Note

[AMS 中的自助服务配置模式](#)而且两者[AMS 高级开发者模式](#)似乎都适合具有植根于原生 AWS 服务的复杂架构的应用程序。在设计工作负载时，您需要根据业务环境在卓越运营和敏捷性之

间进行权衡。这是考虑为应用程序选择 SSP 模式或开发者模式的好方法。选择也可能根据应用程序的 SDLC 阶段而变化。例如：当应用程序已做好生产准备时，SSP 模式可能更合适，因为该模式下的 AMS 护栏更加严格。防护措施以预防性控制的形式强制执行，例如基于 RFC 的 IAM 更新和 SCPs 应用程序 OU 级别的变更控制。这些业务决策可以推动您的工程优先事务。您可以进行优化，以提高处于“预生产”阶段的应用程序所有者的灵活性，但会牺牲治理和运营支持。

MALZ 架构和相关的 AMS 模式

AMS 多账户 landing zone (MALZ) 允许您选择在默认组织单位 (OU) 下自动配置应用程序帐户 (或资源帐户)：客户管理的 OU、托管 OU 或开发 OU。在每个帐户下创建的应用程序帐户中配置的基础架构受这些 OUs 基础 OUs 架构提供的特定 AMS 模式的约束。通常在同一个应用程序帐户中混合使用两种或多种模式。例如：RFC 模式和 SSP 模式可以共存于 AMS 托管帐户中，该帐户托管管道架构，包括用于触发函数的 API Gateway 和 Lambda EC2，以及用于摄取和编排的 S3 和 SQS。在这种情况下，SSP 模式将适用于 Lambda 和 API Gateway。

图 1 显示了 AMS OUs 中如何通过“基础”提供不同的模式。在 AMS 中申请新的应用程序帐户时，必须为该帐户选择 OU。

MALZ 架构和相关的 AMS 模式

AMS 利用 OUs 基于 AWS 最佳实践的基础知识，使用服务控制策略 (SCP) 对帐户进行逻辑管理。这是在每个 AMS 模式下强制执行治理框架的一种方式。应用于基础的任何治理和安全护栏 (以形式 SCPs) OUs 也会自动应用于基础。custom/child OUs SCPs 可以要求为孩子提供额外服务 OUs。重要的是要明白，应用程序帐户与模式不同。模式适用于在帐户中配置的基础设施，并定义了 AMS 和客户之间的运营责任。

图 1：MALZ 架构和相关的 AMS 模式

Note

“限制性”意味着您可以为这些策略申请自定义策略 OUs，这些策略由 AMS 批准，以确保它们不会干扰 AMS 提供卓越运营的能力。case-by-case 有关 AMS 护栏的详细列表，请参阅用户指南中的 [AMS Guardrails](#)。

AMS 模式和应用程序或工作负载

在选择正确的模式时，请考虑应用程序的运营和管理要求，方法是申请新的应用程序帐户或将应用程序托管在现有应用程序帐户中。为每个应用程序或工作负载选择适当的 AMS 模式取决于以下因素：

- 环境将提供的 SDLC 生命周期功能类型（例如，包含未经审核更改的沙箱、具有一些频繁更改的 UAT、更改最少且受到严格监管的生产）
- 所需的治理政策（通过 SCPs OU 级别强制执行）
- 运营模式（如果您想承担运营责任或想将其外包给 AMS）
- 预期的业务成果，例如在云端运营的时间和运营成本。

Note

有关每个 AMS 服务的模式类型的描述，请参阅 [AMS 中的模式和账户类型](#)。
有关不同模式的真实用例，请参阅 [AMS 模式的真实世界用例](#)

下表概述了应用程序所有者在决定最合适的 AMS 模式时需要考虑的关键因素。应用程序所有者应在应用程序迁移之前加入评估阶段，以充分了解哪种模式适用于他们的特定应用程序。示例：对于基于云原生服务或无服务器架构的应用程序，最好的选择可能是在开发人员模式下开始构建和迭代，然后使用 AMS Managed — SSP 模式部署最终的基础设施即代码。在这种情况下，可能需要进行轻度重构，以确保为自动部署创建的任何 CloudFormation 模板都符合 AMS 制定的采集指南。此外，任何 IAM 权限都需要获得 AMS Security 的批准，以确保它们遵循最低权限模式。

为托管应用程序而选择的 AMS 模式可以帮助您朝着所需的云运营模式进行构建。

Note

根据为托管应用程序而选择的不同 AMS 模式，单个 AMS 托管着陆区中可以存在多个云运营模式。

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理

运营准备就绪

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
记录、监控和事件管理	AMS 负责所有托管基础架构			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	客户负责
连续性管理	AMS 负责执行客户选择的备份计划			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
实例级访问管理	AMS 通过本地域的单向 AD 信任进行管理。需要托管基础设施才能加入 AMS 域			不适用	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
安全管理和账户级别访问管理	AMS 对所有托管账户负责			AMS 负责所有托管账户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
补丁管理	AMS 对所有托管账户负责			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
变更管理	AMS 对所有托管账户负责			负责自助配置服务 (SSP) 的客户	负责使用开发者 IAM 角色在 AMS CM 系统之外配置资源的客户	
资源调配管理	针对 AMS 中提供的配置选项进行了规范和标准化	按照 AMS 规范性标准，可以灵活地直接使用适用于 AWS Service Catalog 的 AWS 服务 API	按照 AMS 规范性标准灵活地直接使用 AWS 服务 API	可以灵活地直接使用 AWS 服务 APIs 提供 SSP 服务	可以灵活地直接使用 AWS 服务 API 进行配置	
事件管理和审计	AMS 负责所有托管账户				负责使用开发者 IAM 角色在 AMS 变更管理系统之外配置资源的客户	

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
GuardRails 以及共享基础架构（网络）和安全框架	利用 AMS 核心账户的规范性和标准化					灵活定制利用 AMS 核心账户
应用程序就绪						
应用程序重构	需要轻量化重构				需要轻量级重构（如果使用 AMS 标准 CM 进行配置）	无需重构
对 AWS 服务的支持	仅限于 AMS 支持的内容					不限
业务注意事项						
是时候做好运营准备了	三到六个月			6 个月以上，具体取决于客户的应用程序操作能力		6-18 个月视客户基础架构和应用程序操作能力而定
成本	\$\$\$\$			\$\$\$	\$\$	\$

决策问题	标准 CM 模式/OOD *	AWS Service Catalog	直接更改模式	自助配置	开发者模式	客户管理
应用示例	具有 3 层堆栈的 Web 服务器、符合合规性和监管要求的应用程序			使用 API Gateway 的 Web 服务器、利用 ECS/EKS 的容器化应用程序	对使用 Lambda、Glue、Athena 等的数据库应用程序进行迭代/优化	accounts/applications 像沙盒一样去中心化、第三方托管的应用程序

* Operations On Demand (OOD) 为使用标准 CM 模式的客户提供了通过专用资源管理其变更的服务。有关更多详细信息，请参阅[按需运营产品目录](#)，并咨询您的云服务交付经理 (CSDM)。

 Note

SSP 模式和开发者模式之间的价格比较假设预配置了相同的 AWS 服务。

将 AMS 模式与业务和 IT 目标进行比较

如图所示，如果您正在为应用程序寻找高度可控和标准化的监管模式，那么 AMS 管理的标准变更、AWS Service Catalog 或直接变更模式最为合适。如果您需要以应用程序创新为重点的定制治理模型，而无需做好运营准备，请选择客户管理模式。在 Customer Managed 模式下，您可能需要更长的时间才能运行应用程序，因为您有责任建立人员、流程和工具来支持操作功能，例如事件管理、配置管理、配置管理、安全管理、补丁管理等。

AMS 模式的真实用例

检查这些内容以帮助确定如何使用 AMS 模式。

- 用例 1，企业必须通过时间敏感的数据中心退出来降低成本：具有引人注目的业务事件（例如数据中心退出）的企业有兴趣在云上重新托管其本地应用程序。大多数本地库存都包含混合操作系统版本的 Windows 和 Linux 服务器。在这样做的过程中，客户还希望利用迁移到云端所带来的成本节约，并改善其应用程序的技术和安全状况。客户想要快速行动，但尚未具备内部云运营专业知识。客户必须

在重构之间找到平衡，在时间紧迫的情况下，过多的重构可能会带来风险。但是，通过一些重构，例如更新操作系统版本和优化数据库，应用程序可以实现更高的性能水平。在此示例中，客户可以选择 AMS 管理的 RFC 模式来重新托管其大部分应用程序。AMS 提供基础设施运营，同时还指导客户运营团队了解在云端安全运营的最佳实践。

AMS 管理的 AWS Service Catalog 和 AMS 管理的 Direct Change 模式为客户提供了额外的灵活性，同时实现了相同的业务成果和目标。此外，客户可以使用 AMS 按需运营 (OOD) 产品让专门的 AMS 运营工程师来优先执行变更请求 (RFCs)。

在将无差别的基础设施运营任务（修补、备份、账户管理等）转移给 AMS 的同时，客户可以继续专注于优化其应用程序，增强内部团队的云运营能力。AMS 每月向客户提供成本节约报告，并就资源优化提出建议。在此用例中，如果客户决定不进行重构的旧操作系统版本（如 Windows 2003 和 2008）上托管了 end-of-life 应用程序，则这些应用程序也可以迁移到 AMS 并托管在利用客户管理模式的帐户中。

- 用例 2，在安全 AMS 边界内使用 Lambda、Glue、Athena 构建数据湖：一家企业希望建立数据湖以满足 AMS 中多个应用程序的报告需求。客户希望使用 S3 存储桶来存储数据集，并使用 AWS Athena 来查询每个报告的数据集。S3 和 AWS Athena 将部署在单独的 AMS 托管账户中。使用 S3 的账户还有其他服务，例如 Glue、Lambda 和 Step Functions，可用于构建数据摄取管道。在这种情况下，Glue、Lambda、Athena 和 Step Functions 被视为自助配置 (SSP) 服务。客户还在账户中部署了一个充当临时 tooling/scripting 服务器的 EC2 实例。客户首先请求 AMS 在其 AMS 托管账户中启用 SSP 服务。一旦该角色加入客户的联合解决方案，AMS 就会为客户可以担任的每项服务配置一个 IAM 角色。为便于管理，客户还可以将各个 IAM 角色的策略合并到一个自定义角色中，从而无需在 AWS 服务之间切换角色。在账户中启用该角色后，客户就可以根据自己的要求配置服务。但是，客户必须使用 AMS 变更管理系统来申请额外权限，具体取决于他们的用例。

例如，要访问 Glue Crawlers，Glue 需要额外的权限。还需要其他权限才能为 Lambda 创建事件源。客户将与 AMS 合作更新 IAM 角色，以允许 Athena 跨账户访问查询 S3 存储桶。还需要通过 AMS 变更管理更新服务角色或服务相关角色，让 Lambda 调用 Step Functions 服务，Glue 才能读取和写入所有 S3 存储桶。AMS 与客户合作，确保遵循最低权限访问模式，并且请求的 IAM 更改不会过于宽松，从而使环境面临不必要的风险。客户的数据湖团队花时间规划特定于客户架构的服务所需的所有 IAM 权限，并请求 AMS 启用这些权限。这是因为所有 IAM 更改都是手动处理的，并经过 AMS 安全团队的审查。应用程序部署计划中应考虑处理这些请求所需的时间。

由于 SSP 服务已在账户中运行，因此客户可以通过 AMS 事件管理和服务请求请求支持和报告问题。但是，AMS 不会主动监控 Lambda 的性能和并发指标，也不会主动监控 Glue 的作业指标。客户有责任确保为 SSP 服务启用适当的日志记录和监控。账户中的 EC2 实例和 S3 存储桶完全由 AMS 管理。

- 用例 3，在 AMS 中快速灵活地设置 CICD 部署管道：一位客户希望建立一个基于 Jenkins 的 CICD 管道，以便将代码管道部署到 AMS 中的所有应用程序帐户。客户可能会发现最适合在 AMS 管理的 Direct Change 模式 (DCM) 或 AMS 管理的开发者模式下托管此 CICD 管道，因为它使他们能够灵活地设置 Jenkins 服务器，开启所需的自定义配置 EC2，拥有所需的 IAM 访问权限 CloudFormation 和托管工件存储库的 S3 存储桶。虽然这也可以在 AMS 管理的 RFC 模式下完成，但客户团队需要为 IAM 角色创建多个手册 RFCs，以迭代许可程度最低的已批准权限集，这些权限由 AMS 手动审核。DCM 允许客户在 AWS 上实现运营目标，同时在使用 AMS 管理的 RFC 模式时，无需为 IAM 角色创建多个手册 RFCs 来迭代许可性最低的已批准权限集，这些权限由 AMS 手动审核。要提高 AMS 流程和工具，客户需要时间和教育。使用开发人员模式，客户可以从“开发人员角色”开始，使用原生 AWS 配置基础设施 APIs。设置此管道的最快、最灵活的方法是使用 AMS 托管开发者模式。开发人员模式提供了最快、最简单的方法，同时影响了操作集成，而 DCM 不那么灵活，但提供的操作支持级别与 RFC 模式相同。
- 用例 4，AMS 基金会内部的定制运营模式：客户正在考虑最后期限驱动的数据中心退出，他们的一个企业应用程序完全由第三方 MSP 管理，包括应用程序运营和基础设施运营。假设客户没有时间在计划中重构此应用程序以使其可以由 AMS 运行，那么客户管理模式是一个合适的选择。客户可以利用 AMS 管理的着陆区的自动快速设置。他们可以利用集中式账户管理，通过集中式网络账户控制账户销售和连接。它还通过 AMS Payer 账户合并所有客户管理账户的费用，从而简化了他们的账单。客户可以灵活地设置定制的访问管理模式，将 MSP 与 AMS 托管账户使用的标准访问管理分开。这样，使用客户管理模式，他们可以设置 AMS 托管环境，同时满足腾出本地环境的业务需求。在这种情况下，如果客户还有要迁移到云端的基于 Windows 的应用程序，并选择将其迁移到客户管理的帐户，则客户负责创建云运营模式。这可能很复杂、昂贵且耗时，具体取决于客户转变传统 IT 流程和培训人员的能力。通过将此类工作负载“转移并转移”到 AMS 托管账户，并将基础设施运营转移给 AMS，客户可以节省时间和成本。

Note

客户有时可能会觉得有必要在 RFC 或 SSP 模式的治理框架和开发者模式之间转移应用程序帐户。例如，作为初始迁移和轮班迁移的一部分，客户可能以 AMS 管理模式托管应用程序，但随着时间的推移，客户希望重写该应用程序以针对云原生 AWS 服务对其进行优化。他们可以将预生产账户的模式从 AMS 管理的 RFC 更改为 AMS 管理的开发者模式，从而为他们提供配置基础设施的灵活性和敏捷性。但是，一旦使用“开发人员角色”对基础设施配置进行了更改，就无法将相同的基础设施移回 AMS 管理的 RFC 模式。这是因为 AMS 无法保证在 AMS 变更管理系统之外配置的基础设施的运行。客户可能需要创建一个提供 AMS 管理的 RFC 模式的新应用程序账户，然后通过 CloudFormation 模板或自定义 AMIs 采集到 AMS 管理的账户中重新部署“优化”的基础架构配置。这是部署生产就绪配置的简洁方法。

部署后，该应用程序将处于规范性的 AMS 管理和运营之下。这同样适用于在客户管理模式和 AMS 管理模式之间切换模式。

RFC 模式

RFC 模式是 AMS 高级运营计划客户的默认模式。它包括一个变更管理系统，其中包含变更请求或，RFCs 以及用于请求对账户进行所需添加或更改的变更类型目录。此变更管理系统在限制谁可以更改您的帐户方面提供一定程度的安全性。

有关 AMS 高级更改类型的详细信息，请参阅[什么是 AMS 更改类型？](#)。

有关加入 AMS Advanced 的详细信息，请参阅[AWS Managed Services 入门](#)简介。

有关更改类型示例演练，请参阅[“按分类划分的 AMS 高级更改类型参考变更类型”部分中相关变更类型的“其他信息”部分](#)。

Note

RFC 模式以前被称为“变更管理模式”或“标准 CM 模式”。

主题

- [了解有关 RFCs](#)
- [什么是变更类型？](#)
- [对 AMS 中的 RFC 错误进行故障排除](#)

了解有关 RFCs

变更请求或 RFCs 以双重方式起作用。首先，RFC 本身需要一些参数。这些是 CreateRfc API 中的选项。其次，RFC 的操作需要参数（执行参数）。要了解这些 CreateRfc 选项，请参阅《AMS API 参考》的[CreateRfc](#)部分。这些选项通常显示在“创建 RFC”页面的“其他配置”区域中。

您可以使用 CreateRfc API、aws amscm create-rfc CLI 或使用 AMS 控制台创建 RFC 页面创建和提交 RFC。有关创建 RFC 的教程，请参阅[创建 RFC](#)。

主题

- [什么是 RFCs ?](#)
- [使用 AMS API/CLI 时进行身份验证](#)
- [了解 RFC 安全评论](#)
- [了解 RFC 变更类型分类](#)
- [了解 RFC 操作和活动状态](#)
- [了解 RFC 状态码](#)
- [了解 RFC 更新 CTs 和 CloudFormation 模板偏差检测](#)
- [日程安排 RFCs](#)
- [批准或拒绝 RFCs](#)
- [申请 RFC 限制运行期](#)
- [创建、克隆、更新、查找和取消 RFCs](#)
- [将 AMS 控制台与 RFCs](#)
- [了解常用 RFC 参数](#)
- [注册 RFC 每日电子邮件](#)

什么是 RFCs ?

变更请求 (RFC) 是指您如何在 AMS 管理的环境中进行更改，或者让 AMS 代表您进行更改。要创建 RFC，您可以从 AMS 更改类型中进行选择，选择 RFC 参数（例如计划），然后使用 AMS 控制台或 API 命令 [CreateRfc](#) 提交请求。 [SubmitRfc](#)

RFC 包含两个规范，一个用于 RFC 本身，另一个用于变更类型 (CT) 参数。在命令行中，您可以使用内联 RFC 命令或 JSON 格式的标准 CreateRfc 模板，该模板与您创建的 CT JSON 架构文件（基于 CT 参数）一起填写并提交。CT 名称是对 CT 的非正式描述。CSIO（类别、子类别、项目、操作）是对 CT 的更正式的描述。创建 RFC 时只需要指定 CT ID。

当更改成功完成（成功）或未成功（失败）时，AMS 会通知您。

Note

有关排除 RFC 故障的信息，请参阅[对 AMS 中的 RFC 错误进行故障排除](#)。

下图描述了您提交的 RFC 的工作流程。

使用 AMS API/CLI 时进行身份验证

使用 AMS API/CLI 时，必须使用临时证书进行身份验证。要为联合用户申请临时安全证书，请使用 `cal`、[GetFederationTokenAssumeRole](#)、[AssumeRoleWithSAML](#) 或 [AssumeRoleWithWebIdentity](#) AWS 安全令牌服务 (STS) APIs。

常见的选择是 SAML。设置完成后，您可以为所调用的每个操作添加一个参数。例如：`aws --profile saml amscm list-change-type-categories`。

SAML 2.0 配置文件的一个快捷方式是在每个 API/CLI 配置文件的开头设置配置文件变量 `set AWS_DEFAULT_PROFILE=saml`（对于 Windows；对于 Linux 则是这样 `export AWS_DEFAULT_PROFILE=saml`）。有关设置 CLI 环境变量的信息，请参阅[配置 AWS 命令行界面，环境变量](#)。

了解 RFC 安全评论

AWS Managed Services (AMS) 变更管理批准流程可确保我们对您的账户中所做的更改进行安全审查。

AMS 根据 AMS 技术标准评估所有变更请求 (RFCs)。任何可能因偏离技术标准而降低账户安全状况的变更都要经过安全审查。在安全审查期间，AMS 会重点介绍相关风险，如果存在高或非常高的安全风险，则您的授权安全人员会接受或拒绝 RFC。还对所有变化进行评估，以评估对 AMS 运营能力的负面影响。如果发现潜在的不利影响，则需要在 AMS 内部进行额外的审查和批准。

AMS 技术标准

AMS 技术标准定义了最低安全标准、配置和流程，以建立账户的基本安全性。AMS 和您都必须遵守这些标准。

任何可能因偏离技术标准而可能降低您账户安全状况的变更都要经过风险接受流程，AMS 会强调相关风险，并由您的授权安全人员接受或拒绝。还要对所有这些变化进行评估，以评估是否会对 AMS 的账户运营能力产生任何不利影响，如果是，则需要在 AMS 内部进行额外的审查和批准。

RFC 客户安全风险管理体系 (CSRM) 流程

当您的组织中的某人请求更改您的托管环境时，AMS 会审查更改，以确定该请求是否会超出技术标准，从而恶化您账户的安全状况。如果请求确实降低了账户的安全状况，AMS 会将相关风险通知您的安全团队联系人并执行变更；或者，如果变更给环境带来了高或非常高的安全风险，AMS 将以风险接受的形式寻求您的安全团队联系人的明确批准（详见下文）。AMS 客户风险接受流程旨在：

- 确保清楚地识别风险并将其传达给正确的所有者

- 将已识别的环境风险降至最低
- 获得并记录了解贵组织风险状况的指定安全联系人的批准
- 减少已识别风险的持续运营开销

如何获得技术标准以及高风险或非常高的风险

我们已将 AMS 技术标准文档<https://console.aws.amazon.com/artifact/>作为报告提供给您参考。在提交变更申请 (RFC) 之前，请使用 AMS 技术标准文档，了解变更是否需要您的授权安全联系人接受风险。

使用默认值登录后，在“报告”选项卡搜索栏中搜索“AWS Managed Services (AMS) 技术标准”，即可找到技术标准 AWS Artifact 报告AWSManagedServicesChangeManagementRole。

Note

单账户 landing zone 中的 Customer_ReadOnly_Role 可以访问 AMS 技术标准文档。在多账户 landing zone 中，安全管理员 AWSManagedServicesChangeManagementRole 使用和应用团队 AWSManagedServicesAdminRole 使用的登录区域可用于访问文档。如果您的团队使用自定义角色，请创建一个 Other | Other RFC 来请求访问权限，我们将更新指定的自定义角色。

了解 RFC 变更类型分类

您在提交 RFC 时使用的变更类型分为两大类：

- 部署：此分类用于创建资源。
- 管理：此分类用于更新或删除资源。管理类别还包含访问实例、加密或共享以及启动、停止 AMIs、重启或删除堆栈的更改类型。

了解 RFC 操作和活动状态

RfcActionState(API)/活动状态（控制台）可帮助您了解 RFC 上人为干预或操作的状态。主要用于手动 RFCs，RfcActionState可帮助您了解您或 AMS 运营部门何时需要采取行动，并帮助您了解 AMS 运营部门何时正在积极处理您的 RFC。这提高了 RFC 在其生命周期中所采取行动的透明度。

RfcActionState(API)/活动状态（控制台）定义：

- AwsOperatorAssigned: AWS 运营商正在积极处理您的 RFC。

- `AwsActionPending` : 预计 AWS 会做出回应或采取行动。
- `CustomerActionPending`: 预计客户会做出回应或采取行动。
- `NoActionPending` : AWS 或客户均无需采取任何行动。
- `NotApplicable` : 此状态不能由 AWS 运营商或客户设置，只能用于 RFCs 在此功能发布之前创建的状态。

RFC 操作状态会有所不同，具体取决于提交的变更类型是否需要人工审核以及是否将计划设置为“尽快”。

- 在审核、批准和启动具有延迟计划的手动变更类型期间 RFC `ActionState`更改：
 - 在您提交手册、预定的 RFC 后，`ActionState`系统会自动更改`AwsActionPending`为，表示操作员需要审核和批准 RFC。
 - 当操作员开始积极审查您的 RFC 时，`ActionState`更改为。`AwsOperatorAssigned`
 - 当运营商批准您的 RFC 后，RFC 状态将更改为“已计划”，并`ActionState`自动更改为。`NoActionPending`
 - 到达 RFC 的预定开始时间后，RFC 状态将更改为 `InProgress`，并`ActionState`自动更改为，表示`AwsActionPending`需要指派一名操作员来审查 RFC。
 - 当操作员开始主动运行 RFC 时，他们会将其更改`ActionState`为。`AwsOperatorAssigned`
 - 完成后，操作员将关闭 RFC。这会自动将更改`ActionState`为`NoActionPending`。

Important

- 您无法设置操作状态。它们要么根据 RFC 中的更改自动设置，要么由 AMS 操作员手动设置。
- 如果您向 RFC 添加信件，则会自动设置为。`ActionStateAwsActionPending`
- 创建 RFC 时，会`ActionState`自动设置为。`NoActionPending`
- 提交 RFC 后，会`ActionState`自动设置为。`AwsActionPending`
- 当 RFC 被拒绝、已取消或已完成且状态为“成功”或“失败”时，会自动重置`ActionState`为`NoActionPending`。
- 自动和手动操作状态均启用 RFCs，但手动操作状态最重要，RFCs 因为这些类型的操作 RFCs 通常需要通信。

查看 RFC 操作状态用例示例

用例：手动 RFC 流程的可见性

- 提交手动 RFC 后，RFC 操作状态会自动更改为 `AwsActionPending`，表示操作员需要审核和批准 RFC。当操作员开始积极查看您的 RFC 时，RFC 操作状态将更改为 `AwsOperatorAssigned`。
- 以手动 RFC 为例，该手动 RFC 已获得批准并已安排好开始运行。一旦 RFC 状态更改为 `InProgress`，RFC 操作状态就会自动更改为 `AwsActionPending`。当操作员开始积极运行 RFC 时，它将再次更改为 `AwsOperatorAssigned`。
- 手动 RFC 完成后（以“成功”或“失败”的形式关闭），RFC 操作状态将更改为 `NoActionPending`，表示客户或操作员无需采取进一步的行动。

用例：RFC 通信

- 如果是手动 RFC `Pending Approval`，AMS 操作员可能需要您提供更多信息。运营商将向 RFC 发布信件，并将 RFC 操作状态更改为 `CustomerActionPending`。当您通过添加新的 RFC 通信来回应时，RFC 操作状态会自动更改为 `AwsActionPending`。
- 当自动或手动 RFC 失败时，您可以在 RFC 详细信息中添加对应信息，询问 AMS 操作员 RFC 失败的原因。添加信件后，RFC 操作状态将自动设置为 `AwsActionPending`。当 AMS 操作员拿起 RFC 查看您的信件时，RFC 操作状态将更改为 `AwsOperatorAssigned`。当操作员通过添加新的 RFC 通信来做出回应时，RFC 操作状态可以设置为 `CustomerActionPending`，表示预期的客户还有一个回应，或者设置为 `NoActionPending`，表示不需要或预计客户不需要或预计不需要任何回应。

了解 RFC 状态码

RFC 状态代码可帮助您跟踪您的请求。在 RFC 运行期间，您可以在 CLI 输出中观察这些状态代码，也可以通过刷新控制台中的 RFC 列表页面来观察这些状态代码。

您还可以在该 RFC 的详细信息页面上查看 RFC 的代码，可能如下所示：

你可能会在列表中看到你没有提交的 RFC。当 AMS 操作员使用仅限内部的 CT 时，他们会在 RFC 中提交并显示在您的 RFC 列表中。有关更多信息，请参阅 [仅限内部的变更类型](#)。

⚠ Important

您可以请求 RFC 状态变更通知。有关详细信息，请参阅 [RFC 状态更改通知](#)。

RFC 状态码

成功	Failure
编辑：RFC 已创建但尚未提交	已拒绝：RFCs 通常因为验证失败而被拒绝；例如，指定了不可用的资源，即子网
PendingApproval /已提交：RFC 已提交，系统正在确定是否需要批准，并在需要时获得批准	已取消：RFCs 之所以取消，通常是因为它们在配置的开始时间过去之前未通过验证
AWS 批准/客户批准：RFC 已获得批准。自动 RFCs 由 AWS 批准，手动 RFCs 由操作员批准，有时还需要客户批准	失败：RFC 已失败；有关失败原因，请参阅输出 StatusReason 中的，AMS 操作会自动创建故障单并根据需要与您沟通
已计划：RFC 已通过语法和要求检查并计划运行	
InProgress: RFC 正在运行，RFCs 请注意，配置多个资源或资源长期运行 UserData，需要更长的时间才能运行	
已执行：RFC 已运行	
成功/成功：RFC 已成功完成	

📘 Note

取消或拒绝 RFCs 可使用重新提交 [UpdateRfc](#)；另[更新 RFCs](#)请参阅。

如果 RFC 通过了所有必要条件（例如，指定了所有必需的参数），则状态将更改为 PendingApproval（即使是自动也 CTs 需要批准，如果语法和参数检查通过，则会自动进行审批）。如果未通过，则状态将更改为 Rejected。StatusReason 提供有关拒绝的信息；ExecutionOutput 字段提供有关批准和完成的信息。错误代码包括：

- `InvalidRfcStateException`: RFC 的状态不允许执行被调用的操作。例如，如果 RFC 已变为“已提交”状态，则无法再对其进行修改。
- `InvalidRfcScheduleException`: `StartTime` `EndTime`、或 `TimeoutInMinutes` 参数被破坏。
- `InternalServerError`: 系统遇到了问题。
- `InvalidArgumentException` : 参数指定不正确；例如，使用了不可接受的值。
- `ResourceNotFoundException`: 找不到堆栈 ID 等值。

如果计划请求的开始和结束时间（也称为变更运行窗口）发生在更改获得批准之前，RFC 状态将 `Canceled` 更改为 `Pending`。如果更改获得批准，则 RFC 状态将 `Scheduled` 更改为 `Running`。ASAP 的变更运行窗口 RFCs 是提交时间加上 CT 的 `ExpectedExecutionDuration` 值。

在变更运行窗口到来之前的任何时候，都可以修改或取消计划变更（`RequestedStartTime` 在 CLI 中使用提交）。如果计划更改被修改，则必须重新提交。

当更改开始时间（计划或尽快）到来且批准完成后，状态将更改为 `Running`，无法进行任何修改。`InProgress` 如果更改在指定的变更运行窗口内完成，则状态将更改为 `Success`。如果更改的任何部分失败，或者变更运行窗口结束时更改仍在进行中，则状态将更改为 `Failure`。

Note

在 `InProgressSuccess`、或 `Failure` 更改状态期间，无法修改或取消 RFC。

下图说明了从 `CreatorFC` 调用到解析的 RFC 状态。

了解 RFC 更新 CTs 和 CloudFormation 模板偏差检测

在 AMS 中配置的资源使用修改后的 CloudFormation 模板。如果资源的参数通过服务的 AWS 管理控制台直接更改，则该资源的 CloudFormation 创建记录将不同步。如果发生这种情况，并且您尝试使用 AMS 更新更改类型来更新 AMS 中的资源，则 AMS 将引用原始资源配置并可能重置更改的参数。此重置可能会造成损害，因此，如果检测到任何额外的 AMS 配置更改，AMS 将不允许 RFCs 更新更改类型。

要查看更新更改类型的列表，请使用控制台筛选器。

漂移补救 FAQs

有关 AMS 漂移补救的问题和答案。您可以使用两种更改类型来启动偏差补救，一种是执行模式=手动或“需要审查”，另一种是执行模式=自动。

支持漂移修复的资源 (ct-3king0u4l33zf)

这些是漂移修复更改类型 (ct-3king0u4l33zf) 支持的资源。要修复任何资源，请改用“需要审查” (ct-34sxfo53yuzah) 更改类型。

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

漂移补救更改类型

有关使用 AMS 漂移补救变更类型的问题与解答。

有关漂移修复功能支持的资源列表，请参阅[支持漂移修复的资源 \(ct-3king0u4l33zf\)](#)。

Important

漂移修复会修改堆栈模板 and/or 参数，并且必须更新您的本地模板存储库或任何正在更新这些堆栈的自动化以使用最新的堆栈模板和参数。在不进行同步的情况下使用旧的模板 and/or 参数可能会对底层资源造成破坏性更改。

无需审查、自动化 CT (ct-3kinq0u4l33zf) 仅支持每个 RFC 修复 10 个资源。要在 10 个批次中修复剩余的资源，请创建新的资源，RFCs 直到所有资源都已修复。

我应该使用哪种漂移补救更改类型？

我们建议在以下情况下使用无需复查的自动 CT (ct-3kinq0u4l33zf)：

- 您尝试使用自动 CT 对现有堆栈资源执行更新，但 RFC 按堆栈原样被拒绝。DRIFTED
- 你过去使用过 Update CT，但由于堆栈已漂移，它失败了。您无需再次尝试更新，可以改用所需的审核、手动、CT。

我们建议仅在漂移补救不支持漂移资源类型（无需审查）、自动、CT (ct-3kinq0u4l33zf) 或漂移补救无需审查、自动化、CT (ct-3kinq0u4l33zf) 或漂移补救无需审查、自动化、CT 失败时才使用所需的审核 (ct-34sxfo53yuzah)。

修复期间对堆栈进行了哪些更改？

修复需要更新堆栈模板 and/or 参数，具体取决于偏移的属性。修复还会在修复期间更新堆栈的堆栈策略，并在修复完成后将堆栈策略恢复到之前的值。

我们怎样才能看到对堆栈模板 and/or 参数所做的更改？

在对 RFC 的回复中，提供了包含以下信息的变更摘要：

- ChangeSummaryJson：包含作为偏差补救一部分的堆栈模板 and/or 参数的更改摘要。补救分多个阶段执行。此变更摘要包含各个阶段的更改。如果修复成功，请检查最后一个阶段的更改。有关按顺序执行的阶段，请参阅 ExecutionPlan JSON 中的。例如，存在时 RestoreReferences 段总是在最后执行，并且包含用于修复后更改的 JSON。如果在 DryRun 模式下运行修复，则这些更改都不会应用于堆栈。
- PreRemediationStackTemplateAndConfigurationJson：包含在 CloudFormation 堆栈上触发修复 StackPolicyBody 之前的堆栈配置快照，包括模板、参数、输出。

执行修复后我需要做什么？

Important

您需要使用 RFC 摘要中提供的最新模板和参数来更新本地模板存储库或任何将更新已修复堆栈的自动化。这样做非常重要，因为使用旧的模板 and/or 参数可能会对堆栈资源造成进一步的破坏性更改。

在此补救期间，我的应用程序会受到影响吗？

补救是一个离线过程，只能在 CloudFormation 堆栈配置上执行。不对底层资源执行任何更新。

修复后，我能否继续使用管理 | 其他 | 其他 RFCs 来更新资源？

我们建议您始终使用可用的自动更新来更新堆栈资源 CTs。如果可用的更新 CTs 不支持您的用例，请使用管理 | 其他 | 其他请求。

修复是否会在堆栈中创建任何新资源？

修复不会在堆栈中创建任何新资源。但是，修复会创建新的输出并更新堆栈模板[元数据](#)部分以存储修复摘要供您参考。

补救总是成功吗？

修复需要仔细分析和验证模板配置，以确定是否可以执行。在这些验证失败的情况下，修复过程将停止，并且不会对堆栈模板或参数进行任何更改。此外，只能对支持的资源类型执行修复。

如果修复不成功，如何更新堆栈资源？

你可以使用“管理 | 其他 | 其他 | 更新 CT” (ct-0xdawir96cy7k) 来请求更改。AMS 对此类情况进行监控，并努力改进补救解决方案。

我能否修复同时具有受支持和不支持的资源类型的堆栈？

是。但是，只有在堆栈中发现支持的资源类型存在漂移时，才会执行修复。如果有任何不受支持的资源类型为 DRIFTED，则修复不会继续。

我能否请求对通过非 CFN Ingest 创建的堆栈进行补救？CTs

是。无论用于创建堆栈的更改类型如何，都可以对堆栈执行修复。

我能否知道在补救之前会对堆栈执行哪些更改？

是。两种更改类型都提供了一个DryRun选项，您可以使用该选项来请求在堆栈修复后将要执行的更改。但是，最终的补救更改可能会有所不同，具体取决于补救时堆栈上存在的偏差。

日程安排 RFCs

“日程安排”功能允许您选择的开始时间 RFCs。“日程安排”功能中提供了以下选项：

- 尽快执行此更改：AMS 一经批准，就会立即运行 RFC。大多数 CTs 都是自动批准的。如果不希望 RFC 在特定时间启动，请使用此选项。

- 安排此更改：设置 RFC 运行的日期、时间和时区。对于自动变更类型，最佳做法是在计划提交 RFC 后至少 10 分钟后申请开始时间。要查看必需的变更类型，您需要在计划提交 RFC 后至少 24 小时内申请开始时间。如果 RFC 在配置的开始时间之前未获得批准，则 RFC 将被拒绝。

设置 RFC 时间表

要安排 RFC，请使用以下方法之一：

尽快执行此更改：

- 主机：什么都不做。这使用默认的 RFC 时间表。
- API 或 CLI：删除“创建 RFC”操作中的 RequestedStartTime 和 RequestedEndTime 选项。

如果在提交后的三十天内未获得批准，ASAP “需要审核” RFCs 将自动被拒绝。

安排此更改：

- 控制台：选择“安排此更改”单选按钮。将打开“开始时间”区域。手动输入日期或使用日历控件选择日期。输入以 ISO 8601 格式表示的 UTC 时间，然后使用下拉列表选择地点。默认情况下，AMS 使用 ISO 8601 格式 YYYYMMDDThhmmss Z 或:mm:ss YYYY-MM-DDThh z，这两种格式都被接受。

Note

默认结束时间是从您输入的开始时间算起 4 小时。要将计划更改的结束时间设置为 4 小时以上，请使用 API 或 CLI 运行更改。

- API 或 CLI：在“创建 RFC”操作中提交 RequestedStartTime 和 RequestedEndTime 参数的值。传递配置 RequestedEndTime 并不能停止已经启动的自动更改类型的运行。对于“需要审核”的变更类型，如果在 AMS 运营研究仍在进行期间达到，并且您正在与 AMS 沟通，则可以申请延期，或者可能会要求您重新提交 RFC。RequestedEndTime

Tip

有关世界标准时间读数的示例，请参阅 Time-is 网站上的 [UTC](#)。下午 2 点 20 分 date/time 值为 2016-12-05 的 ISO 8601 格式示例：2016-12-05T14:20:00 Z 或 20161205T142000Z。

如果你提供...

- 只有 `aRequestedStartTime` , RFC 被视为已定时`RequestedEndTime`的, 并使用该`ExecutionDurationInMinutes`值填充。
- 只有 `aRequestedEndTime` , 我们扔一个 `InvalidArgumentException`。
- 两者`RequestedStartTime`兼而有之`RequestedEndTime` , 我们`RequestedEndTime`用指定的开始时间加上该`ExecutionDurationInMinutes`值覆盖。
- `RequestedStartTime`也不是`RequestedEndTime` , 我们将这些值保留为空, 并且 RFC 被视为 ASAP RFC。

Note

对于所有已安排的时间 RFCs , 将未指定的结束时间写成指定的时间`RequestedStartTime`加上已提交的更改类型的`ExpectedExecutionDurationInMinutes`属性。例如, 如果`ExpectedExecutionDurationInMinutes`为 “60” (分钟) , 指定`RequestedStartTime`为`2016-12-05T14:20:00Z` (2016 年 12 月 5 日凌晨 4:20) , 则实际结束时间将设置为 2016 年 12 月 5 日凌晨 5:20。要查找`ExpectedExecutionDurationInMinutes`特定更改类型的, 请运行以下命令:

```
aws amscm --profile saml get-change-type-version --  
change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.  
{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

使用 RFC 优先级选项

使用`execution mode = manual`变更类型中的“优先级”选项提醒 AMS 运营部门注意请求的紧迫性。

优先级选项位于`execution mode = manual`:

将手动 RFC 的优先级指定为“高”、“中”或“低”。RFCs 在 RFC 服务级别目标 (SLOs) 及其提交时间的前提下, 在 RFCs 归类为“中”之前要经过审核和批准。RFCs 如果指定了低优先级或未指定优先级, 则按提交顺序进行处理。

批准或拒绝 RFCs

RFCs 提交时需要批准（手动）CTs 必须获得您或 AMS 的批准。系统会自动处理预先批准 CTs。有关更多信息，请参阅 [CT 批准要求](#)。

Note

使用“需要审核”时 CTs，AMS 建议您使用“尽快安排”选项（在控制台中选择“尽快”，在 API/CLI 中将开始和结束时间留空），因为这些选项 CTs 要求 AMS 操作员检查 RFC，并可能在批准和运行之前与您沟通。如果您安排这些活动 RFCs，请务必留出至少 24 小时的时间。如果在预定开始时间之前未获得批准，RFC 将被自动拒绝。

如果 AMS 成功提交了需要批准的 RFC，则必须得到您的明确批准。或者，如果您提交需要批准的 RFC，则必须获得 AMS 的批准。如果您需要批准 AMS 提交的 RFC，则会向您发送电子邮件或其他预先确定的通信，请求批准。通信包括 RFC ID。发送通信后，请执行以下任一操作：

- 控制台批准或拒绝：使用 RFC 详细信息页面查看相关 RFC：
- API/CLI 批准：将更改 [ApproveRfc](#) 标记为已批准。如果所有者和操作者都需要，则必须同时采取行动。以下是 CLI 批准命令的示例。在以下示例中，将 RFC_ID 替换为相应的 RFC ID。

```
aws amscm approve-rfc --rfc-id RFC_ID
```

- API/CLI 拒绝：将更改 [RejectRfc](#) 标记为已拒绝。以下是 CLI 拒绝命令的示例。在以下示例中，将 RFC_ID 替换为相应的 RFC ID。

```
aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
```

申请 RFC 限制运行期

以前称为封锁日，您可以请求限制某些时间段。在这段时间内无法进行任何更改。

要设置限制运行时段，请使用 [UpdateRestrictedExecutionTimes](#) API 操作并以 UTC 为单位设置特定的时间段。您指定的时间段会覆盖之前指定的任何时段。如果您在指定的受限运行时间内提交 RFC，则提交失败并显示错误“RFC 计划无效”。您最多可以指定 200 个受限时间段。默认情况下，未设置限制期限。以下是请求命令示例（配置了 SAML 身份验证）：

```
aws amscm --profile saml update-restricted-execution-times --restricted-execution-times='[{"TimeRange":{"StartTime":"2018-01-01T12:00:00Z","EndTime":"2018-01-01T12:00:01Z"}}]'
```

您也可以通过运行 [ListRestrictedExecutionTimes](#) API 操作来查看当前 RestrictedExecutionTimes 设置。示例：

```
aws amscm --profile saml list-restricted-execution-times
```

如果您想在指定的受限执行时间内提交 RFC，请添加值为 OverrideRestrictedTimeRanges，然后像往常一样提交 RFC。RestrictedExecutionTimesOverrideId 最佳做法是仅将此方法用于关键或紧急 RFC。有关更多信息，请参阅的 API 参考 [SubmitRfc](#)。

创建、克隆、更新、查找和取消 RFCs

以下示例将引导您完成各种 RFC 操作。

主题

- [创建 RFC](#)
- [使用 AMS 控制台进行克隆 RFCs（重新创建）](#)
- [更新 RFCs](#)
- [查找 RFCs](#)
- [取消 RFCs](#)

创建 RFC

使用控制台创建 RFC

以下是 AMS 控制台中 RFC 创建流程的第一页，其中快速卡片已打开，浏览更改类型处于活动状态：

以下是 AMS 控制台中 RFC 创建流程的第一页，按类别选择处于活动状态：

它是如何运作的：

1. 导航到“创建 RFC”页面：在 AMS 控制台的左侧导航窗格中，单击 RFCs 打开 RFCs 列表页面，然后单击“创建 RFC”。

2. 在默认的“浏览更改类型”视图中选择常用更改类型 (CT)，或者在“按类别选择”视图中选择 CT。

- 按更改类型浏览：您可以单击“快速创建”区域中的常用 CT，立即打开“运行 RFC”页面。请注意，您不能使用快速创建来选择较旧的 CT 版本。

要进行排序 CTs，请使用卡片视图或表格视图中的所有更改类型区域。在任一视图中，选择一个 CT，然后单击“创建 RFC”打开“运行 RFC”页面。如果适用，“创建 RFC”按钮旁边会出现“使用旧版本创建”选项。

- 按类别选择：选择类别、子类别、项目和操作，CT 详细信息框将打开，并显示“使用旧版本创建”选项（如果适用）。单击“创建 RFC”打开“运行 RFC”页面。
3. 在“运行 RFC”页面上，打开 CT 名称区域以查看 CT 详细信息框。必须填写主题（如果您在“浏览更改类型”视图中选择 CT，则会为您填写此主题）。打开“其他配置”区域以添加有关 RFC 的信息。

在执行配置区域中，使用可用的下拉列表或输入所需参数的值。要配置可选的执行参数，请打开其他配置区域。

4. 完成后，单击“运行”。如果没有错误，则会显示成功创建的 RFC 页面，其中包含已提交的 RFC 详细信息和初始运行输出。
5. 打开运行参数区域以查看您提交的配置。刷新页面以更新 RFC 的执行状态。（可选）取消 RFC 或使用页面顶部的选项创建一个 RFC 的副本。

使用 CLI 创建 RFC

它是如何运作的：

- 使用 Inline Create（您发出包含所有 RFC 和执行参数的 `create-rfc` 命令）或模板创建（创建两个 JSON 文件，一个用于 RFC 参数，一个用于执行参数），然后以这两个文件作为输入发出 `create-rfc` 命令。这里描述了这两种方法。
- 提交带有返回的 RFC ID 的 RFC: `aws amscm submit-rfc --rfc-id ID` 命令。

监控 RFC: `aws amscm get-rfc --rfc-id ID` 命令。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CT_ID
```

Note

您可以将任何CreateRfc参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。`--notification "{\"Email\": {\"EmailRecipients\": [\"email@example.com\"]}}\"`有关所有 CreateRfc 参数的列表，请参阅《[AMS 变更管理 API 参考](#)》。

内联创建：

使用内联提供的执行参数（内联提供执行参数时使用转义引号）发出 create RFC 命令，然后提交返回的 RFC ID。例如，你可以用这样的东西替换内容：

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

模板创建：

Note

此创建 RFC 的示例使用了 Load Balancer (ELB) 堆栈更改类型。

1. 找到相关的 CT。以下命令在 CT 分类摘要中搜索项目名称中包含“ELB”的摘要，并以表格形式创建类别、项目、操作和 ChangeType ID 的输出（两者的子类别均为Advanced stack components）。

```
aws amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[?contains(Item,'ELB')]. [Category,Item,Operation,ChangeTypeId]" --output table
```

CtSummaries				
Deployment	Load balancer (ELB) stack	Create	ct-123h45t6uz7j1	
Management	Load balancer (ELB) stack	Update	ct-01tm873rsebx9	

2. 查找 CT 的最新版本：

ChangeTypeIdandChangeTypeVersion：本演练的更改类型 ID 是 ct-123h45t6uz7jl（创建 ELB），要查找最新版本，请运行以下命令：

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
```

3. 了解选项和要求。以下命令将架构输出到名为 CreateElbParams.json 的 JSON 文件中。

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
"ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. 修改并保存执行参数 JSON 文件。此示例将文件命名为 CreateElbParams.json。

对于配置 CT，包含 StackTemplateId 在架构中，并且必须在执行参数中提交。

对于 TimeoutInMinutes，在 RFC 失败之前允许创建堆栈多少分钟，此设置不会延迟 RFC 的执行，但您必须留出足够的时间（例如，不要指定“5”）。对于 CTs 长时间运行 UserData：创建 EC2 和创建 ASG，有效值为“60”到“360”。我们建议所有其他配置 CTs 的最大允许值为“60”。

提供您要在其中创建堆栈的 VPC 的 ID；您可以使用 CLI 命令获取 VPC ID `aws amsskms list-vpc-summaries`。

```
{
  "Description":      "ELB-Create-RFC",
  "VpcId":             "VPC_ID",
  "StackTemplateId":  "stm-sdhopv000000000000",
  "Name":              "MyElbInstance",
  "TimeoutInMinutes": 60,
  "Parameters": {
    "ELBSubnetIds":    ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold": 4,
    "ELBHealthCheckInterval": 5,
    "ELBHealthCheckTarget": "HTTP:80/",
    "ELBHealthCheckTimeout": 60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":       false
  }
}
```

5. 将 RFC JSON 模板输出到当前文件夹中名为 CreateElbRfc.json 的文件中：


```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. 修改并保存 CreateElbRfc.json 文件。由于您在单独的文件中创建了执行参数，因此请删除该 ExecutionParameters 行。例如，你可以用这样的东西替换内容：

```
{
  "ChangeTypeVersion":    "2.0",
  "ChangeTypeId":         "ct-123h45t6uz7jl",
  "Title":                "Create ELB"
}
```

7. 创建 RFC。以下命令指定执行参数文件和 RFC 模板文件：

```
aws amscm create-rfc --cli-input-json file:///CreateElbRfc.json --execution-parameters file:///CreateElbParams.json
```

您在响应中收到新 RFC 的 ID，并可以使用它来提交和监控 RFC。在您提交之前，RFC 仍处于编辑状态且无法启动。

提示

Note

您可以使用 AMS 创建 RFC API/CLI，而无需创建 RFC JSON 文件或 CT 执行参数 JSON 文件。为此，您可以使用 create-rfc 命令并将所需的 RFC 和执行参数添加到命令中，这称为“Inline Create”。请注意，所有配置 CTs 都在 execution-parameters 区块中包含一个包含资源参数的 Parameters 数组。参数必须使用反斜杠 (\) 对引号进行转义。

另一种记录在案的创建 RFC 的方法叫做“模板创建”。在这里，您可以为 RFC 参数创建一个 JSON 文件，为执行参数创建另一个 JSON 文件，然后使用 create-rfc 命令提交这两个文件。这些文件可以用作模板并在将来 RFCs 重复使用。

RFCs 使用模板创建时，您可以使用命令通过发出如下所示的命令来创建包含所需内容的 JSON 文件。这些命令使用显示的内容创建一个名为“parameters.json”的文件；你也可以使用这些命令来创建 RFC JSON 文件。

使用 AMS 控制台进行克隆 RFCs（重新创建）

您可以使用 AMS 控制台克隆现有的 RFC。

要使用 AMS 控制台克隆或重新创建 RFC，请执行以下步骤：

1. 找到相关的 RFC。在左侧导航栏中，单击 RFCs。

RFCs 仪表板打开。

2. 滚动浏览页面，直到找到要克隆的 RFC。使用“筛选”选项缩小列表范围。选择要克隆的 RFC。

RFC 详细信息页面打开。

3. 单击“创建副本”。

将打开“创建更改请求”页面，所有选项的设置都与原始 RFC 中的设置相同。

4. 根据需要进行更改。要设置其他选项，请将“基本”选项更改为“高级”。设置完所有选项后，选择提交。

活动的 RFC 详细信息页面打开时会显示克隆的 RFC 的新 RFC ID，克隆的 RFC 将显示在 RFC 控制面板中。

更新 RFCs

您可以通过更新 RFC 然后提交或重新提交来重新提交已被拒绝或尚未提交的 RFC。请注意，大多数 RFCs 都被拒绝，因为指定的值在提交前 RequestedStartTime 已通过，或者指定的值 TimeoutInMinutes 不足以运行 RFC（由于 TimeoutInMinutes 不会延长成功的 RFC，因此对于长期运行的 Amazon EC2 或 Amazon A EC2 uto Scaling 组，我们建议始终将其设置为至少“60”，最多设置为“360”）。UserData 本节介绍如何使用 UpdateRfc 命令的 CLI 版本使用新的 RFC 参数更新 RFC，或者使用字符串化的 JSON 或更新的参数文件来更新 RFC。

此示例介绍如何使用 CLI 版本的 AMS UpdateRfc API（参见[更新 RFC](#)）。虽然有些更改类型可用于更新某些资源（DNS 私有和公有、负载均衡器堆栈以及堆栈修补配置），但没有 CT 可以更新 RFC。

我们建议您一次提交一个 UpdateRfc 操作。如果您提交多个更新（例如在 DNS 堆栈上），则尝试同时更新 DNS 时，更新可能会失败。

必填数据:RfcId: 您正在更新的 RFC。

可选数据:ExecutionParameters: 除非你要更新非必填字段，比如 Description，否则你需要提交修改后的执行参数来解决导致 RFC 被拒绝或取消的问题。所有提交的非空值都会覆盖原始 RFC 中的这些值。

1. 找到相关的已拒绝或已取消的 RFC，您可以使用以下命令（可以将值替换为 Canceled）：

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
```

2. 您可以修改以下任何 RFC 参数：

```
{
  "Description": "string",
  "ExecutionParameters": "string",
  "ExpectedOutcome": "string",
  "ImplementationPlan": "string",
  "RequestedEndTime": "string",
  "RequestedStartTime": "string",
  "RfcId": "string",
  "RollbackPlan": "string",
  "Title": "string",
  "WorstCaseScenario": "string"}
```

更新描述字段的命令示例：

```
aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
--region us-east-1
```

更新 ExecutionParameters VpcId 字段的命令示例：

```
aws amscm update-rfc --execution-parameters "{\"VpcId\": \"VPC_ID\"}" --rfc-id
"RFC_ID" --region us-east-1
```

使用包含更新的执行参数文件更新 RFC 的命令示例；参见步骤 2 中的示例执行参数文件：[EC2 stack | Create](#) e:

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. 使用 submit-rfc 与首次创建 RFC 时相同的 RFC 编号重新提交 RFC：

```
aws amscm submit-rfc --rfc-id RFC_ID
```

如果 RFC 成功，则您不会在命令行收到任何确认或错误消息。

4. 要监控请求的状态并查看执行输出，请运行以下命令。

```
aws amscm get-rfc --rfc-id RFC_ID
```

查找 RFCs

使用控制台查找变更请求 (RFC)

要使用 AMS 控制台查找 RFC，请按照以下步骤操作。

Note

此过程仅适用于未使用 ASAP 选项的已计划 RFCs。RFCs

1. 在左侧导航栏中，单击RFCs。

RFCs 仪表板打开。

2. 滚动浏览列表或使用“筛选”选项来细化列表。

根据筛选标准，RFC 列表会发生变化。

3. 选择所需的 RFC 的“主题”链接。

将打开该 RFC 的 RFC 详细信息页面，其中包含包括 RFC ID 在内的信息。

4. 如果仪表板 RFCs 中有许多内容，则可以使用“筛选器”选项按 RFC 进行搜索：

- 主题：创建 RFC 时向其提供的主题行或标题（在 API/CLI 中）。
- RFC ID：RFC 的标识符。
- 活动状态：如果您知道 RFC 状态，则可以在AwsOperatorAssigned表示操作员当前正在查看 RFC（AwsActionPending即 AMS 操作员必须在 RFC 执行之前执行某项操作）或CustomerActionPending表示您需要在 RFC 执行之前采取一些操作之间进行选择。
- 状态：如果您知道 RFC 状态，则可以在以下选项中进行选择：
 - 已计划：RFCs 那是预定的。
 - 已取消：RFCs 已取消。
 - 进行中：RFCs 进行中。
 - 成功：RFCs 成功执行。
 - 已拒绝：RFCs 已被拒绝。

- 编辑：RFCs 正在编辑中。
- 失败：RFCs 失败了。
- 待批准：在 AMS 或您批准之前，RFCs 这无法继续进行。通常，这表示您需要批准 RFC。您将在服务请求列表中收到有关此问题的服务通知。
- 更改类型：选择“类别”、“子类别”、“物料”和“操作”，系统将为您检索更改类型 ID。
- 请求的开始时间或请求的结束时间：此筛选选项允许您选择“之前”或“之后”，然后输入日期，也可以输入时间（可选）（hh:mm 和时区）。此过滤器只能按计划成功运行 RFCs（不是 ASAP RFCs）。
- 状态：“已计划”、“已取消”、“进行中”、“成功”、“已拒绝”、“正在编辑”或“失败”。
- 主题：您向 RFC 提供的主题（或标题，如果 RFC 是使用 API/CLI 创建的）。
- 变更类型 ID：使用与 RFC 一起提交的变更类型的标识符。

搜索允许您添加过滤器，如以下屏幕截图所示。

5. 点击所需的 RFC 的“主题”链接。

将打开该 RFC 的 RFC 详细信息页面，其中包含包括 RFC ID 在内的信息。

使用 CLI 查找变更请求 (RFC)

您可以使用多个筛选器来查找 RFC。

要检查更改类型版本，请使用以下命令：

```
aws amscm list-change-type-version-summaries --filter
Attribute=ChangeTypeId,Value=CT_ID
```

Note

您可以将任何 CreateRfc 参数与任何 RFC 一起使用，无论它们是否属于变更类型的架构的一部分。例如，要在 RFC 状态更改时收到通知，请将此行添加到请求的 RFC 参数部分（不是执行参数）。`--notification '{"Email": {"EmailRecipients": [{"email@example.com"}]}'`有关所有 CreateRfc 参数的列表，请参阅《[AMS 变更管理 API 参考](#)》。

如果您没有写下 RFC ID，需要稍后查找，则可以使用 AMS 变更管理 (CM) 系统进行搜索并使用筛选器或查询来缩小结果范围。

1. CM API [ListRfcSummaries](#)操作具有过滤器。您可以根据Attribute和Value组合在逻辑 AND 运算中[筛选](#)结果，也可以基于AttributeCondition、a 和筛选结果Values。

RFC 过滤

属性	有效值	有效条件	默认条件	备注
ActualEndTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前”或“之后”条件仅接受“值”字段中的一个值。“介于”条件的“值”字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期
ActualStartTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前”或“之后”条件仅接受“值”字段中的一个值。“介于”条件的“值”字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期
AutomationStatusId	手动、自动	Equals	Equals	只有两种自动化状态
ChangeTypeId	任何有效的更改类型 ID；例如，ct-123h45t6uz7jl	Equals	Equals	查找变更类型或 CSIO
ChangeTypeVersion	任何有效的更改类型 ID；例如 1.0	Equals	Equals	查找变更类型或 CSIO
CreatedBy	任何字符串（允许的最大长度为 2048 个字符）	包含	包含	RFC 的 CreatedBy 字段包含创建它的用户的 ARN

属性	有效值	有效条件	默认条件	备注
CreatedTime	任何表示 ISO8601 日期时间的字符串 (例如 , “20170101T000000Z”)	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值 , 其中第一个值应表示第二个值之前的日期
LastModifiedTime	任何表示 ISO8601 日期时间的字符串 (例如 , “20170101T000000Z”)	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值 , 其中第一个值应表示第二个值之前的日期
LastSubmittedTime	任何表示 ISO8601 日期时间的字符串 (例如 , “20170101T000000Z”)	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值 , 其中第一个值应表示第二个值之前的日期
RequestedEndTime	任何表示 ISO8601 日期时间的字符串 (例如 , “20170101T000000Z”)	之前、之后、之间	无	“之前” 或 “之后” 条件仅接受 “值” 字段中的一个值。“介于” 条件的 “值” 字段中必须恰好有两个值 , 其中第一个值应表示第二个值之前的日期

属性	有效值	有效条件	默认条件	备注
RequestedStartTime	任何表示 ISO8601 日期时间的字符串（例如，“20170101T000000Z”）	之前、之后、之间	无	“之前”或“之后”条件仅接受“值”字段中的一个值。“介于”条件的“值”字段中必须恰好有两个值，其中第一个值应表示第二个值之前的日期
RfcStatusId	已取消、正在编辑、失败、InProgress、PendingApproval、已拒绝、已计划、成功	Equals	Equals	刷新 AMS 控制台中的 RFC 列表或运行 GetRfc
职务	任何有效的 RFC 标题	包含	包含	不支持每个字段中的正则表达式。不区分大小写的搜索

示例：

要查找所有与 SQS RFCs 相关的（其中 SQS 包含在 CT 的项目部分），可以使用以下命令：IDs

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

它返回的结果是这样的：

```
-----
|                               ListRfcSummaries                               |
+-----+-----+-----+-----+-----+-----+
|Deployment| Advanced Stack Components      |SQS   |Create |ct-123h45t6uz7j1|
|Management| Monitoring & Notification    |SQS   |Update |ct-123h45t6uz7j1|
+-----+-----+-----+-----+-----+-----+-----+
```

另一个可用的过滤器list-rfc-summaries是AutomationStatusId，寻找 RFCs 自动或手动的过滤器：


```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

另一个可用的过滤器 `list-rfc-summaries` 是 `Title` (控制台中的主题) :

```
Attribute=Title,Value=RFC-TITLE
```

JSON 中的新请求结构示例, 其返回 RFCs 位置为 :

- (标题包含 “Windows 2012” 或 “亚马逊 Linux” 这句话) 和
- (`RfcStatusId` 等于 “成功” 或 `InProgress`) 和
- (`20170101T000000Z` $\leq$ `RequestedStartTime` $\leq$ `20170103T000000Z`) 和 (`ActualEndTime` $\leq$ `20170103T000000Z`)

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

 Note

在更高级的版本中Filters，AMS 打算在即将发布的版本中弃用以下字段：

- 值：“值”字段是“筛选器”字段的一部分。使用支持更多高级功能的“值”字段。
- RequestedEndTimeRange: 使用支持更高级功能的“过滤器”字段 RequestedEndTime 内部
- RequestedStartTimeRange：使用支持更高级功能的“过滤器”字段 RequestedStartTime 内部。

有关使用 CLI 查询的信息，请参阅[如何使用--query 选项过滤输出](#)和查询语言参考[JMESPath 规范](#)。

2. 如果您使用的是 AMS 控制台：

转到RFCs列表页面。如果需要，您可以在 RFC 主题上进行筛选，这是您在创建 RFC Title 时输入的内容。

提示

 Note

此过程仅适用于未使用 ASAP 选项的已计划 RFCs。RFCs

取消 RFCs

您可以使用控制台或 AMS API/CLI 取消 RFC。

要使用控制台取消 RFC，请在您的 RFC 列表中找到 RFC，将其打开，单击“取消”。

所需数据：

- Reason: 你为什么要取消 RFC。
- RfcId: 您要取消的 RFC。

1. 通常，您会在提交 RFC 后立即将其取消（因此 RFC ID 应该很方便）；否则，除非您安排了它并且在指定的开始时间之前，否则您将无法取消它。如果需要查找 RFC ID，则可以使用以下命令（可以Value用PendingApproval替换手动批准的 RFC）：

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. 取消 RFC 的命令示例：

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --region us-east-1
```

将 AMS 控制台与 RFCs

AMS 控制台提供的功能可帮助您成功创建和提交 RFCs。

使用 RFC 列表页面（控制台）

AMS 控制台RFCs列表页面为您提供以下选项：

- 通过过滤器进行高级 RFC 搜索。有关信息，请参阅[查找 RFCs](#)。
- 查找 RFC 上次修改的时间。此值表示上次更改 RFC 状态的时间。
- 使用 RFC 主题查看 RFC 详细信息。选择此链接将打开该 RFC 的详细信息页面。
- 查看 RFC 状态。有关信息，请参阅。[了解 RFC 状态码](#)

使用 RFC 快速创建（控制台）

使用 RFC 快速创建卡片或列表表，或者 RFCs 按分类选择更改类型。

要了解更多信息，请参阅[创建 RFC](#)。

添加 RFC 信件和附件（控制台）

您可以在 RFC 提交后和获得批准之前向其添加信件；例如，当它处于“PendingApproval”状态时。在 RFC 获得批准（处于“已计划”或 InProgress “” 状态）后，无法添加信件，因为它可能被解释为对请求的更改。RFC 完成后（处于“已取消”、“已拒绝”、“成功”或“失败”状态），将再次启用通信，但在 RFC 关闭超过 30 天后，通信将被禁用。

 Note

每封信件不得超过 5,000 个字符。

附件的限制：

- 每封信件只有三个附件。
- 每个 RFC 限制五十个附件。
- 每个附件的大小必须小于 5 MB。
- 仅接受文本文件，例如纯文本 (.txt)、逗号分隔值 ()、JSON (.csv) 或 YAM .json L ()。 .yaml 如果是 YAML 格式，则必须使用文件扩展名 .yaml 附加文件。

 Note

禁止包含 XML 内容的文本文件。如果您有 XML 内容要与 AMS 共享，请使用服务请求。

- 文件名限制为 255 个字符，只能包含数字、字母、空格、破折号 (-)、下划线 (_) 和点 (.)。
- 目前不支持在 RFC 上更新和删除附件。

要向 RFC 添加信件和附件，请执行以下步骤：

1. 在 AMS 控制台中，在 RFC 的 RFC 详细信息页面上，找到页面底部的“通信”部分。

在任何通信之前：

经过一番信件后：

2. 要添加新的信件，请在回复文本框中键入您的消息。要附加与信件相关的文件，请选择“添加附件”，然后选择所需的文件。
3. 完成后，选择“提交”。

新的信件以及所附文件的链接出现在 RFC 详细信息页面的信件列表中。

配置 RFC 电子邮件通知 (控制台)

AMS 控制台的“更改请求创建”页面为您提供了添加电子邮件地址以接收 RFC 状态变更通知的选项：

此外，您可以将通知的电子邮件地址添加到任何更改类型，例如：

```
aws amscm create-rfc --change-type-id <Change type ID>
                    --change-type-version 1.0 --title "TITLE"
                    --notification "{\"Email\": {\"EmailRecipients\" :
[\"email@example.com\"]}}\""
```

在请求的 RFC 参数部分，而不是参数部分，向任何更改类型内联或模板请求添加类似的行 (--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}\").

了解常用 RFC 参数

以下是您需要提交的 RFC 参数以及中 RFCs 常用的参数：

- 更改类型信息：ChangeTypeId 和 ChangeTypeVersion。有关更改类型 IDs 和版本号的列表，请参阅[更改类型参考](#)。

使用 query 参数 list-change-type-classification-summaries 在 CLI 中运行以缩小结果范围。例如，缩小结果范围以更改 Item 名称中包含“Access”的类型。

```
aws amscm list-change-type-classification-summaries --query
'ChangeTypeClassificationSummaries [?contains (Item, 'access')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

运行 get-change-type-version 并指定更改类型 ID。以下命令获取 ct-2tylseo8rxfsc 的 CT 版本。

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
```

- 标题：RFC 的名称；它成为 AMS 控制台 RFC 列表中 RFC 的主题，您可以使用 GetRfc 命令和过滤器对其进行搜索 Title
- 计划：如果您想要预定的 RFC，则必须包含 RequestedStartTime 和 RequestedEndTime 参数，或者使用“安排此更改”控制台选项。对于 ASAP RFC（在获得批准后立即运行），在使用 CLI 时，

请保留RequestedStartTime并RequestedEndTime为 null。使用控制台时，请接受“尽快”选项。

如果错过RequestedStartTime，则 RFC 将被拒绝。

- 配置 CTs：执行参数，或者Parameters是配置资源所需的特定设置。根据 CT 的不同，它们差异很大。
- 非预配 CTs：CTs 未配置资源（例如访问权限 CTs 或其他 | 其他）或删除堆栈的执行参数最少且没有Parameters阻塞。
- 有些 RFCs 还要求您在 RFC 失败之前指定创建堆栈的时间或允许多少分钟。TimeoutInMinutes对于长时间运行 UserData，有效值为 60（分钟）到 360。如果在超过之前无法完成执行，则 TimeoutInMinutes RFC 将失败。但是，此设置不会延迟 RFC 的执行。
- RFCs 创建实例（例如 S3 存储桶或 ELB）通常会提供允许您添加最多七个标签（键/值对）的架构。您可以使用部署 | 高级堆栈组件 | 标签 | 创建更改类型(ct-3cx7we852p3af) 提交 RFC，从而向 S3 存储桶添加更多标签。EC2、EFS、RDS 和多层（HA 双层和 HA 单层）架构最多允许 50 个标签。标签是在架构的ExecutionParameters部分中指定的。提供标签可能非常有价值。有关更多信息，请参阅[标记您的 Amazon EC2 资源](#)。

使用 AMS 控制台时，必须打开其他配置区域才能添加标签。

Tip

许多 CT 架构的架构顶部附近都有一个Description和Name字段。这些字段用于命名堆栈或堆栈组件，它们不会命名您正在创建的资源。有些架构提供参数来命名您正在创建的资源，有些则没有。例如，Create EC2 堆栈的 CT 架构不提供用于命名 EC2 实例的参数。为此，您必须使用密钥为“Name”和您想要的名称的值创建一个标签。如果您未创建此类标签，则您的 EC2 实例将在 EC2 控制台中显示，但不带名称属性。

使用 RFC AWS 区域选项

AMS API 和 CLI（amscm和amsskms）端点已在us-east-1。如果您使用安全断言标记语言 (SAML) 进行联合，则会在入门时为您提供将您的区域设置为 us-east-1 的脚本。AWS 如果您使用 SAML，则在发出命令时无需指定该--region选项。如果您的 SAML 配置为使用 us-east-1，但您的账户不在 AWS 在该区域内，则在发出其他命令（例如）时，您必须指定您的账户已注册区域。AWS aws s3

 Note

本指南中提供的大多数命令示例都不包含该 `--region` 选项。

注册 RFC 每日电子邮件

您可以使用 RFC 摘要功能注册每日一封电子邮件，总结过去 24 小时内您账户中的 RFC 活动。RFC 摘要功能是一个简化的流程，可减少您收到的有关您账户的电子邮件通知的 RFCs 数量。RFC 摘要可能会降低您错过等待回复的操作的可能性。

要打开 RFC 摘要功能，请联系您的 AMS 云服务交付经理 (CSDM)。CSDM 会为您订阅。您可以请求将最多 20 个电子邮件地址（或别名）添加到 RFC 摘要电子邮件列表中。当前的电子邮件时间表固定在 09:00 UTC-8。

要关闭 RFC 摘要功能，请联系您的 CSDM 并提出您的请求。

如果您没有设置 RFC 摘要并想要有关您的通知 RFCs，或者您想要的信息 RFCs 比 RFC 摘要提供的内容更详细，请使用变更管理系统为您想要了解的每个 RFC 设置 CloudWatch 事件通知或电子邮件通知。有关设置 RFC 通知的信息，请参阅 [RFC 状态更改](#) 通知。

RFC 摘要中包含的主题包括以下内容：

- 等待买家批准：RFCs 处于 PendingApproval 状态正在等待您批准的列表
- 待处理的买家回复：RFCs 正在等待您回复 RFC 信件清单
- 待定 AWS 批准或回复：等待 AMS 回复或批准的清单 RFCs
- 已完成：列表状态 RFCs 为成功、失败、已取消和已拒绝

以下是 RFC 摘要示例：

什么是变更类型？

变更类型是指 AWS Managed Services (AMS) 变更请求 (RFC) 执行的操作，包括变更操作本身，以及变更类型（手动与自动）。AMS 拥有大量未被其他 Amazon 网络服务使用的变更类型。在提交变更请求 (RFC) 以部署、管理或访问资源时，您可以使用这些更改类型。

主题

- [自动和手动 CTs](#)
- [CT 批准要求](#)
- [更改类型版本](#)
- [创建变更类型](#)
- [更新变更类型](#)
- [仅限内部的变更类型](#)
- [更改类型架构](#)
- [管理变更类型的权限](#)
- [编辑变更类型中的敏感信息](#)
- [使用查询选项查找更改类型](#)

自动和手动 CTs

对更改类型的限制是它们是自动还是手动的，这是更改类型AutomationStatusId属性，在 AMS 控制台中称为执行模式。

自动变更类型具有预期的结果和执行时间，并通过AMS自动化系统运行，通常在一小时或更短的时间内（这在很大程度上取决于CT配置的资源）。手动更改类型并不常见，但它们的处理方式有所不同，因为它们要求 AMS 操作员在运行 RFC 之前对其进行操作。这有时意味着要与 RFC 提交者沟通，因此，手动更改类型需要不同的时间才能完成。

对于所有已安排的时间 RFCs，将未指定的结束时间写成指定的时间RequestedStartTime加上已提交的更改类型的ExpectedExecutionDurationInMinutes属性。例如，如果ExpectedExecutionDurationInMinutes为“60”（分钟），指定RequestedStartTime为2016-12-05T14:20:00Z（2016 年 12 月 5 日凌晨 4:20），则实际结束时间将设置为 2016 年 12 月 5 日凌晨 5:20。要查找ExpectedExecutionDurationInMinutes特定更改类型的，请运行以下命令：

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Note

在控制台中，RFCs 使用执行模式 = 手动进行调度，必须设置为将来至少 24 小时运行。此注意事项不适用于 AMS API/CLI，但 RFCs 至少提前 8 小时安排手动计划仍然很重要。

Note

使用“需要审核”时 CTs，AMS 建议您使用“尽快安排”选项（在控制台中选择“尽快”，在 API/CLI 中将开始和结束时间留空），因为这些选项 CTs 要求 AMS 操作员检查 RFC，并可能在批准和运行之前与您沟通。如果您安排这些活动 RFCs，请务必留出至少 24 小时的时间。如果在预定开始时间之前未获得批准，RFC 将被自动拒绝。

AMS 的目标是在四小时内对手动 CT 做出回应，并将尽快对应，但是 RFC 可能需要更长的时间才能真正运行。

有关手动 CTs 且需要 AMS 审核的内容的列表，请参阅控制台开发者资源页面上的更改类型 CSV 文件。

YouTube 视频：[如何查找 AMS 的自动变更类型 RFCs？](#)

要在 AMS 控制台中查找 CT 的执行模式，必须使用浏览更改类型搜索选项。结果显示匹配的变更类型或变更类型的执行模式。

要使用 AMS CLI 查找特定更改类型的，请运行以下命令：AutomationStatus

```
aws amscm --profile sam1 get-change-type-version --change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

您还可以在 [AMS 变更类型参考中查找变更类型](#)，该参考提供了有关所有 AMS 变更类型的信息。

Note

AMS 目前不 API/CLI 是 AWS 的一部分 API/CLI。To access the AMS API/CLI，您可以通过 AMS 控制台下载 AMS 开发工具包。

CT 批准要求

AMS CTs 总是有两个批准条件 AwsApprovalId，CustomerApprovalId 这表明 RFC 是要求 AMS 还是你或任何人批准执行。

批准条件与执行模式有些相关；有关详细信息，请参阅 [自动和手动 CTs](#)。

要找出 CT 的批准条件，您可以查看 [AMS 变更类型参考](#) 或运行 [GetChangeTypeVersion](#)。两者还将为您提供 CT AutomationStatusId 或执行模式。

您可以使用 AMS 控制台或使用以下命令进行批准 RFCs：

```
aws amscm approve-rfc --rfc-id RFC_ID
```

CT 批准条件

如果 CT 批准条件是	它需要获得批准	并且
AwsApprovalId: Required	AMS 变更类型系统，	无需采取行动。这种情况是自动化的典型情况 CTs。
AwsApprovalId: NotRequiredIfSubmitter	AMS 变更类型系统，没有其他人，如果提交的 RFC 是针对其提交时所针对的账户，	无需采取行动。这种情况是手动操作的典型情况，CTs 因为 AMS 操作员将始终对其进行审查。
CustomerApprovalId: NotRequired	AMS 变更类型系统，	如果 RFC 通过了语法和参数检查，则会自动获得批准。
CustomerApprovalId: Required	AMS 变更类型系统而你，	系统会向您发送通知，您必须通过回复通知或运行 ApproveRfc 操作来明确批准 RFC。
CustomerApprovalId: NotRequiredIfSubmitter	如果您提交了 RFC，AMS 将更改类型系统，而没有其他人可用。	如果 RFC 通过了语法和参数检查，则会自动获得批准。
紧急安全事件或补丁	AMS	已通过 auto 批准并实施。

更改类型版本

当对变更类型进行重大更新时，变更类型会被版本控制，版本也会发生变化。

使用 AMS 控制台选择更改类型后，您可以选择打开其他配置区域并选择更改类型版本。您也可以在 API/CLI 命令行中指定更改类型版本。您可能出于各种原因想要这样做，包括：

- 您知道您想要的“更新”更改类型的版本必须与您用于创建现在要更新的资源的“创建变更”类型的版本相匹配。例如，您可能有一个使用 ELB 创建的 Elastic Load Balancer (ELB) 实例。创建更改类型版本 1。要对其进行更新，请选择 ELB 更新版本 1。
- 您想要使用的更改类型版本中包含的选项与最新的更改类型不同。我们不建议这样做，因为 AMS 更新更改类型主要是出于安全考虑，我们建议您始终选择最新版本。

创建变更类型

创建变更类型 version-to-version 与更新变更类型相匹配。也就是说，用于置备资源的更改类型版本必须与您稍后用于修改该资源的更新更改类型的版本相匹配。例如，如果您使用创建 S3 存储桶更改类型为 2.0 的 S3 存储桶，之后又想提交 RFC 来修改该 S3 存储桶，则即使版本 3.0 中存在更新 S3 存储桶更改类型，也必须使用更新 S3 存储桶更改类型版本 2.0。

我们建议记录您在使用创建变更类型置备资源时使用的变更类型 ID 和版本，以备日后您想使用更新更改类型对其进行修改。

更新变更类型

AMS 提供更新更改类型，以更新使用“创建更改类型”创建的资源。更新更改类型必须 version-to-version 与最初用于置备资源的“创建”更改类型相匹配。

我们建议记录您在配置资源时使用的更改类型 ID 和版本，以便于更新。

YouTube 视频：[如何使用更新 CTs 来更改 AWS Managed Services \(AMS\) 账户中的资源？](#)

仅限内部的变更类型

您可以看到仅供内部使用的更改类型。这样您就可以知道 AMS 可以或正在采取哪些行动。如果您想提供仅限内部使用的变更类型，请提交服务请求。

例如，只有内部才有“管理”|“监控和通知”|“CloudWatch 警报抑制”|“更新 CT”。AMS 使用它来部署基础设施更新（例如修补），以关闭更新可能错误触发的警报通知。提交此 CT 后，您将在您的 RFC 列表中注意到 CT 的 RFC。部署在 RFC 中的任何仅限内部的 CT 都会显示在您的 RFC 列表中。

更改类型架构

所有变更类型都提供一个 JSON 架构，供您在创建、修改或访问资源时输入内容。架构提供参数及其描述，供您创建更改请求 (RFC)。

成功执行 RFC 会产生执行输出。为了进行配置 RFCs，执行输出包括一个“stack_id”，它表示中的堆栈 CloudFormation，可以在控制台中搜索。CloudFormation 执行输出有时包括创建的实例 ID 的输出，

该 ID 可用于在相应的 AWS 控制台中搜索该实例。例如，创建 ELB CT 执行输出包括一个可在中搜索的“stack_id”，CloudFormation 并输出一个可在亚马逊控制台中搜索 Elastic Load Balancing <stack-xxxx>的 key=elb value=。EC2

让我们来看看 CT 架构。这是 CodeDeploy 应用程序创建的架构，这是一个相当小的架构。有些架构的Parameter区域非常大。

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv000000000000",
      "type": "string",
      "enum": ["stm-sft6rv000000000000"]
    },
    "Name": {
      "description": "A name for the stack or stack component
;
this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
```

架构的第一部分向
AMS 提供有关请求的
更改类型的信息。

```

    categorize the resource.",
    "type": "array",
    "items": {
      "type": "object",
      "properties": {
        "Key": {
          "type": "string",
          "minLength": 1,
          "maxLength": 127
        },
        "Value": {
          "type": "string",
          "minLength": 1,
          "maxLength": 255
        }
      },
      "additionalProperties": false,
      "required": [
        "Key",
        "Value"
      ]
    },
    "minItems": 1,
    "maxItems": 7
  },
  "TimeoutInMinutes": {
    "description": "The maximum amount of time, in minutes,
to
    allow for execution of the change. This will not prolong
execution,
    but the RFC fails if the change is not completed in the
specified time.
    Valid values are 60 up to 360, for long-running
UserData.",
    "type": "number",
    "minimum": 0,
    "maximum": 60
  },
  "Parameters": {
    "description": "Specifications for the stack.",
    "type": "object",
    "properties": {
      "CodeDeployApplicationName": {

```

该 TimeoutInMinutes 参数允许您指定运行变更类型的边界时间。对于长时间运行 UserData，有效值为 60 到 360。

在“参数”部分中，您可以为正在创建的资源或您请求的操作指定设置。

“其他属性”部分让您知道哪些参数是必需的，哪些是可选的。

```

        "description": "The name of an AWS CodeDeploy
application.",
        "type": "string",
        "minLength": 1,
        "maxLength": 100,
        "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
    },
    "additionalProperties": false,
    "required": [
        "CodeDeployApplicationName"
    ]
},
"additionalProperties": false,
"required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
]
}

```

Note

此架构最多允许 7 个标签；但是，EFS EC2、RDS 和多层创建架构最多允许 50 个标签。

管理变更类型的权限

您可以使用自定义策略来限制哪些更改类型 (CTs) 可供不同的群组或用户使用。

要了解有关执行此操作的更多信息，请参阅 AMS 用户指南中的[设置权限](#)部分。

编辑变更类型中的敏感信息

AMS 更改类型架构提供参数属性，"metadata":"ams:sensitive":"true"该属性用于包含密码等敏感信息的参数。设置此属性后，所提供的输入将被遮盖。请注意，您无法设置此参数属性；但是，如果您正在与 AMS 合作创建更改类型，并且想要在输入时隐藏某个参数，则可以请求这样做。

使用查询选项查找更改类型

此示例演示如何使用 AMS 控制台查找要提交的 RFC 的相应更改类型。

您可以使用控制台或 API/CLI 来查找更改类型 ID (CT) 或版本。有两种方法，要么是搜索，要么是选择分类。对于这两种选择类型，您可以通过选择“最常用”、“最近使用”或“按字母顺序”对搜索进行排序。

YouTube 视频：[如何使用 AWS Managed Services CLI 创建 RFC，在哪里可以找到 CT 架构？](#)

在 AMS 控制台中，在 RFCs-> 创建 RFC 页面上：

- 选择“按更改类型浏览”（默认）后，可以：
 - 使用快速创建区域从 AMS 最受欢迎的 AMS 中进行选择 CTs。点击标签，将打开“运行 RFC”页面，并自动为您填充主题选项。根据需要完成其余选项，然后单击“运行”提交 RFC。
 - 或者，向下滚动到“所有变更类型”区域并开始选项框中键入 CT 名称，您不必输入确切或完整的更改类型名称。您还可以通过输入相关词语按更改类型 ID、分类或执行模式（自动或手动）搜索 CT。

选择默认卡片视图后，匹配的 CT 卡片会在您键入时出现，选择一张卡片并单击“创建 RFC”。选择表格视图后，选择相关的 CT，然后单击“创建 RFC”。两种方法都会打开“运行 RFC”页面。

- 或者，要浏览更改类型选择，请单击页面顶部的按类别选择以打开一系列下拉选项框。
- 选择“类别”、“子类别”、“物料”和“工序”。该更改类型的信息框显示在页面底部显示一个面板。
- 准备就绪后，按 Enter，将显示匹配的更改类型列表。
- 从列表中选择更改类型。该更改类型的信息框出现在页面底部。
- 选择正确的更改类型后，选择“创建 RFC”。

Note

必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用户指南》中的“AMS 信息资源”部分。您可能需要添加身份验证 `--profile` 选项；例如，`aws amsskms ams-cli-command --profile SAML`。您可能还需要添加该 `--region` 选项，因为所有 AMS 命令都将使用 `us-east-1`；例如。`aws amscm ams-cli-command --region=us-east-1`

 Note

AMS API/CLI (amscm 和 amsskms) 终端节点位于 AWS 弗吉尼亚北部区域。us-east-1根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令--region us-east-1时进行添加。如果这是您的身份验证方法--profile saml，则可能还需要添加。

要使用 AMS CM API (参见 [ListChangeTypeClassificationSummaries](#)) 或 CLI 搜索更改类型，请执行以下操作：

您可以使用筛选器或查询进行搜索。该 ListChangeTypeClassificationSummaries 操作具有Category、SubcategoryItem、和的“[筛选器](#)”选项Operation，但这些值必须与现有值完全匹配。要在使用 CLI 时获得更灵活的结果，可以使用--query选项。

使用 AMS CM API/CLI 更改类型筛选

属性	有效值	有效/默认条件	备注
ChangeTypeId	任何表示 a 的字符串 ChangeTypeId (例如：ct-abc123xyz7890)	Equals	有关更改类型 IDs，请参阅 更改类型参考 。 有关变更类型 IDs，请参阅查找变更类型或 CSIO。
类别	任何自由格式的文本	包含	不支持每个字段中的正则表达式。不区分大小写的搜索
子类别			
Item			
操作			

1. 以下是一些商品变更类型分类的示例：

以下命令列出了所有更改类型类别。

```
aws amscm list-change-type-categories
```


以下命令列出了属于指定类别的子类别。

```
aws amscm list-change-type-subcategories --category CATEGORY
```

以下命令列出了属于指定类别和子类别的项目。

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

2. 以下是一些使用 CLI 查询搜索变更类型的示例：

以下命令在 CT 分类摘要中搜索项目名称中包含“S3”的摘要，并以表格形式创建类别、子类别、项目、操作和更改类型 ID 的输出。

```
aws amscm list-change-type-classification-summaries --query
  "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
  [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-----+
|               ListChangeTypeClassificationSummaries               |
+-----+-----+-----+-----+-----+-----+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+-----+-----+-----+-----+-----+-----+-----+
```

3. 然后，您可以使用更改类型 ID 获取 CT 架构并检查参数。以下命令将架构输出到名为 creates3Params.schema.json 的 JSON 文件中。

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
  --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
  CreateS3Params.schema.json
```

有关使用 CLI 查询的信息，请参阅[如何使用--query 选项过滤输出](#)和查询语言参考[JMESPath 规范](#)。

4. 获得变更类型 ID 后，我们建议您验证变更类型的版本，以确保它是最新版本。使用以下命令查找指定更改类型的版本：

```
aws amscm list-change-type-version-summaries --filter
  Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

要查找AutomationStatus特定更改类型的，请运行以下命令：

```
aws amscm --profile sam1 get-change-type-version --change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

要查找ExpectedExecutionDurationInMinutes特定更改类型的，请运行以下命令：

```
aws amscm --profile sam1 get-change-type-version --change-type-id ct-14027q0sjyt1h --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

对 AMS 中的 RFC 错误进行故障排除

可以通过 CloudFormation 文档调查许多 AMS 配置 RFC 故障。参见 [AWS 疑难解答 CloudFormation：错误疑难解答](#)

以下各节提供了其他疑难解答建议。

AMS 中的“管理” RFC 错误

AMS “管理”类别更改类型 (CTs) 允许您请求访问资源并管理现有资源。本节介绍一些常见问题。

RFC 访问错误

- 确保您在 RFC 中指定的用户名和 FQDN 正确且存在于域中。有关查找您的 FQDN 的帮助，请参阅[查找您的 FQ DN](#)。
- 确保您为访问而指定的堆栈 ID 是 EC2 相关的堆栈。诸如 ELB 和 Amazon Simple Storage Service (S3) 之类的堆栈不适合访问 RFCs，而是使用您的只读访问权限角色来访问这些堆栈资源。有关查找堆栈 ID 的帮助，请参阅[查找堆栈 IDs](#)
- 请确保您提供的堆栈 ID 正确且属于相关账户。

有关其他访问 RFC 故障的帮助，请参阅[访问管理](#)。

YouTube 视频：[如何正确提出变更申请 \(RFC\) 以避免被拒绝和失败？](#)

RFC (手动) CT 调度错误

大多数更改类型是 ExecutionMode = Automated，但有些是 ExecutionMode = Manual，这会影响您应如何安排更改以避免 RFC 失败。

如果 RFCs 使用 AMS 控制台创建 R ExecutionMode FC，则必须将其设置为将来至少 24 小时内执行。此注意事项不适用于 AMS API/CLI，但 RFCs 至少提前 8 小时安排手动操作仍然很重要。

AMS 的目标是在四小时内对手动 CT 做出回应，并将尽快回复，但是 RFC 可能需要更长的时间才能真正执行。

RFCs 与手动更新一起使用 CTs

如果您要更新的堆栈类型有“更新”更改类型，则 AMS Operations 会拒绝“管理”|“其他 RFCs”|“其他”更新堆栈。

RFC 删除堆栈错误

RFC 删除堆栈失败：如果您使用管理 | 标准堆栈 | 堆栈 | 删除 CT，则将在 CloudFormation 控制台中看到带有 AMS 堆栈名称的堆栈的详细事件。您可以通过将堆栈与 AMS 控制台中的名称进行核对来识别堆栈。CloudFormation 控制台提供了有关故障原因的更多详细信息。

在删除堆栈之前，应考虑堆栈是如何创建的。如果您使用 AMS CT 创建堆栈，但未添加或编辑堆栈资源，则可以毫无问题地将其删除。但是，在提交针对堆栈的删除堆栈 RFC 之前，最好先从堆栈中移除所有手动添加的资源。例如，如果您使用完整堆栈 CT (HA Two Tier) 创建堆栈，则它会包含一个安全组- SG1。如果您随后使用 AMS 创建另一个安全组- SG2，并引用 SG1 已创建的作为完整堆栈一部分的新 SG2 安全组，然后使用删除堆栈 CT 删除该堆栈，则 SG1 不会像引用的那样将其删除 SG2。

Important

删除堆栈可能会带来意想不到和意想不到的后果。出于这个原因，AMS 倾向于*不*代表客户删除堆栈或堆栈资源。请注意，AMS 只会代表您删除无法使用相应的自动更改类型进行删除的资源（通过提交的管理 | 其他 | 其他 | 更新更改类型）。其它注意事项：

- 如果资源启用了“删除保护”，则如果您提交“管理 | 其他 | 其他 | 更新”更改类型，AMS 可以帮助解除此限制，并且删除保护后，您可以使用自动 CT 删除该资源。
- 如果堆栈中有多个资源，并且您只想删除堆栈资源的子集，请使用 CloudFormation 更新更改类型（参见载[CloudFormation 入堆栈：更新](#)）。您也可以提交“管理”|“其他”|“其他”|“更新”变更类型，如果需要，AMS 工程师可以帮助您制作变更集。
- 如果由于偏差而在使用 CloudFormation 更新 CT 时出现问题，AMS 可以提供帮助，方法是您提交管理 | 其他 | 其他 | 其他 | 更新来解决偏差（在 AWS CloudFormation 服务支持的范围 Management/Custom Stack/Stack From CloudFormation Template/Approve 内），并提供一个 ChangeSet 您可以随后使用自动 CT、变更集和更新进行验证和执行的更新。

AMS 维持上述限制，以帮助确保不会出现意外或意外的资源删除。

有关更多信息，请参阅 [AWS 疑难解答 CloudFormation：删除堆栈失败](#)。

RFC 更新 DNS 错误

多次 RFCs 更新 DNS 托管区域可能会失败，有些是无缘无故的。同时创建多个 RFCs 用于更新 DNS 托管区域（私有或公共）可能会 RFCs 导致某些区域失败，因为它们正在尝试同时更新同一个堆栈。由于另一个 RFC 已经更新堆栈而无法更新堆栈，AMS 变更管理会拒绝或失败 RFCs。AMS 建议您一次创建一个 RFC，等待 RFC 成功后再为同一个堆栈筹集一个新的 RFC。

RFC IAM 实体错误

AMS 将许多默认 IAM 角色和配置文件配置到 AMS 账户中，以满足您的需求。但是，您可能需要偶尔请求其他 IAM 资源。

提交 RFCs 请求自定义 IAM 资源的流程遵循手动标准工作流程 RFCs，但批准流程还包括安全审查，以确保适当的安全控制措施到位。因此，该过程通常比其他手册花费更长的时间 RFCs。要缩短这些产品的周期时间 RFCs，请遵循以下准则。

有关我们所说的 IAM 审查的含义以及它如何与我们的技术标准和风险接受流程对应的信息，请参阅[了解 RFC 安全评论](#)。

常见的 IAM 资源请求：

- 如果您要求提供与主要云兼容应用程序相关的政策，例如 CloudEndure，请参阅 AMS 预先批准的 IAM CloudEndure 政策：解压[WIGs 云端耐久着陆区示例](#)文件并打开 customer_cloud_endure_policy.json

Note

如果您想要更宽松的政策，请与您讨论您的需求，CloudArchitect/CSDM 并在必要时获得 AMS 安全审查和签署，然后再提交实施该政策的 RFC。

- 如果您想修改默认情况下由 AMS 在您的账户中部署的资源，我们建议您索要该资源的修改副本，而不是更改现有资源。
- 如果您正在为人类用户请求权限（而不是向用户授予权限），请将权限附加到某个角色，然后向该用户授予担任该角色的权限。有关执行此操作的详细信息，请参阅[临时 AMS 高级控制台访问权限](#)。

- 如果您需要特殊权限来执行临时迁移或工作流程，请在请求中提供这些权限的结束日期。
- 如果您已经与安全团队讨论了请求的主题，请尽可能详细地向您的 CSDM 提供他们批准的证据。

如果 AMS 拒绝 IAM RFC，我们会提供明确的拒绝理由。例如，我们可能会拒绝 IAM 策略创建请求，并解释该策略的哪些内容不合适。在这种情况下，您可以进行已确定的更改并重新提交请求。如果需要进一步明确请求的状态，请提交服务请求或联系您的 CSDM。

以下列表描述了 AMS 在审核您的 IAM 时试图降低的典型风险 RFCs。如果您的 IAM RFC 存在上述任何风险，则可能会导致 RFC 被拒绝。如果您需要例外，AMS 会要求您的安全团队批准。要寻求这样的例外，请与您的 CSDM 进行协调。

Note

AMS 可以出于任何原因拒绝对账户内的 IAM 资源进行任何更改。如对任何 RFC 拒绝有任何疑问，请通过服务请求与 AMS 运营部门联系，或联系您的 CSDM。

- 权限升级，例如允许您修改自己的权限或修改账户内其他资源的权限的权限。示例：
 - iam:PassRole 与另一个更具特权的角色一起使用。
 - 角色或用户对 attach/detach IAM 策略的权限。
 - 账户中 IAM 策略的修改。
 - 能够在管理基础架构的上下文中进行 API 调用。
- 修改向您提供 AMS 服务所需的资源或应用程序的权限。示例：
 - 修改 AMS 基础设施，例如堡垒、管理主机或 EPS 基础架构。
 - 删除日志管理 AWS Lambda 函数或日志流。
 - 删除或修改默认 CloudTrail 监控应用程序。
 - 目录服务活动目录 (AD) 的修改。
 - 禁用 CloudWatch (CW) 警报。
 - 修改作为 landing zone 一部分部署在账户中的委托人、策略和命名空间。
- 在最佳实践之外部署基础架构，例如允许在危及信息安全的状态下创建基础设施的权限。示例：
 - 创建公有或未加密的 S3 存储桶或公开共享 EBS 卷。
 - 公有 IP 地址的配置。
 - 修改安全组以允许广泛访问。

- 过于宽泛的权限会对应用程序造成影响，例如可能导致数据丢失、完整性丢失、配置不当或基础架构和账户内应用程序服务中断的权限。示例：
 - 禁用或重定向通过 APIs like `ModifyNetworkInterfaceAttribute` 或 `UpdateRouteTable` 的网络流量。
 - 通过将卷与托管主机分离来禁用托管基础架构。
- 服务权限不在 AMS 服务描述中，也不受 AMS 支持。

AMS 服务说明中未列出的服务不能用于 AMS 账户。要请求某项功能或服务的支持，请联系您的 CSDM。

- 权限不符合您的既定目标，因为它们要么过于慷慨，要么过于保守，要么应用于错误的资源。示例：
 - 对 `s3:PutObject` 具有强制性 KMS 加密的 S3 存储桶的权限请求，但没有相关密钥的 `KMS:Encrypt` 权限。
 - 与账户中不存在的资源相关的权限。
 - IAM，RFCs 其中 RFC 的描述似乎与请求不符。

“部署” RFC 错误

AMS “部署”类别更改类型 (CTs) 允许您请求将各种 AMS 支持的资源添加到您的账户。

创建资源的大多数 AMS CTs 都是基于 CloudFormation 模板的。作为客户，您可以只读访问所有 AWS 服务 CloudFormation，包括，您可以使用 CloudFormation 控制台根据 CloudFormation 堆栈描述快速识别代表您的堆栈的堆栈。失败的堆栈可能处于 `DELETE_COMPLETE` 状态。确定 CloudFormation 堆栈后，事件将向您显示创建失败的特定资源及其原因。

使用 CloudFormation 文档进行故障排除

大多数 AMS 配置都 RFCs 使用 CloudFormation 模板，该文档可能有助于进行故障排除。请参阅该 CloudFormation 模板的文档：

- 创建应用程序负载均衡器失败：[AWS::ElasticLoadBalancingV2::LoadBalancer \(Application Load Balancer\)](#)
- 创建 Auto Scaling 组：[AWS::AutoScaling::AutoScalingGroup \(Auto Scaling 组\)](#)
- 创建 memcached 缓存：[AWS::ElastiCache::CacheCluster \(缓存集群\)](#)
- 创建 Redis 缓存：[AWS::ElastiCache::CacheCluster \(缓存集群\)](#)
- 创建 DNS 托管区域 (与创建 DNS 私有/公用)：[AWS::Route53::HostedZone \(R53 托管区域\)](#)

- 创建 DNS 记录集 (与创建 DNS 私有/公共 DNS 一起使用) : [AWS::Route53::RecordSet](#) ([资源记录集](#))
- 创建 EC2 堆栈 : [AWS::EC2::Instance](#) ([弹性计算云](#))
- 创建弹性文件系统 (EFS): [AWS::EFS::FileSystem](#) ([弹性文件系统](#))
- 创建负载均衡器 : [AWS::ElasticLoadBalancing::LoadBalancer](#) ([Elastic Load Balancer](#))
- 创建 RDS 数据库: [AWS::RDS::DBInstance](#) ([关系数据库](#))
- 创建 Amazon S3 : [AWS::S3::Bucket](#) ([简单存储服务](#))
- 创建队列 : [AWS::SQS::Queue](#) ([简单队列服务](#))

RFC 创建错误 AMIs

亚马逊机器映像 (AMI) 是一种包含软件配置 (例如 , 操作系统、应用程序服务器和应用程序) 的模板。从 AMI 启动一个实例 , 该实例是在云中作为虚拟服务器运行的 AMI 的副本。AMIs 非常有用 , 是创建 EC2 实例或 Auto Scaling 组所必需的 ; 但是 , 您必须遵守一些要求 :

- 您为其指定的实例 `Ec2InstanceId` 必须处于停止状态 , RFC 才能成功。请勿为此参数使用 Auto Scaling 组 (ASG) 实例 , 因为 ASG 将终止已停止的实例。
- 要创建 AMS Amazon 系统映像 (AMI) , 必须从 AMS 实例开始。在使用该实例创建 AMI 之前 , 您必须确保它已停止并与其域断开连接 , 从而对其进行准备。有关详细信息 , 请参阅[使用 Sysprep 创建标准亚马逊系统映像](#)
- 您为新 AMI 指定的名称在账户中必须是唯一的 , 否则 RFC 将失败。[AMI | Create](#) 中描述了如何执行此操作 , 有关更多详细信息 , 请参阅和 [AWS AMI 设计](#)。

Note

有关为 AMI 创建做准备的其他信息 , 请参阅 [AMI | 创建](#)。

RFCs 正在创建 o EC2s r ASGs 错误

对于带超时 EC2 的 ASG 故障 , AMS 建议您确认所使用的 AMI 是否已自定义。如果是 , 请参阅本指南中包含的 AMI 创建步骤 (参见 [AMI | Create](#)) , 以确保正确创建 AMI。创建自定义 AMI 时的一个常见错误是未按照指南中的步骤重命名或调用 Sysprep。

RFCs 创建 RDS 错误

Amazon Relational Database (RDS) 失败的原因可能有很多，因为您在创建 RDS 时可以使用许多不同的引擎，而且每个引擎都有自己的要求和限制。在尝试创建 AMS RDS 堆栈之前，请仔细查看 AWS RDS 参数值，请参阅[创建DBInstance](#)。

要了解有关 Amazon RDS 的更多信息，包括大小建议，请参阅[亚马逊关系数据库服务文档](#)。

RFCs 创建 Amazon S3 错误

创建 S3 存储桶时的一个常见错误是该存储桶没有使用唯一的名称。如果您提交的 S3 存储桶 Create CT 的名称与之前提交的存储桶名称相同，则该存储桶将失败，因为已经存在与之同名的 S3 存储桶 BucketName。这将在 CloudFormation 控制台中详细介绍，您将在控制台中看到堆栈事件显示存储桶名称已在使用中。

RFC 验证与执行错误

在选定的 RFC 的 AMS 控制台 RFC 详细信息页面上，RFC 失败和相关消息的输出消息有所不同：

- 验证失败的原因仅在“状态”字段中可用
- 执行失败的原因可在执行输出和状态字段中找到。

RFC 错误消息

当您在列出的更改类型 (CTs) 中遇到以下错误时，可以使用这些解决方案来帮助您找到问题的根源并进行修复。

```
{"errorMessage":"An error has occurred during RFC execution. We are investigating the issue.", "errorType":"InternalError"}
```

如果您在参考以下故障排除选项后需要进一步的帮助，请通过 RFC 通信与 AMS 联系或创建服务请求。有关更多详细信息，请参阅[RFC 通信和附件（控制台）](#)和[在 AMS 中创建服务请求](#)。

工作负载摄取 (WIGS) 错误

Note

可以下载适用于 Windows 和 Linux 的验证工具，并直接在您的本地服务器上运行，也可以在 AWS 中的 EC2 实例上运行。这些内容可通过《AMS 高级应用程序开发者指南迁移工作负载：Linux 摄取前验证》和《[迁移工作负载：Windows 摄取前验证](#)》中找到。

- 确保目标 AMS 账户中存在 EC2 实例。例如，如果您已将非 AMS 账户的 AMI 共享到 AMS 账户，则必须先使用共享 AMI 在您的 AMS 账户中创建一个 EC2 实例，然后才能提交工作负载摄取 RFC。
- 检查连接到实例的安全组是否允许出口流量。SSM 代理需要能够连接到其公共端点。
- 检查该实例是否具有连接 SSM 代理的正确权限。这些权限附带了 `customer-mc-ec2-instance-profile`，您可以在 EC2 控制台中查看：

EC2 实例堆栈停止错误

- 检查实例是否已处于停止或已终止状态。
- 如果 EC2 实例处于联机状态并且您看到 `InternalError` 错误，请提交服务请求让 AMS 进行调查。
- 请注意，你不能使用更改类型管理 | 高级堆栈组件 | EC2 实例堆栈 | 停止 `ct-3mvvt2zkyveqj` 来停止 Auto Scaling 组 (ASG) 实例。如果您需要停止 ASG 实例，请提交服务请求。

EC2 实例堆栈创建错误

`InternalError` 消息来自 CloudFormation；一个 `CREATION_FAILED` 状态的原因。您可以按照以下步骤在堆栈事件中找到有关 CloudWatch 堆栈故障的详细信息：

- 在 AWS 管理控制台中，您可以在创建、更新或删除堆栈时查看堆栈事件列表。从该列表中，找到失败事件，然后查看该事件的状态原因。

状态原因可能包含来自 AWS CloudFormation 或特定服务的错误消息，可以帮助您了解问题。

- 有关查看堆栈事件的更多信息，请参阅[在 AWS 管理控制台上查看 AWS CloudFormation 堆栈数据和资源](#)。

EC2 实例卷恢复错误

当 EC2 实例卷恢复失败时，AMS 会创建内部故障排除 RFC。之所以这样做，是因为 EC2 实例卷恢复是灾难恢复 (DR) 的重要组成部分，AMS 会自动为您创建此内部故障排除 RFC。

创建内部疑难解答 RFC 后，会显示一个横幅，为您提供指向 RFC 的链接。此内部故障排除 RFC 可让您更清楚地了解 RFC 故障，与其提交 RFCs 导致相同错误的重试或手动联系 AMS 解决此故障，不如跟踪更改并知道 AMS 正在处理故障。这也降低了他们变更的 time-to-recovery (TTR) 指标，因为 AMS 操作员会主动处理 RFC 故障，而不是等待您的请求。

如何获得有关 RFC 的帮助

您可以联系 AMS 以确定失败的根本原因。AMS 的工作时间为每年 365 天、每周 7 天、每天 24 小时。

AMS 提供了多种途径供您寻求帮助或提出服务请求。

- 要询问信息或建议，或访问 AMS 托管的 IT 服务，或向 AMS 申请其他服务，请使用 AMS 控制台并提交服务请求。有关详细信息，请参阅[创建服务请求](#)。有关 AMS 服务请求的一般信息，请参阅[服务请求管理](#)。
- 要报告影响您的托管环境的 AWS 或 AMS 服务性能问题，请使用 AMS 控制台并提交事件报告。有关详细信息，请参阅[报告事件](#)。有关 AMS 事件管理的一般信息，请参阅[事件响应](#)。
- 有关您或您的资源或应用程序如何使用 AMS 的具体问题，或者要升级事件，请通过电子邮件发送以下一项或多封电子邮件：
 1. 首先，如果您对服务请求或事件报告回复不满意，请发送电子邮件至 CSDM：ams-csdm@amazon.com
 2. 接下来，如果需要升级，你可以发送电子邮件给 AMS 运营经理（但你的 CSDM 可能会这样做）：ams-opsmanager@amazon.com
 3. 进一步升级将向 AMS 局长提出：ams-director@amazon.com
 4. 最后，你可以随时联系 AMS 副总裁：ams-vp@amazon.com

AMS 中的直接更改模式

主题

- [直接更改模式入门](#)
- [安全性和合规性](#)

- [直接更改模式下的变更管理](#)
- [使用“直接更改”模式创建堆栈](#)
- [直接更改模式用例](#)

AWS Managed Services (AMS) 直接变更模式 (DCM) 通过提供对 AMS Advanced Plus 和高级账户的本地 AWS 访问权限来配置和更新 AWS 资源，从而扩展了 AMS 高级变更管理。使用 DCM，您可以选择使用原生 AWS API（控制台或 CLI/SDK）或 AMS Advanced 变更管理请求进行更改（RFCs），无论哪种情况，AMS 都完全支持资源及其更改，包括监控、补丁、备份、事件响应管理。通过 DCM 配置的资源在 AMS 服务知识管理系统 (SKMS) 中注册，加入 AMS 托管 Active Directory 域（如果适用），并运行 AMS 管理代理。使用现有工具（例如 SDK 和 CD AWS K）开发和部署 AMS CloudFormation 管理的堆栈。 CloudFormation

Note

直接更改模式不会删除 AMS 变更管理 RFCs。通过 DCM，您可以完全访问 AM RFCs S。

[观看 Akash 的视频以了解更多信息 \(6:30\)](#)

直接更改模式入门

首先检查先决条件，然后在符合条件的 AMS Advanced 账户中提交变更申请 (RFC)。

1. 确认您要在 DCM 中使用的账户是否符合要求：
 - 该账户是 AMS 高级增强版或高级版。
 - 该账户未启用 Service Catalog。我们目前不支持同时登录 DCM 和 Service Catalog 的账号。如果您已加入 Service Catalog 但对 DCM 感兴趣，请与您的云服务交付经理 (CSDM) 讨论您的需求。如果您决定从 Service Catalog 切换到 DCM，请在下面的变更请求中加入询问。有关 AMS 中的服务目录的详细信息，请参阅 [AMS 和服务目录](#)。
2. 使用管理 | 托管账户 | 直接更改模式 | 启用更改类型 (ct-3rd4781c2nnhp) 提交变更申请 (RFC)。有关演练示例，请参阅[直接更改模式 | 启用](#)。

处理 CT 后，将在指定账户中配置预定义AWSManagedServicesUpdateRole的 IAM 角色AWSManagedServicesCloudFormationAdminRole和。

3. 使用您的内部联合流程为需要 DCM 访问权限的用户分配相应的角色。

 Note

您可以指定任意数量的 SAMLIdentity提供商、AWS 服务和 IAM 实体（角色、用户等）来担任这些角色。您必须至少提供一个：SAMLIdentityProviderARNsIAMEntityARNs、或AWSServicePrincipals。有关更多信息，请咨询贵公司的 IAM 部门或 AMS 云架构师 (CA)。

直接更改模式 IAM 角色和策略

在账户中启用直接更改模式后，将部署以下新的 IAM 实体：

AWSManagedServicesCloudFormationAdminRole：此角色授予访问 CloudFormation 控制台、创建和更新 CloudFormation 堆栈、查看偏差报告以及创建和执行 CloudFormation ChangeSets 的权限。此角色的访问权限由您的 SAML 提供商管理。

部署并附加到角色的托管策略AWSManagedServicesCloudFormationAdminRole有：

- AMS 高级多账号 landing zone (MALZ) 应用程序账户
 - AWSManagedServices_CloudFormationAdminPolicy1
 - AWSManagedServices_CloudFormationAdminPolicy2
 - 此策略代表授予的权限AWSManagedServicesCloudFormationAdminRole。您和合作伙伴使用此政策授予对账户中现有角色的访问权限，并允许该角色启动和更新账户中的 CloudFormation 堆栈。这可能需要额外的 AMS 服务控制策略 (SCP) 更新，以允许其他 IAM 实体启动 CloudFormation 堆栈。
- AMS 高级单账号 landing zone (SALZ) 账户
 - AWSManagedServices_CloudFormationAdminPolicy1
 - AWSManagedServices_CloudFormationAdminPolicy2
 - cdk-legacy-mode-s3 次访问 [内联政策]
 - AWS ReadOnlyAccess 政策

AWSManagedServicesUpdateRole：此角色授予对下游 AWS 服务的受限访问权限 APIs。该角色采用托管策略部署，这些策略提供变更和非变更的 API 操作，但通常限制针对某些服务（例如 IAM、KMS、GuardDuty VPC、AMS 基础设施资源和配置等Create/Delete/PUT）的变更操作（例如）。此角色的访问权限由您的 SAML 提供商管理。

部署并附加到角色的托管策略AWSManagedServicesUpdateRole有：

- AMS 高级多账号 landing zone 应用程序账号
 - AWSManagedServicesUpdateBasePolicy
 - AWSManagedServicesUpdateDenyPolicy
 - AWSManagedServicesUpdateDenyProvisioningPolicy
 - AWSManagedServicesUpdateEC2而且 RDSPolicy
 - AWSManagedServicesUpdateDenyActionsOnAMSInfra政策
- AMS 高级单账号 landing zone 账号
 - AWSManagedServicesUpdateBasePolicy
 - AWSManagedServicesUpdateDenyProvisioningPolicy
 - AWSManagedServicesUpdateEC2而且 RDSPolicy
 - AWSManagedServicesUpdateDenyActionsOnAMSInfra政策 1
 - AWSManagedServicesUpdateDenyActionsOnAMSInfra政策 2

除此之外，托管策略AWSManagedServicesUpdateRole角色还ViewOnlyAccess附加了 AWS 托管策略。

安全性和合规性

安全与合规是 AMS Advanced 和您作为我们的客户的共同责任。AMS Advanced Direct Change 模式不会更改此项共同责任。

直接更改模式下的安全性

AMS Advanced 通过规范性的着陆区、变更管理系统和访问管理提供了额外的价值。使用“直接变更”模式时，此责任模型不会改变。但是，您应该注意其他风险。

直接更改模式“更新”角色（参见[直接更改模式 IAM 角色和策略](#)）提供了提升的权限，允许有权访问该角色的实体更改您账户中由 AMS 支持的 service 的基础设施资源。权限提升后，会存在不同的风险，具体取决于资源、service 和操作，尤其是在由于疏忽、错误或缺乏对内部流程和控制框架的遵守而导致错误更改的情况下。

根据AMS技术标准，已经确定了以下风险并提出了以下建议。有关 AMS 技术标准的详细信息可通过以下网址获取 AWS Artifact。要进行访问 AWS Artifact，请联系您的 CSDM 获取说明或前往[入门](#)。AWS Artifact

AMS-STD-001：标记

标准	它坏了吗	风险	建议
所有 AMS 拥有的资源都必须具有以下键值对 除上面列出的标签外，所有 AMS 拥有的标签都必须具有类似AMS*或MC*大小写的前缀。upper/lower/mix	是。中断了 CloudFormation、CloudTrail、EFS、OpenSearch、Logs、CloudWatch Alarms、SQS、SNS、SM、Tagging api，因为这些服务不支持限制 AMS 命名空间标记的aws:TagsKey 条件。 下表 AMS-STD-003 中给出的标准说明您可以更改环境和 AppId AppName，但不能更改 AMS 拥有的资源。无法通过 IAM 权限实现。	在 AMS 方面，对 AMS 资源进行错误标记可能会对您的资源的报告、警报和修补操作产生不利影响。	必须限制访问权限，才能对 AMS 团队以外的任何人的 AMS 默认标签要求进行任何更改。
不得根据您的更改请求删除 AMS 拥有的堆栈上的任何标签。	是的。CloudFormation 不支持限制 AMS 命名空间标签的aws:TagsKey 条件。		
不允许您在基础设施中使用 AMS 标签命名约定，如下表 AMS-STD-002 所述。	是。breaks for CloudWatch or CloudFormation CloudTrail、Amazon Elastic File System (EFS) OpenSearch、Logs、Amazon Systems		

标准	它坏了吗	风险	建议
	Queue S EC2 ervice (SQS)、Amazon Systems Manager (SSM)、标记 API ; 这些服务不支持aws:TagsKey 限制 AMS 命名空间标记的条件。		

AMS-STD-002：身份和访问管理 (IAM) Access Management

标准	它坏了吗	风险	建议
4.7 不得允许绕过变更管理流程 (RFC) 的操作，例如启动或停止实例、创建 S3 存储桶或 RDS 实例等。只要在分配的角色范围内执行操作，开发者模式账户和自助服务预置模式服务 (SSP) 就可以获得豁免。	是。自助操作的目的允许您绕过 AMS RFC 系统执行操作。	安全访问模式是 AMS 的核心技术方面，用于控制台或编程访问的 IAM 用户可以规避这种访问控制。AMS 变更管理不监控 IAM 用户的访问权限。访问权限 CloudTrail 仅限登录。	IAM 用户应有时间限制，并根据最低权限向其授予权限。 need-to-know

AMS-STD-003：网络安全

标准	它坏了吗	风险	建议
S2。EC2 实例上的弹性 IP 只能与正式的风险接受协议或内部团队的有效用例一起使用。	是。自助操作允许您关联和取消关联弹性 IP 地址 (EIP)。	向实例添加弹性 IP 会使其暴露在互联网上。这增加了信息泄露和未经授权活动的风险。	通过安全组阻止任何不必要的流量进入该实例，并验证您的安全组是否与该实例相连，以确保该实例仅

标准	它坏了吗	风险	建议
			在出于业务原因需要时才允许流量。
S14。可以允许属于同一客户的账户之间的 VPC 对等连接和终端节点连接。	是。无法通过 IAM 策略实现。	离开您的 AMS 账户的流量一旦超出账户边界，就不会受到监控。	我们建议仅与您拥有的 AMS 账户建立对等关系。如果您的用例需要这样做，请使用安全组和路由表来限制可以通过相关连接输出的流量范围、资源和类型。
AMS 基础 AMIs 可以在 AMS 管理的账户和非托管账户之间共享，前提是我们可以验证它们归同一个组织所有。AWS		AMIs 可能包含敏感数据，并且可能会泄露给非预期的帐户。	仅 AMIs 与您的组织拥有的账户共享，或者在组织外部共享之前验证用例和账户信息。

AMS-STD-007：日志记录

标准	它坏了吗	风险	建议
19. 任何日志都可以从一个 AMS 账户转发到同一客户的另一个 AMS 账户。	是。由于无法通过 IAM 策略验证客户账户属于同一个组织，因此客户日志可能不安全。	日志可能包含敏感数据，并且可能会泄露给非预期的帐户。	仅与组织管理的账户共享日志，或者在 AWS 组织外部共享之前验证用例和账户信息。我们可以通过多种方式进行验证，请咨询您的云服务交付经理 (CSDM)。
20。只有当非 AMS 账户归同一 AMS 客户所有（通过确认他们属于同一账户，或者将电子邮件域名与客户的公司名称和 PAYER 关联 AWS Organizat			

标准	它坏了吗	风险	建议
ions 账户进行匹配) 时，才能使用内部工 具将任何日志从 AMS 转发到非 AMS 账户。			

与您的内部授权和身份验证团队合作，相应地控制直接更改模式角色的权限。

直接更改模式下的合规性

直接更改模式与生产和非生产工作负载兼容。您有责任确保遵守任何合规标准（例如 PHI、HIPAA、PCI），并确保直接变更模式的使用符合您的内部控制框架和标准。

直接更改模式下的变更管理

变更管理是 AMS Advanced 用来实施变更请求的流程。变更请求 (RFC) 是由您或 AMS Advanced 通过 AMS Advanced 界面创建的对托管环境进行更改的请求，其中包含特定操作的 AMS 高级更改类型 (CT) ID。有关更多信息，请参阅[变更管理](#)。

 Note

直接更改模式不会移除 AMS 变更管理 RFCs，您仍然可以使用 DCM 完全访问 AMS RFCs。

AMS Direct Change 模式 (DCM) 通过提供对 AMS Advanced Plus 和高级账户的本机 AWS 访问权限来配置和更新 AWS 资源，从而扩展了 AMS 高级变更管理。通过 IAM 角色获得直接更改模式权限的用户可以使用原生 AWS API 访问权限在其 AMS Advanced 账户中配置和更改资源。用户仍然可以使用相同的 IAM 角色 RFCs 使用 AMS 高级变更管理。在这两种情况下，AMS 都完全支持资源及其更改，包括监控、补丁、备份、事件响应管理。在这些账户中没有适当角色的用户必须使用 AMS Advanced 变更管理 RFC 流程进行更改。

变更管理用例

出于安全考虑，AMS Advanced 中的某些更改只能通过变更管理变更申请 (RFC) 流程来完成。AWSManagedServicesCloudFormationAdminRole仅限于通过 CloudFormation (CFN) 采取的行动。有关如何通过 DCM 创建堆栈的更多信息，请参阅[使用 Direct Change 模式创建堆栈](#)。AWSManagedServicesUpdateRole仅限于以下操作。

有关每种变更类型的演练，包括[管理 | 托管账户 | 直接更改模式 | 启用 \(ct-3rd4781c2nnhp\) 变更类型](#)，请参阅“其他信息”部分，了解按分类划分的高级更改类型参考变更类型部分的相关变更类型。

服务	操作
AWS Key Management Service (AWS KMS)	更新
AWS Certificate Manager	创建
AWS Identity and Access Management (IAM)	任何
Site-to-Site VPN	任何
AMS 资源调度器	
AWS Backup	创建备份计划
AMS 工作负载接入 () WIGs	任何
AMS 出口过滤 (托管帕洛阿尔托)	
AMS 高级 MALZ 账户变更	
Amazon GuardDuty	
AMS 高级堆栈访问权限	任何
亚马逊 Elastic Block Store (EBS) 交易量	删除
亚马逊 Elastic Block Store (EBS) 默认加密	启用默认加密
亚马逊弹性计算云 (亚马逊 EC2)	更改主机名
亚马逊机器映像 (AMI)	删除、分享
亚马逊 EC2 安全组	任何
AMS 高级 SSP	
AWS 微软 AD 托管	
AMS 高级开发者模式	

服务	操作
Amazon Simple Storage Service (Amazon S3)	创建 S3 存储桶策略
AWS Systems Manager	创建

使用“直接更改”模式创建堆栈

为了让 AMS 管理堆栈AWSManagedServicesCloudFormationAdminRole，在 CloudFormation 使用中启动堆栈时有两个要求：

- 模板必须包含AmsStackTransform。
- 堆栈名称必须以前缀开头，stack-后跟一个 17 个字符的字母数字字符串。

 Note

要成功使用AmsStackTransform，您必须确认您的堆栈模板包含相应CAPABILITY_AUTO_EXPAND功能，以便 CloudFormation (CFN) 创建或更新堆栈。为此，您可以将CAPABILITY_AUTO_EXPAND作为创建堆栈请求的一部分传递。如果模板中包含此功能时未确认此功能，则 CFN 会拒绝该请求。AmsStackTransform如果您的模板中有转换，CFN 控制台可确保您通过此功能，但是当您通过 CFN 控制台与 CFN 进行交互时，可能会错过此功能。 APIs
无论何时使用以下 CFN API 调用，都必须通过此功能：

- [CreateChangeSet](#)
- [CreateStack](#)
- [UpdateStack](#)

使用 DCM 创建或更新堆栈时，将在堆栈上执行 CFN Ingest 和堆栈更新的 CTs 相同验证和增强，有关更多信息，请参阅载[CloudFormation 入指南、最佳实践](#)和限制。唯一的例外是，AMS 默认安全组 (SGs) 不会附加到 Auto Scaling 组中的任何独立 EC2 EC2 实例或 Auto Scaling 组 (ASGs) 中的实例。使用独立 EC2 实例或创建 CloudFormation 模板时 ASGs，可以附加默认实例 SGs。

 Note

现在可以使用创建和管理 IAM 角色 `AWSManagedServicesCloudFormationAdminRole`。

AMS 默认 SGs 具有入口和出口规则，允许实例成功启动，并允许稍后由 AMS 操作和您通过 SSH 或 RDP 进行访问。如果您发现 AMS 的默认安全组过于宽松，则可以创建自己的安全组，并 SGs 使用更严格的规则将其附加到您的实例，前提是它仍然允许您和 AMS 操作人员在事件发生期间访问该实例。

AMS 的默认安全组如下：

- `SentinelDefaultSecurityGroupPrivateOnly`: 可以通过此 SSM 参数在 CFN 模板中进行访问 `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- `SentinelDefaultSecurityGroupPrivateOnlyEgressAll`: 可以通过此 SSM 参数在 CFN 模板中进行访问 `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

AMS 转型

在 CloudFormation 模板 Transform 中添加声明。这将添加一个 CloudFormation 宏，用于在启动时验证堆栈并将其注册到 AMS。

JSON 示

```
"Transform": {
  "Name": "AmsStackTransform",
  "Parameters": {
    "StackId": {"Ref" : "AWS::StackId"}
  }
}
```

YAML 示例

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

在更新现有堆栈的模板时，还要添加该 Transform 语句。

JSON 示

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
  "Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

YAML 示例

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
```

TopicName: !Ref *TopicName*

堆栈名称

堆栈名称必须以前缀开头，stack-后跟一个 17 个字符的字母数字字符串。这是为了保持与在 AMS 堆栈上运行的其他 AMS 系统的兼容性 IDs。

以下是生成兼容堆栈的方法示例 IDs：

Bash：

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python：

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell：

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17 | %
{[char]$_})) )
```

直接更改模式用例

以下是直接更改模式的应用例：

通过以下方式提供和管理资源 CloudFormation

- 整合 CloudFormation 基于现有工具和流程。

持续的资源管理和更新

- 原子变化小，风险低。
- 本来需要通过手动或自动 RFC 进行的更改。
- 需要原生 AWS API 访问权限的工具。
- 如果您处于迁移阶段，则可以使用 DCM 角色。迁移团队利用 DCM 的权限来创建或修改堆栈。

- DCM 角色可以在 CI/CD 管道中用于构建新角色 AMIs、创建 Amazon ECS 任务等。

AMS 高级开发者模式

主题

- [AMS 高级开发者模式入门](#)
- [开发者模式下的安全性与合规性](#)
- [开发者模式下的变更管理](#)
- [在 AMS 开发者模式下配置基础架构](#)
- [AMS 开发者模式下的 Detective 控件](#)
- [在 AMS 开发者模式下记录、监控和事件管理](#)
- [AMS 开发者模式下的事件管理](#)
- [AMS 开发者模式下的补丁管理](#)
- [AMS 开发人员模式下的连续性管理](#)
- [AMS 开发者模式下的安全和访问管理](#)

AWS Managed Services (AMS) 开发者模式使用 AMS 高级增强版和高级版账户中的提升权限在 AMS 高级变更管理流程之外配置和更新 AWS 资源。AMS 高级开发人员模式通过利用 AMS 高级虚拟私有云 (VPC) 中的原生 AWS API 调用来实现这一点，使您能够在托管环境中设计和实施基础设施和应用程序。

使用启用了开发者模式的账户时，将为通过 AMS 高级变更管理流程或使用 AMS Amazon 系统映像 (AMI) 配置的资源提供连续性管理、补丁管理和变更管理。但是，这些 AMS 管理功能不适用于通过本机 AWS APIs 配置的资源。

您负责监控在 AMS Advanced 变更管理流程之外配置的基础设施资源。开发者模式与生产和非生产工作负载兼容。有了更高的权限，您就有更多的责任来确保遵守内部控制。

Important

只有使用 AMS Advanced 变更管理流程创建您使用开发者模式创建的资源才能由 AMS Advanced 管理。

开发者模式是您可以采用的 AMS 高级模式之一。有关更多信息，请参阅 [模式概述](#)。

AMS 高级开发者模式入门

了解使用 AMS 高级开发者模式的各种 AMS 高级账户以及如何成功实现开发者模式。

主题

- [开始使用 AMS 开发者模式之前](#)
- [AMS 开发者模式的先决条件](#)
- [如何实现 AMS 高级开发者模式](#)
- [AMS 高级开发者模式权限](#)

开始使用 AMS 开发者模式之前

在实现开发者模式之前，你应该知道几件事。

AMS Advanced 无法管理在 AMS Advanced 变更管理流程之外通过变更请求创建的 DevMode 账户中的现有堆栈或资源 (RFCs)。但是，当账户处于开启状态时 DevMode，AMS Advanced 将继续使用管理通过 AMS Advanced 变更管理流程配置的 RFCs 资源。

您不能先使用 DevMode 账户，然后再将其转换为 AMS Advanced 管理的应用程序账户。

AMS 开发者模式的先决条件

以下是实现开发者模式的先决条件：

- 您必须是 AMS Advanced 客户，并且至少有一个已注册的 AMS Advanced Plus 或高级账户。
- 您使用的任何账户都必须是 AMS Advanced Plus 或高级账户。
- 多账户登录区 (MALZ)：您必须使用 `AWSManagedServicesDevelopmentRole` 预定义的 AWS Identity and Access Management (IAM) 角色。你申请这个角色。下一节介绍如何获取开发者模式权限。
- 单账户登录区 (SALZ)：您必须使用 `customer_developer_role` 预定义的 AWS Identity and Access Management (IAM) 角色。你申请这个角色。下一节介绍如何获取开发者模式权限。

如何实现 AMS 高级开发者模式

您可以通过请求为符合条件的 AMS Advanced 账户配置预定义的 IAM 角色来实现开发者模式：

- MALZ：AWSManagedServicesDevelopmentRole

- SALZ : customer_developer_role

然后，您将该角色分配给联合网络中的相关用户。

AMS Advanced 建议您确保开发者模式的使用符合您的内部控制框架和标准，因为开发者模式会带来两个变革向量：AMS Advanced 管理的资源的 AMS Advanced 变更管理以及针对您（作为我们的客户）管理的资源的客户管理角色联合。虽然 AMS Advanced 流程仍然符合我们的声明，但可能需要更新客户流程和控制框架。

在您的 AMS 高级账户中实现开发者模式

1. 确认您要在开发者模式下使用的账户符合中列出的要求[AMS 开发者模式的先决条件](#)。
2. 使用变更类型 (CT) 管理 | 托管账户 | 开发者模式 | 启用（需要审核）提交变更申请 (RFC)。有关如何使用此 CT 的示例，请参阅[开发者模式 | 启用（需要审阅）](#)。

处理 CT 后，将在请求的账户中配置预定义的 IAM 角色

（AWSManagedServicesDevelopmentRole对customer_developer_role于MALZ，对于SALZ）。

3. 使用您的内部联合流程为需要开发者模式访问权限的用户分配相应的角色。

AMS Advanced 建议您限制访问权限，以防止不必要或未经批准地配置或更改资源。

AMS 高级开发者模式权限

预定义角色（适用AWSManagedServicesDevelopmentRole于

MALZ，customer_developer_role对于SALZ）授予在AMS高级VPC中创建应用程序基础设施资源的权限，包括IAM角色，同时限制访问由AMS Advanced运营的共享服务组件（例如，管理主机、域控制器、趋势科技EPS、堡垒和不支持的AWS服务）。该角色还限制对以下内容的访问AWS服务：Amazon GuardDuty、AWS Organizations AWS Directory Service APIs、和AMS高级日志。

虽然该角色允许您创建其他IAM角色，但开发人员模式访问权限中包含的相同权限限制也适用于由创建的任何IAM角色AWSManagedServicesDevelopmentRole。

开发者模式下的安全性与合规性

安全与合规是AMS Advanced和您作为我们的客户的共同责任。AMS Advanced Developer模式将您在变更管理流程之外配置的资源或通过变更管理配置但使用开发者模式权限更新的资源的共同责任转移给您。有关分担责任的更多信息，请参阅[AWS Managed Services](#)。

注意事项：

- DevMode 允许您和您的授权团队绕过 AMS 安全的核心 deny-by-default 原则。必须权衡自助服务、减少等待 AMS 的优点和缺点，任何人都可以在安全团队不知情的情况下执行意想不到的破坏性操作。用于启用开发模式和直接更改模式的自动更改类型已公开，您组织中的任何授权人员都可以运行这些类型 CTs 并启用这些模式。
- 您负责从您的用户群中管理 CT 执行权限。
- AMS 不管理 CT 执行权限

建议

- 保护
 - 客户可以通过权限阻止访问此 CT，请参阅[使用 IAM 角色策略声明限制权限](#)
 - 通过实施代理（例如 ITSM 系统）来阻止对此 CT 的访问
 - 利用服务控制策略 (SCPs)，根据需要阻止策略和行为，请参阅[AMS Preventative 和 Detective Controls 库](#)
- 检测
 - 监视你的 RFC 是否正在执行这些内容 CTs（启用开发者模式 ct-1opjmhuddw194 和直接更改模式，启用 ct-3rd4781c2nnhp）并做出相应的响应
 - 查看 and/or 您的账户是否存在 IAM 资源，以确定部署了开发者模式或直接变更模式的账户
- 回应
 - 根据需要在开发者模式下移除账户

开发者模式下的安全性

AMS Advanced 通过规范性的着陆区、变更管理系统和访问管理提供了额外的价值。使用开发者模式时，AMS Advanced 的安全值通过使用与标准 AMS Advanced 账户相同的账户配置来保持 AMS Advanced 的安全值，该账户配置与 AMS Advanced 的基准安全强化网络相同。网络受角色中强制执行的权限边界的保护（AWSManagedServicesDevelopmentRole 对于 MALZ，customer_developer_role 对于 SALZ），这限制了用户破坏在设置账户时建立的保护。

例如，具有该角色的用户可以访问 Amazon Route 53，但是 AMS 高级内部托管区域受到限制。对创建的 IAM 角色强制执行相同的权限边界 AWSManagedServicesDevelopmentRole，从而限制用户破坏账户加入 AMS Advanced 时建立的保护。AWSManagedServicesDevelopmentRole

开发者模式下的合规性

开发者模式与生产和非生产工作负载兼容。您有责任确保遵守任何合规标准（例如 PHI、HIPAA、PCI），并确保开发人员模式的使用符合您的内部控制框架和标准。

开发者模式下的变更管理

变更管理是 AMS Advanced 服务用来实施变更请求的流程。变更请求 (RFC) 是您或 AMS Advanced 通过 AMS Advanced 界面创建的对托管环境进行更改的请求，其中包括特定操作的更改类型 (CT) ID。有关更多信息，请参阅 [更改管理模式](#)。

在授予开发者模式权限的 AMS Advanced 账户中，不强制执行变更管理。已获得 IAM 角色的开发者模式权限 (`AWSManagedServicesDevelopmentRole` 适用于 `MALZ`、`customer_developer_role` `SALZ`) 的用户可以使用原生 AWS API 访问权限在其 AMS 高级账户中配置和更改资源。在这些账户中没有相应角色的用户必须使用 AMS Advanced 变更管理流程进行更改。

 Important

只有使用 AMS Advanced 变更管理流程创建您使用开发者模式创建的资源才能由 AMS Advanced 管理。对于在 AMS Advanced 变更管理流程之外创建的资源，提交给 AMS Advanced 的更改请求会被 AMS Advanced 拒绝，因为这些请求必须由您处理。

自助配置服务 API 限制

开发者模式支持所有 AMS Advanced 自行配置服务。对自行配置服务的访问受每项服务的相应用户指南部分中概述的限制。如果您的开发者模式角色无法使用自行配置的服务，则可以通过开发者模式更改类型请求更新的角色。

以下服务不提供对服务的完全访问权限 APIs：

自配服务在开发者模式下受到限制

服务	备注
Amazon API Gateway	允许所有网关 APIs 呼叫，但以下情况除外 <code>SetWebACL</code> 。
Application Auto Scaling	只能注册或取消注册可扩展目标，以及放置或删除扩展策略。

服务	备注
AWS CloudFormation	无法访问或修改名称前缀为的 CloudFormation 堆栈。mc -
AWS CloudTrail	无法访问或修改名称前缀为的 CloudTrail 资源。ams - and/or mc -
Amazon Cognito (用户池)	无法关联软件令牌。 无法创建用户池、用户导入任务、资源服务器或身份提供商。
AWS Directory Service	Connect和WorkSpaces 服务只需要 Directory Service 执行以下操作。开发者模式权限边界策略拒绝所有其他 Directory Service 操作： • ds:AuthorizeApplication • ds:CreateAlias • ds:CreateIdentityPoolDirectory • ds>DeleteDirectory • ds:DescribeDirectories • ds:GetAuthorizedApplication Details • ds:ListAuthorizedApplications • ds:UnauthorizeApplication 在单账户 landing zone 账户中，边界策略明确拒绝访问 AMS Advanced 用于维护对启用开发模式的账户的访问权限的 AMS Advanced 托管目录。

服务	备注
Amazon Elastic Compute Cloud	无法访问包含以下字符串 EC2 APIs 的 Amazon : DhcpOptions Gateway、Subnet、VPC、和VPN。 无法访问或修改标签前缀为AMS、、mcManagementHostASG 、 and/or sentinel的 Amazon EC2 资源。
亚马逊 EC2 （ 报告 ）	仅授予查看权限（ 不能修改 ）。注意：Amazon EC2 Reports 正在更新。“报告”菜单项将从 Amazon EC2 控制台导航菜单中删除。要在删除后查看您的 Amazon EC2 使用情况报告，请使用 AWS Billing 和成本管理控制台。
AWS Identity and Access Management (IAM)	无法删除现有权限界限，也无法修改 IAM 用户密码策略。 除非您使用正确的 IAM 角色（ 对于 MALZ ，对AWSManagedServicesDevelopmentRole 于 S ALZ ）, customer_developer_role 否则无法创建或修改 IAM 资源。 无法修改前缀为:ams、、mccustomer_deny_policy 、 and/or sentinel的 IAM 资源。 创建新的 IAM 资源（ 角色、用户或群组 ）时，必须附加权限边界（ MALZ: AWSManagedServicesDevelopmentRolePermissionsBoundary 、 SALZ:ams-app-infra-permissions-boundary ）。
AWS Key Management Service (AWS KMS)	无法访问或修改 AMS 高级管理的 KMS 密钥。
AWS Lambda	无法访问或修改前缀为的 AWS Lambda 函数。AMS

服务	备注
CloudWatch 日志	无法访问名称前缀为:mc、 、awslambda、 and/or AMS的 CloudWatch 日志流。
Amazon Relational Database Service (Amazon RDS)	无法访问或修改名称前缀为:mc - 的亚马逊关系数据库服务 (Amazon RDSDBs) 数据库 ()。
AWS Resource Groups	只能访问GetList、和Search资源组 API 操作。
Amazon Route 53	无法访问或修改 Route53 AMS 高级维护的资源。
Amazon S3	无法访问名称前缀为:ams - *、 、ams或的 Amazon S3 存储桶。ms - a mc - a
AWS Security Token Service	唯一允许的安全令牌服务 API 是DecodeAuthorizationMessage 。
Amazon SNS	无法访问名称前缀为:AMS-Energon-Topic 、或的 SNS 主题。MMS-Topic
AWS Systems Manager 经理 (SSM)	无法修改以ams、mc或为前缀的 SSM 参数。svc 无法SendCommand 对标签前缀为或的 Amazon EC2 实例使用 SSM API。ams mc
AWS 标记	您只能访问前缀为的 AWS 标记 API 操作。Get

服务	备注
AWS Lake Formation	以下 AWS Lake Formation API 操作被拒绝： - lakeformation:DescribeResource - lakeformation:GetDataLakeSettings - lakeformation:DeregisterResource - lakeformation:RegisterResource - lakeformation:UpdateResource - lakeformation:PutDataLakeSettings
Amazon Elastic Inference	您只能调用 Elastic Inference API 操作。elastic-inference:Connect 此权限包含在customer_sagemaker_admin_policy 所附的权限中customer_sagemaker_admin_role 。此操作允许您访问 Elastic Inference 加速器。
AWS Shield	无法访问任何此服务 APIs 或控制台。
Amazon Simple Workflow Service	无法访问任何此服务 APIs 或控制台。

在 AMS 开发者模式下配置基础架构

在启用开发者模式的账户中AWSManagedServicesDevelopmentRole，没有开发者模式 IAM 角色的用户必须遵循利用 AMS Advanced 的 AMS 高级变更管理流程。AMIs角色正确 (MALZ:AWSManagedServicesDevelopmentRole、SALZ:customer_developer_role) 的用户可以使用 AMS Advanced 变更管理系统和 AMS Advanced，AMIs 但不是必需的。

 Note

未通过 AWS AMS 高级工作负载摄取处理或在 AMS 高级账户中创建的 AMI 将不包含 AMS Advanced 所需的配置。

AMS 开发者模式下的 Detective 控件

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。

在 AMS 开发者模式下记录、监控和事件管理

对于在 AMS Advanced 变更管理流程之外配置的资源，或者通过变更管理配置然后由使用开发者模式权限的账户更改的资源，不可使用记录、监控和事件管理。

AMS 开发者模式下的事件管理

事件响应时间没有变化。对于在变更管理流程之外配置的资源，或者通过变更管理配置的资源，然后由使用开发者模式权限的账户进行更改，应尽力解决事件。

Note

AMS 服务等级协议 (SLA) 不适用于在 AMS 变更管理系统之外创建或更新的资源（包括更改请求或 RFCs），包括开发人员模式；因此，在开发者模式下更新或创建的资源会自动降级为 P3，AMS 支持是尽力而为。

AMS 开发者模式下的补丁管理

补丁管理不适用于在 AMS Advanced 变更管理流程之外置备的资源，也不可用于通过变更管理配置然后由使用开发者模式权限的账户更改的资源。修补时间：

- 对于重要的安全更新：供应商发布通过变更管理配置然后由使用开发者模式权限的账户更改的资源后 10 个工作日内。
- 重要更新：供应商发布通过变更管理配置的资源，然后由使用开发者模式权限的账户进行更改的资源后 2 个月内。

AMS 开发人员模式下的连续性管理

连续性管理不适用于在 AMS Advanced 变更管理流程之外配置的资源，也不可用于通过变更管理配置然后由使用开发者模式权限的账户更改的资源。

对于在 AMS Advanced 变更管理流程之外配置的资源，或者对于通过变更管理配置然后由使用开发者模式权限的账户更改的资源，环境恢复启动时间可能长达 12 小时。

AMS 开发者模式下的安全和访问管理

防恶意软件保护是指您对在 AMS Advanced 变更管理流程之外配置的资源，或者对通过变更管理配置然后由使用开发者模式权限的账户更改的资源的责任。对未通过 AMS 高级变更管理配置的亚马逊弹性计算云 (Amazon EC2) 实例的访问可能由密钥对控制，而不是提供联合访问权限。

AMS 中的自助服务配置模式

AWS Managed Services (AMS) 自助服务配置 (SSP) 模式提供对 AMS 托管账户中原生 AWS 服务和 API 功能的完全访问权限。您可以通过标准化的、范围缩小的 AWS Identity and Access Management 角色来访问服务。AMS 提供服务请求和事件管理。警报、监控、记录、修补、备份和变更管理是您的责任。在许多情况下，自助服务配置服务 (SSP) 是自我管理或无服务器的，不需要管理某些操作任务，例如修补。在 AMS 护栏定义的环境边界内使用这些服务将使您受益，任何 IAM 更改（包括服务关联角色、服务角色、跨账户角色或策略更新）都需要获得 AMS Operations 的批准，以维护平台的基准安全性。您可以利用 CloudFormation 模板自动部署这些服务，但并非所有 SSP 服务都支持此功能。

Important

在您的 AWS Managed Services (AMS) 账户中使用 SSP 模式访问和使用 AWS 服务，但限制如上所述。

在您 AWS 服务的 AMS 账户中，有些无需管理 AMS 即可使用。本节介绍了自助服务配置模式服务（简称 SSP）、如何将它们添加到您的 AMS 账户以及 FAQs 每项服务。

自助配置服务按原样提供，您负责管理这些服务。AMS 不为与这些服务相关的资源提供警报、监控、日志记录或修补。AMS 提供 IAM 角色，使您能够安全地使用 AMS 账户中的服务。AMS SLAs 不适用。

对于您通过自助服务配置的资源，AMS 通过服务请求提供事件管理、侦探控制和护栏、报告、指定资源（云服务交付经理和云架构师）、安全和访问权限以及技术支持。此外，在适用的情况下，您负责在 AMS 变更管理系统之外配置或配置的资源连续性管理、补丁管理、基础设施监控和变更管理。

AMS 中的 SSP 模式入门

自助配置是您可以使用的多账户着陆区 (MALZ) 的 AMS 模式之一。有关更多信息，请参阅 [模式概述](#)。

为了提供自助服务配置功能，AMS 创建了具有权限界限的提升的 IAM 角色，以限制直接 AWS 服务访问的意外更改。这些角色并不能阻止所有更改，您必须遵守内部控制和合规政策，并验证所有 AWS 服务使用的角色是否符合所需的认证。这是自助配置模式。有关 AWS 合规性要求的详细信息，请参阅 [AWS 合规性](#)。

要向您的多账户 landing zone Application 账户添加自助配置 AWS 服务，请按照服务的说明使用管理 | 服务 | 自配置服务 | 添加变更类型 (CT)，即需要审阅的 CT 或自动 CT。

Note

要请求 AMS 提供额外的自助服务配置服务，请提交服务请求。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon API Gateway

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon API Gateway 功能。[Amazon API Gateway](#) 是一项完全托管的服务，让开发人员可以轻松以任何规模创建、发布、维护、监控和保护 APIs。[使用 AWS 管理控制台可以创建 REST WebSocket APIs](#)，它可以作为应用程序访问后端服务的数据、业务逻辑或功能的前门，例如在亚马逊弹性计算云 (Amazon EC2) 上运行的工作负载、在上面运行的代码 AWS Lambda、任何 Web 应用程序或实时通信应用程序。

API Gateway 可处理接受和处理多达数十万个并发 API 调用所涉及的所有任务，包括流量管理、授权和访问控制、监控以及 API 版本管理。API Gateway 没有最低费用或启动成本。您只需为收到的 API 调用和传出的数据量付费，而且，借助 API Gateway 分层定价模型，您可以随着 API 使用量的扩大而降低成本。要了解更多信息，请参阅 [Amazon API Gateway](#)。

常见问题：AMS 中的 API Gateway

问：如何使用我的 AMS 账户申请访问亚马逊 API Gateway？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 API Gateway。此 RFC 为您的账户配置以下 IAM 角色：`customer_apigateway_author_role` 和 `customer_apigateway_cloudwatch_role`。在您的账户中配置后，您必须在联合解决方案中加入角色。

问：在我的 AMS 账户中使用 Amazon API Gateway 有哪些限制？

- API Gateway 配置仅限于不带前缀AMS-或MC-前缀的资源，以防止对 AMS 基础设施进行任何修改。
- CREATE的权限已禁 VPCLink 用，以防止不受监管地创建弹性负载均衡器。如果 VPCLinks 需要，请参阅 App [lication Load Balancer | Create](#)。

问：在我的 AMS 账户中使用 Amazon API Gateway 有哪些先决条件或依赖关系？

这取决于您要部署的 API Gateway 的类型。它可以是独立服务，但也可以请求访问现有服务（例如，网络负载均衡器）。

使用 AMS SSP 在你的 AMS 账户中配置 Alexa for Business

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Alexa for Business 功能。Alexa for Business 是一项服务，可让您的组织和员工使用 Alexa 来完成更多工作。有了 Alexa for Business，您可以使用 Alexa 作为智能助手，在会议室、办公桌前，甚至使用已经在家中或旅途中使用的 Alexa 设备提高工作效率。IT 和设施经理可以使用 Alexa for Business 来衡量和提高工作场所现有会议室的利用率。

要了解更多信息，请参阅 [Alexa for Business](#)。

AWS Managed Services 中的 Alexa for Business 常见问题解答

问：如何使用我的 AMS 账户申请访问 Alexa for Business？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_alex_console_role。还customer_alex_device_setup_user为 Alexa for Business 提供的设备设置工具创建了 A；然后可以使用此设备设置工具来设置您的设备。在您的账户中配置角色后，您必须在联合解决方案中加入角色。

Alexa for Business 网关使您可以将 Alexa for Business 连接到思科 Webex 和 Poly Group 系列终端，从而使用语音控制会议。网关软件在您的本地硬件上运行，可以安全地将会议指令从 Alexa for Business 代理到您的思科终端。网关需要两对 AWS 凭据才能与 Alexa for Business 通信。我们提供两个访问受限的IAM用户：customer_alex_gateway_installer_user以及customer_alex_gateway_execution_user您的Alexa for Business网关，一个用于安装网关，一个用于操作网关；可以通过提交带有部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建实体或策略（需要审查）更改类型 (ct-3dpg8mdd9jn1r) 的RFC来申请。

 Note

要生成使用情况报告并将其发送到 Amazon S3，请在自配置服务 RFC 中指定 Amazon S3 存储桶名称。

问：在我的 AMS 账户中使用 Alexa for Business 有哪些限制？

没有任何限制。Alexa for Business 的全部功能可通过 Alexa for Business 自行配置服务角色获得。

问：在我的 AMS 账户中使用 Alexa for Business 有哪些先决条件或依赖条件？

- 如果您打算使用 E WPA2 nterprise Wi-Fi 来设置共享设备，请在设备设置工具中指定此网络安全类型，该工具需要使用。AWS 私有证书颁发机构
- AMS 仅创建以命名空间“A4B”开头的密钥。这仅限于此命名空间。

问：Alexa for Business 的哪些功能需要 RFCs单独使用？

要向 Alexa for Business 注册 Alexa 语音服务 (AVS) 设备，请提供对 Alexa 内置设备制造商的访问权限。为此，需要在 Alexa for Business 控制台中创建一个 IAM 角色，该角色可以使用管理 | 其他 | 其他更改类型进行部署。这允许 AVS 设备制造商代表您在 Alexa for Business 上注册和管理设备。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon AppStream 2.0

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon AppStream AppStream 2.0 (2.0) 功能。AppStream 2.0 允许您将桌面应用程序移至 AWS，而无需重写它们。您可以在 AppStream 2.0 上安装应用程序，设置启动配置，并向用户提供应用程序。AppStream 2.0 提供了多种虚拟机选项，因此您可以选择最符合应用程序要求的实例类型，并设置自动缩放参数，以便轻松满足最终用户的需求。AppStream 2.0 使您能够在自己的网络中启动应用程序，这意味着您的应用程序可以与现有 AWS 资源进行交互。

Amazon AppStream 2.0 使您能够使用映像生成器快速轻松地安装、测试和更新应用程序。支持在微软 Windows Server 2012 R2、Windows Server 2016 或 Windows Server 2019 上运行的任何应用程序，你无需进行任何修改。测试完成后，您可以设置应用程序启动配置、默认用户设置，并发布图像以供用户访问。

要了解更多信息，请参阅 [AppStream 2.0](#)。

AppStream AWS Managed Services 常见问题中的 2.0

问：如何在 AMS 账户中申请访问 AppStream 2.0？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-3qe6io8t6jtny) 更改类型提交 RFC，请求访问 AppStream 2.0。此 RFC 为您的账户配置以下 IAM 角色:customer_appstream_console_role。

还部署 A customer_appstream_stream_role 以流式传输要求用户使用 Active Directory 登录凭据进行身份验证的应用程序。

在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问：在我的 AMS 账户中使用 AppStream 2.0 有什么限制？

- 以下功能必须由 AMS Support 团队进行配置，并且需要特定 RFCs。有关请求其他功能的说明可在第 4 节中找到。
 - 从接口 VPC 终端节点创建和流式传输。
 - 支持 Amazon S3 终端节点，用于主文件夹和应用程序设置在私有网络上的持久性。
 - 创建并选择将在所有队列流实例上可用的 IAM 角色。
 - 加入 AppStream 2.0 舰队和图像生成器微软 Active Directory 域名。
 - 创建 AppStream 2.0 自定义使用情况报告。
 - 目前不支持自定义品牌。

问：在我的 AMS 账户中使用 AppStream 2.0 有哪些先决条件或依赖关系？

在向板载 AppStream 2.0 提交 RFC 时，请包括用于 AppStream 2.0 使用情况报告的 Amazon S3 存储桶名称。存储桶名称将添加到加customer-appstream-usagereports-policy载 AppStream 2.0 时创建的。

问：哪些 AppStream 2.0 功能需要单独使用 RFCs？

- 要为 AppStream 2.0 选择接口 VPC 终端节点，请提交管理 | 其他 | 其他 | 更新更改类型 RFC 以在您的账户中创建 VPC 终端节点。有关为 2.0 创建自定义终端节点的步骤，请参阅 AppStream 2.0 用户指南中的[从接口 VPC 终端节点创建和流式传输](#)。AppStream
- 通过使用“管理 | 其他 | 其他 | 其他 | 创建更改类型 RFC”请求 Amazon S3 VPC 终端节点，即可配置对主文件夹和应用程序设置在私有网络上的持久性的支持。RFC 必须包括分别托管主文件夹内容的目标 Amazon S3 存储桶或应用程序设置 Amazon S3 存储桶。此 RFC 将为 AppStream 2.0 提

供其访问 Amazon S3 VPC 终端节点所需的权限。有关为流创建自定义终端节点的步骤，请参阅 AppStream 2.0 用户指南中的[将 Amazon S3 VPC 终端节点用于主文件夹和应用程序设置持久性](#)。

- 要创建和选择将在所有队列流实例上可用的 IAM 角色，请提交部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建实体或策略 (需要审查) 更改类型 (ct-3dpd8mdd9jn1r) RFC 请求使用所需策略的 IAM 角色。IAM 角色名称应始终以前缀 “customer_appstream” 开头。
- 要将 Amazon AppStream 2.0 舰队和映像生成器加入到 Microsoft Active Directory 中的域中，可以在 Active Directory (AD) 中提交 “管理 | 其他 | 其他 | 其他 | 更新” 更改类型 RFC 以创建服务账户。加入 Microsoft Active Directory 所需的最低[权限在授予创建和管理 Active Directory 计算机对象的权限](#)的 AppStream 2.0 文档中定义。
- 要创建自定义 AppStream 2.0 使用情况报告，请提交管理 | 其他 | 其他 | 创建更改类型 RFC，请求以下内容：
 - “AppStreamUsageReports” CFN 堆栈创建
 - 在账户中配置 “customer_appstream_usagereports_role”
 - 此外，请提供以下详细信息：
 - 提供 CRON 表达式来安排 Crawler 运行。默认情况下，每天为世界标准时间 23:00。
 - 用于获取 Athena 查询结果的 Amazon S3 存储桶 ARN。这个存储桶应该有前缀：aws-athena-query-results
 - 适用于 AppStream 2.0 的 Amazon S3 存储桶 ARN 使用情况报告日志。

配置角色后，将该角色加入您的联合解决方案并登录，然后使用使用情况报告角色访问 AWS GlueAWS Glue 和 Athena 以生成自定义报告。有关使用 AppStream 2.0 使用情况报告的详细信息，请参阅 2.0 文档中的[创建自定义报告和分析 AppStream AppStream 2.0 使用情况数据](#)。

使用 AMS SSP 在你的 AMS 账户中配置亚马逊 Athena

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 Athena (Athena) 功能。Athena 是一项交互式查询服务，可帮助您使用标准 SQL 分析 Amazon S3 中的数据。Athena 没有服务器，没有要管理的基础设施，只需为运行的查询付费。您指向 Amazon S3 中的数据，定义架构，然后开始使用标准 SQL 进行查询。大多数结果会在几秒钟内送达。有了 Athena，无需 extract-transform-load 复杂的 (ETL) 任务来准备数据以供分析。这使得任何具有 SQL 技能的人都可以直接快速分析大规模数据集。要了解更多信息，请参阅[亚马逊 Athena](#)。

常见问题：AMS 中的 Athena

问：如何使用我的 AMS 账户申请访问亚马逊 Athena？

使用管理 AWS | 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Athena。此 RFC 为您的账户配置以下 IAM 角色:customer_athena_console_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Athena 有哪些限制？

没有任何限制。您的 AMS 账户中提供亚马逊 Athena 的全部功能。

问：在我的 AMS 账户中使用 Amazon Athena 的先决条件或依赖条件是什么？

Athena 主要依赖 AWS Glue 该服务，因为它使用使用创建的数据。catalog/metastore AWS Glue 因此，AWS Glue 权限包含在成功的 Athena RFC 中。

该角色customer_athena_console_role具有 Amazon S3 存储桶的先决条件。要创建新的存储桶，请使用自动化 CTct-1a68ck03fn98r (部署 | 高级堆栈组件 | S3 存储 | 创建)。当您使用此自动 CT 为 Athena 创建 S3 存储桶时，存储桶名称必须以前缀开头。athena-query-results-*

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Bedrock

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Bedrock 功能。Amazon Bedrock 是一项完全托管的服务，可制作来自领先的 AI 初创公司的高性能基础模型 (FMs)，并通过统一的 API AWS 供您使用。您可以从各种根基模型中选择，找到最适合您的用例的模型。Amazon Bedrock 还提供了一系列广泛的功能，可以构建生成式人工智能应用程序，为您提供安全可靠的专属人工智能服务。利用 Amazon Bedrock，您可以轻松试验和评估用例的常用根基模型，使用微调和检索增强生成 (RAG) 等技术，通过自己的数据进行量身定制，并构建使用企业系统和数据来源执行任务的代理。

借助 Amazon Bedrock 的无服务器体验，您可以快速入门，使用自己的数据私下自定义基础模型，并使用 AWS 工具轻松安全地将其集成和部署到您的应用程序中，而无需管理任何基础设施。有关更多信息，请参阅 [Amazon Bedrock](#)。

常见问题：AMS 中的 Amazon Bedrock

问：如何使用我的 AMS 账户申请访问 Amazon Bedrock？

要申请访问亚马逊 Bedrock，请使用管理 | AWS 服务 | 自行配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 提交一个 RFC 更改类型。此 RFC 为您的账户配置以下 IAM 角色:customer_bedrock_console_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Bedrock 有哪些限制？

- 默认情况下，作为 SSP 角色的一部分，不支持 Amazon Bedrock 知识库，因为它依赖亚马逊无服务器 OpenSearch 服务，AMS 目前不支持该服务。
- 由于依赖亚马逊等不受支持的服务，因此不支持 Bedrock Studio。DataZone

问：在我的 AMS 账户中使用 Amazon Bedrock 有哪些先决条件或依赖关系？

- 需要 AWS Marketplace 权限的第三方模型订阅必须由默认角色完成 (AWSManagedServicesAdminRole 在 MALZ 和 SALZ Customer_ReadOnly_Role 上)。这是因为默认角色包括 AWS Marketplace 权限。
- 如果使用数据加密，则在请求创建控制台角色时必须提供 AWS KMS 密钥 ARN。此外，正在使用的 Amazon S3 存储桶的名称中必须有“基石”。

使用 AMS SSP CloudSearch 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 CloudSearch 功能。Amazon CloudSearch 是一项 AWS 云端托管服务，您可以经济高效地使用它来设置、管理和扩展您的网站或应用程序的搜索解决方案。Amazon CloudSearch 支持 34 种语言和热门搜索功能，例如突出显示、自动完成和地理空间搜索。要了解更多信息，请参阅 [Amazon CloudSearch](#)。

Note

AWS 自 2024 年 7 月 25 日起 CloudSearch，已关闭新买家访问亚马逊的权限。Amazon CloudSearch 现有客户可以继续照常使用该服务。AWS 继续投资于 Amazon 的安全性、可用性和性能改进 CloudSearch，但我们不打算推出新功能。

要了解亚马逊 CloudSearch 和亚马逊 OpenSearch 服务之间的区别，以及如何过渡到 OpenSearch 服务，请联系您的云架构师 (CA) 寻求指导。有关过渡到 OpenSearch 服务的更多信息，请参阅[从亚马逊过渡 CloudSearch 到亚马逊 OpenSearch 服务服务](#)。

AWS Managed Services CloudSearch 中的亚马逊常见问题解答

问：如何使用我的 AMS 账户申请访问亚马逊 CloudSearch ？

使用管理 | AWS 服务 | 自行配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问亚马逊 CloudSearch。此 RFC 为您的账户配置以下 IAM 角

色：customer_csearch_admin_role和。customer_csearch_dev_role在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：CloudSearch 在我的 AMS 账户中使用亚马逊有哪些限制？

您的 AMS 账户中提供 CloudSearch 了 Amazon 的全部功能。Amazon 目前支持所有 AMS 支持的数据库解决方案。CloudSearch 请注意，当前，DynamoDB 是唯一无法建立索引的 AWS 托管数据库解决方案。

问：在我的 AMS 账户 CloudSearch 中使用 Amazon 的先决条件或依赖条件是什么？

Amazon CloudSearch 依靠 Amazon S3 与身份提供商合作来自动分析输入数据并确定表字段。此 RFC 不提供对 Amazon S3 的访问权限，因此必须在服务请求中单独申请。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon CloudWatch Synthetics

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon CloudWatch Synthetics 功能。你可以使用 Amazon S CloudWatch ynthetic 创建“加那利群岛”来监控你的终端节点，然后。APIs

Canarie 是用 Node.js 或 Python 编写的可配置脚本，按计划运行。它们以 Node.js 或 Python 为框架在您的账户中创建 Lambda 函数。金丝雀通过 HTTP 和 HTTPS 两种协议工作。Canaries 会检查您的终端节点的可用性和延迟，并可以存储加载时间数据和 UI 屏幕截图。他们监控您的 REST APIs 和网站内容，并可以检查网络钓鱼、代码注入和跨站脚本是否存在未经授权的更改。URLs

加那利群岛遵循与客户相同的路线和执行相同的操作，因此即使您的应用程序上没有任何客户流量，您也可以持续验证客户体验。使用金丝雀，您可以早于客户先行发现问题。要了解更多信息，请参阅 [Amazon CloudWatch：使用综合监控](#)。

AWS Manage CloudWatch d Services 中的亚马逊 Synthetics 常见问题解答

问：如何使用我的 AMS 账户申请访问亚马逊 S CloudWatch ynthetic ？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66 CloudWatch n899dct) 更改类型提交 RFC，请求访问 Amazon Synthetics。此 RFC 为您的账户配置以下 IAM 角色：“customer_cw_synthetic_console_role”和“customer_cw_synthetic_canary_lambda_role”。在您的账户中配置后，您必须在联合解决方案中加入“customer_cw_synthetic_console_role”角色。

问：在我的 AMS 账户中使用 Amazon S CloudWatch ynthetic 有哪些限制？

在您的 AMS 账户中使用 Amazon S CloudWatch ynthetic 没有任何限制。禁止在 AMS 提供的服务角色“customer_cw_synthetic_canary_lambda_role”之外为加那利群岛创建角色。

问：在我的 AMS 账户中使用 Amazon S CloudWatch ynthetic 有哪些先决条件或依赖条件？

加那利群岛创建并使用默认的 Amazon Synth CloudWatch etics S3 存储桶：cw-syn-results“--”
`${accountnumber} ${default-region}`

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Cognito 用户池

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Cognito 用户池功能。Amazon Cognito 用户池提供了一个安全的用户目录，可扩展到数亿用户。作为一项完全托管的服务，Amazon Cognito 用户池的设置无需担心服务器基础设施的架设问题。此服务使您能够管理最终用户池，您可以使用这些用户与内部应用程序集成。此服务为您提供了自定义数据库或网络或移动应用程序最终用户目录的替代方案。同时，Amazon Cognito 用户池提供了目录服务的全套功能，例如密码策略、多因素身份验证、密码恢复和自助注册服务。它还允许该应用程序联合访问其他流行的公共服务，例如 OpenID、Facebook、Amazon 或 Google。

亚马逊 Cognito 分为两个主要产品。亚马逊 Cognito 用户池和亚马逊 Cognito 身份提供商。本节重点介绍 Amazon Cognito 用户池，这些用户池提供对亚马逊 S3 或 DynamoDB 等其他 AWS 服务的访问权限。该服务允许您使用 Amazon Cognito 用户池或第三方身份提供商来提供对服务的访问权限。AWS 它还通过匿名访客访问提供对 AWS 服务的访问。由于 Amazon Cognito 用户池的强大特性，它将 case-by-case 作为操作手动服务进行手动管理，以避免账户受到潜在的安全漏洞。要了解更多信息，请参阅 [Amazon Cognito 用户池](#)。

AWS Managed Services 常见问题解答中的 Amazon Cognito 用户池

常见问题和答案：

问：如何申请访问我的 AMS 账户中的 Amazon Cognito 用户池？

在 AMS 中实施 Amazon Cognito 用户池分为两个步骤：

1. 提交管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型并请求在您的 AMS 账户中创建 Amazon Cognito 用户池。包括以下信息：
 - AWS 区域。
 - Cognito 用户池的名称。
 - 如果您想使用亚马逊简单电子邮件服务 (Amazon SES) 来发送消息和通知，而不是默认的内部 Cognito 邮件服务，则客户应在账户中提供一个已经过验证的 Amazon SES 服务电子邮件地址。此地址将用于邮件的“发件人”和“回复至”字段。它们还必须注明激活亚马逊 SES 的地区 (us-east-1、eu-west-1 或 us-west-2) 。
 - 如果您想使用短信进行一次性密码和验证，则客户应注明。

2. 通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来请求用户访问权限。

此 RFC 为您的账户配置以下 IAM 角色：

色：`customer_cognito_admin_role`和。`customer_cognito_importjob_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。这些角色允许您管理 Amazon Cognito 用户池、管理池中的用户和群组、为用户创建导入任务、修改通知和订阅消息、将应用程序关联到用户池、自行管理向池中添加联合服务以及删除已创建的池。

问：在我的 AMS 账户中使用 Amazon Cognito 用户池有哪些限制？

您将无法创建 Amazon Cognito 用户池。该操作需要创建 IAM 角色才能利用亚马逊 Cognito 使用的服务，例如亚马逊 SES 和亚马逊简单通知服务 (Amazon SNS) Service。

问：在我的 AMS 账户中使用 Amazon Cognito 用户池有哪些先决条件或依赖关系？

如果您想使用 Amazon SES 通过电子邮件向您的用户池发送消息和通知，他们应该已经在账户中激活 Amazon SES 服务，并且已经验证了应在已发送电子邮件的“发件人”和“回复”字段中使用的电子邮件地址。有关使用 Amazon SES 验证电子邮件地址的更多信息，请参阅在 Amazon S [ES 中验证电子邮件地址](#)。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Comprehend

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Comprehend 功能。Amazon Comprehend 是一项自然语言处理 (NLP) 服务，它使用机器学习在文本中查找见解和关系，无需任何机器学习经验。Amazon Comprehend 使用机器学习来帮助您发现非结构化数据中的见解和关系。该服务识别文本的语言；提取关键短语、地点、人物、品牌或事件；了解文本的正面或负面程度；使用分词和部分语音分析文本；并按主题自动整理文本文件集。您还可以使用 Amazon Comprehend 中的 AutoML 功能来构建一组专为您的组织需求量身定制的自定义实体或文本分类模型。要了解更多信息，请参阅[亚马逊 Comprehend](#)。

AWS Managed Services 常见问题解答中的亚马逊 Comprehend

问：如何使用我的 AMS 账户申请访问亚马逊 Comprehend？

可以通过提交两个 AMS 服务来申请 Amazon Comprehend 控制台和数据访问角色：RFCs

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：`customer_comprehend_console_role`。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Comprehend 有哪些限制？

通过 Amazon Comprehend 控制台创建新的 IAM 角色功能受到限制。否则，Amazon Comprehend 的全部功能都可以在你的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Comprehend 有哪些先决条件或依赖关系？

如果亚马逊 S3 存储桶使用密钥加密，则必须使用 Amazon S3 和 AWS Key Management Service (AWS KMS) 才能使用 Amazon Comprehend。AWS KMS

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Connect

Note

经过深思熟虑，我们决定从 2026 年 5 月 20 日起终止对 Amazon Connect 语音识别的支持。从 2025 年 5 月 20 日起，Amazon Connect 语音识别将不再接受新客户。作为在 2025 年 5 月 20 日之前注册该服务的账户的现有客户，您可以继续使用 Amazon Connect 语音识别功能。2026 年 5 月 20 日之后，您将无法再使用 Amazon Connect 语音识别码。

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Connect 功能。Amazon Connect 是一个全渠道云联络中心，可帮助公司以更低的成本提供卓越的客户服务。Amazon Connect 为客户和代理提供无缝的语音和聊天体验。这包括一套基于技能的路由工具、强大的实时和历史分析以及 easy-to-use 直观的管理工具，所有这些都包含 pay-as-you-go 定价。

您可以在 AMS 多账户 landing zone 或单账户着陆区账户中创建虚拟联络中心实例的一个或多个实例。您可以使用现有的 SAML 2.0 身份提供商进行代理访问或使用 Amazon Connect 原生支持进行用户生命周期管理。

此外，您可以从 Amazon Connect 控制台申请每个 Amazon Connect 实例的收费 free/direct 拨电话号码。您可以使用 easy-to-use 图形用户界面创建丰富的联系流程，以实现所需的客户体验和路由。联系流可以利用 AWS Lambda 函数与本地数据存储和 API 集成。你也可以使用 Kinesis Streams 和 Firehose 启用数据流。

通话记录、聊天记录和报告存储在使用 AWS KMS 密钥加密的 Amazon S3 存储桶中。可以将联络流日志保存到 CloudWatch 日志组中。

要了解更多信息，请参阅 [Amazon Connect](#)。

AWS Managed Services 常见问题中的 Amazon Connect

问：如何使用我的 AMS 账户申请访问 Amazon Connect？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角

色：customer_connect_console_role和。customer_connect_user_role在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Connect 有哪些限制？

没有任何限制。您的 AMS 账户中提供了 Amazon Connect 的全部功能。

问：在我的 AMS 账户中使用 Amazon Connect 有哪些先决条件或依赖条件？

- 您必须使用标准 AMS 创建 AWS KMS 密钥和 Amazon S3 存储桶 RFCs；Amazon S3 存储桶是存储通话录音和聊天记录所必需的。
- 如果您想与 Active Directory (AD) 集成，则需要 AD 连接器才能在 AMS 托管的 Amazon Connect 实例和您的本地目录服务之间进行集成。可以通过请求“管理 | 其他 | 其他”RFC 在您的账户中配置 AD Connector。
- 您可以根据您的联系流要求启用以下可选的自行配置服务。
 - AWS Lambda: 您可以使用 Lambda 函数扩展联系流程，以利用现有的本地数据存储或。APIs您可以使用 Lambda 自行配置的服务来创建 Lambda 函数。
 - Amazon Kinesis Data Streams：您可以创建数据流以实现向外部应用程序传输数据。您可以流式传输联系人追踪记录或座席事件。
 - Amazon Kinesis Data Firehose：您可以创建 Data Firehose，将大量联系人追踪记录流式传输到外部应用程序。
 - Amazon Lex：您可以利用 Amazon Lex 聊天机器人创建智能联系流程，利用亚马逊 Alexa 服务，实现丰富的客户体验和自动化。
- 问：如何请求添加拨出或呼入电话的国家/地区列表？

要添加拨出或呼入电话的国家/地区列表，请向 AMS 提交服务请求。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Data Firehose

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Data Firehose 功能。Firehose 是将流数据可靠地加载到数据湖、数据存储和分析工具的最简单方法。它可以捕获、转换流数据并将其加载到 Amazon S3、Amazon Redshift、Amazon S OpenSearch ervice 和 [Splunk](#) 中，从而使用你目前正在使用的现有商业智能工具和仪表板实现近乎实时的分析。它是一项完全托管的服务，可自动扩展以匹配您的数据吞吐量，并且无需持续管理。它还可以在加载数据之前对其进行批

处理、压缩、转换和加密，从而最大限度地减少目的地使用的存储量并提高安全性。要了解更多信息，请参阅[什么是亚马逊数据 Firehose](#)？

AWS Managed Services 常见问题解答中的 Firehose

常见问题和答案：

问：如何通过我的 AMS 账户申请访问亚马逊数据 Firehose ？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_kinesis_firehose_user_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Firehose 有什么限制？

没有任何限制。Amazon Data Firehose 的全部功能可在您的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Firehose 的先决条件或依赖条件是什么？

必须为每个交付流请求新的服务相关的 IAM 角色。您还可以使用所需的资源权限 (包括 S3 存储桶/KMS 密钥/Lambda Functions/Kinesis 流) 更新角色策略，从而为所有直播重复使用单个服务相关角色。

在您提交 RFC 以添加 Firehose 后，AMS 运营工程师将通过服务请求与您联系，请求您想要与 Data Firehose 连接的资源 (例如 S3 AWS KMS、Lambda 和 Kinesis Streams) 。 ARNs

使用 AMS SSP 在你的 AMS 账户中配置 Amazon DevOps Guru

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon DevOps Guru 功能。Amazon DevOps Guru 是一项完全托管的运营服务，可让开发人员和操作员轻松提高其应用程序的性能和可用性。DevOpsGuru 可以让你卸下与识别操作问题相关的管理任务，这样你就可以快速实施改进应用程序的建议。DevOpsGuru 创建了反应式见解，您可以立即使用这些见解来改进您的应用程序。它还可以提供主动见解，帮助您避免将来可能影响应用程序的操作问题。DevOpsGuru 应用机器学习来分析您的运营数据以及应用程序指标和事件，以识别偏离正常操作模式的行为。当 DevOps Guru 检测到操作问题或风险时，您会收到通知。对于每个问题，DevOpsGuru 都会提出明智的建议，以解决当前和预测的未来运营问题。

要了解更多信息，请参阅[什么是 Amazon DevOps Guru](#)。

AWS Managed Services 常见问题解答中的 Amazon DevOps Guru

问：如何使用我的 AMS 账户申请访问 Amazon DevOps Guru ？

要申请访问权限，请提交管理 | AWS 服务 | 自配服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型。此 RFC 为您的账户配置以下 IAM 角色:customer_devopsguru_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon DevOps Guru 有哪些限制？

没有任何限制。Amazon DevOps Guru 的全部功能可在您的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon DevOps Guru 的先决条件或依赖条件是什么？

没有先决条件。DevOpsGuru 利用以下 AWS 服务：Amazon Log CloudWatch s、RDS Insights、AWS X-Ray AWS Lambda、和。AWS CloudTrail

使用 AMS SSP 在你的 AMS 账户中配置亚马逊 DocumentDB (兼容 MongoDB)

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 DocumentDB (兼容 MongoDB) 功能。Amazon DocumentDB (兼容 MongoDB) 是一种快速、可扩展、高度可用且完全托管的文档数据库服务，支持 MongoDB 工作负载。Amazon DocumentDB 为您提供大规模操作任务关键型 MongoDB 工作负载时所需的性能、可扩展性和可用性。Amazon DocumentDB 通过模拟 MongoDB 客户端期望从 MongoDB 服务器获得的响应来实现 Apache 2.0 开源 MongoDB 3.6 API，允许您在亚马逊 DocumentDB 上使用现有的 MongoDB 驱动程序和工具。在 Amazon DocumentDB 中，存储和计算是分离的，允许两者独立扩展，无论您的数据大小如何，您都可以通过添加多达 15 个低延迟只读副本将读取容量增加到每秒数百万个请求。Amazon DocumentDB 专为 99.99% 的可用性而设计，可在三个 AWS 可用区复制六份数据副本 ()。AZs您可以免费使用 AWS Database Migration Service (DMS) (六个月) 将本地或亚马逊弹性计算云 (Amazon) MongoDB 数据库迁移到亚马逊 EC2 DocumentDB，几乎无需停机。要了解更多信息，请参阅[亚马逊文档数据库 \(兼容 MongoDB \)](#)。

AWS Managed Services 常见问题解答中的亚马逊 DocumentDB

问：如何使用我的 AMS 账户申请访问亚马逊文档数据库？

可以通过提交两个 AMS RFCs (控制台访问权限和数据访问权限) 来请求 Amazon DocumentDB 控制台和数据访问角色：

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问亚马逊文档数据库。此 RFC 为您的账户配置以下 IAM 角色:customer_documentdb_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 DocumentDB 有哪些限制？

亚马逊 DocumentDB 需要亚马逊 RDS 特定的权限。由于 AMS 完全管理亚马逊 RDS，因此 Amazon DocumentDB 的 IAM 角色包括对亚马逊 RDS 操作的一些限制。以下限制适用：

- 对 DeleteDBInstance 和的访问 DeleteDBCluster APIs 已受到限制。要使用这些删除功能 APIs，请提交 RFC，其中包含管理 | 高级堆栈组件 | 身份和访问管理 (IAM) | 更新实体或策略 (需要审查) 更改类型 (ct-27tuth19k52b4)。
- 您无法在 Amazon RDS 实例中添加或删除标签。
- 您无法将您的亚马逊文档数据库实例设为公有。

问：在我的 AMS 账户中使用亚马逊 DocumentDB 有哪些先决条件或依赖关系？

如果亚马逊 S3 存储桶使用密钥加密，AWS KMS 则必须使用 Amazon S3 和，才能使用亚马逊 DocumentDB。AWS KMS

使用 AMS SSP 在你的 AMS 账户中配置亚马逊 DynamoDB

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 DynamoDB (DynamoDB) 功能。Amazon DynamoDB 是一个关键值和文档数据库，可在任何规模上提供个位数的毫秒级性能。它是一个完全托管的多区域、多活动数据库，具有内置安全性、备份和恢复功能，以及适用于互联网规模应用程序的内存缓存。要了解更多信息，请参阅[Amazon DynamoDB](#)。

Amazon DynamoDB Accelerator (DAX) 是一项直写缓存服务，旨在简化将缓存添加到 DynamoDB 表的过程。DAX 适用于需要高性能读取的应用程序。

AWS Managed Services 中的 DynamoDB 常见问题解答

问：如何使用我的 AMS 账户请求访问 DynamoDB 和 DAX？

使用管理 AWS | 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 DynamoDB 和 DAX。此 RFC 为您的账户配置以下 IAM 角色和策略：

- DynamoDB 角色名称：customer_dynamodb_role
DAX 服务角色名称：customer_dax_service_role
- DynamoDB 策略名称：customer_dynamodb_policy
DAX 服务政策：customer_dax_service_policy

在您的账户中配置后，您必须在联合解决方案 customer_dynamodb_role 中加载。

问：在我的 AMS 账户中使用 DynamoDB 有哪些限制？

支持所有 DynamoDB 功能，包括 DynamoDB 加速器 (DAX)。

为任何给定表创建警报时，警报名称必须以“customer*”为前缀；例如，。customer-employee-table-high-put-latency

为 DynamoDB 创建 Amazon SNS 主题时，必须将其命名为：。dynamodb

要删除 DynamoDB 创建的 Amazon SNS 主题，请提交“管理 | 其他 | 其他 | 其他 | 更新更改类型 RFC”。

问：在我的 AMS 账户中使用 DynamoDB 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 DynamoDB 没有任何先决条件或依赖关系。

使用 AMS SSP 在您的 AMS 账户中配置 Amazon 弹性容器注册表

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊弹性容器注册表 (Amazon ECR) Container Registry 功能。Amazon Elastic Container Registry 是一个完全托管的 [Docker](#) 容器注册表，可让开发人员轻松存储、管理和部署 Docker 容器镜像。Amazon ECR 已与[亚马逊弹性容器服务 \(Amazon ECS\) Service](#) 集成，简化了从开发到生产的工作流程。Amazon ECR 让您无需操作自己的容器存储库，也不必担心底层基础设施的扩展。Amazon ECS 将您的映像托管在高度可用且可扩展的架构中，使您能够可靠地为应用程序部署容器。与 AWS Identity and Access Management (IAM) 集成提供了对每个存储库的资源级控制。使用 Amazon ECR，无需支付任何预付费用或承诺。您只需为存储在存储库中的数据量和传输到 Internet 的数据量付费。

要了解更多信息，请参阅 [Amazon 弹性容器注册表](#)。

AWS Managed Services 中的亚马逊弹性容器注册表常见问题解答

问：如何申请访问我的 AMS 账户中的 Amazon ECR？

使用管理 | AWS 服务 | 自行配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问亚马逊 ECR。此 RFC 将以下 IAM 角色分别配置到您的账户：customer_ecr_console_role、以及customer_ecr_poweruser_instance_profile关联的 IAM 策略customer_ecr_console_policy和customer_ecr_poweruser_instance_profile_policy。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon ECR 有哪些限制？

在您的 AMS 账户中使用 Amazon ECR 时，AMS 命名空间存在限制。容器镜像不得以“AMS-”或“Sentinel-”为前缀。

问：在我的 AMS 账户中使用 Amazon ECR 有哪些先决条件或依赖条件？

在您的 AMS 账户中使用 Amazon ECR 没有任何先决条件或依赖关系。

使用 AMS SSP 在你的 AMS 账户中配置 EC2 Image Builder

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 EC2 Image Builder 功能。EC2 Image Builder 是一项完全托管的 AWS 服务，它可以更轻松地自动创建、管理和部署自定义、安全和 up-to-date “黄金” 服务器映像，这些映像已预先安装并预先配置了软件和设置，以满足特定 IT 标准。

您可以使用 AWS 管理控制台、AWS CLI 或 APIs 在您的 AWS 账户中创建自定义映像。当您使用时 AWS 管理控制台，Amazon EC2 Image Builder 向导会指导您完成以下步骤：

- 提供起始构件
- 添加和删除软件
- 自定义设置和脚本
- 运行选定的测试
- 将图像分发到 AWS 区域

您构建的映像是在您的账户中创建的，可以持续配置操作系统补丁。要了解更多信息，请参阅 [EC2 Image Builder](#)。

EC2 AWS Managed Services 常见问题中的 Image Builder

常见问题和答案：

问：如何使用我的 AMS 账户申请访问 EC2 Image Builder？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更

改类型来申请访问权限。通过此 RFC，将在您的账户中配置以下 IAM 角色：

customer_ec2_imagebuilder_role在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：EC2 Image Builder 有哪些限制？

AMS 不支持使用服务默认值进行基础设施配置。您可以创建新的基础架构配置或使用现有基础架构配置。

AMS 目前不支持创建容器配方。

问：启用 Image Builder 的先决条件或依赖关系是什么？

- EC2 Image Builder 服务相关角色：您无需手动创建服务相关角色。当您在 AWS 管理控制台、CLI 或 AWS AP AWS I 中创建第一个 Image Builder 资源时，Image Builder 会为您创建服务相关角色。
- 用于使用 Image Builder 构建映像和运行测试的实例必须有权访问 Systems Manager 服务。如果 SSM 代理尚不存在，将在源镜像上安装该代理，并在创建镜像之前将其删除。
- AWS IAM：您与实例配置文件关联的 IAM 角色必须有权运行映像中包含的构建和测试组件。必须将以下 IAM 角色策略附加到与实例配置文件关联的 IAM 角色：EC2InstanceProfileForImageBuilder和AmazonSSMManagedInstanceCore。IAM 角色名称应包含*imagebuilder*关键字。
- 如果配置日志记录，在基础设施配置中指定的实例配置文件必须具有目标存储桶 (arn:aws:s3:::{bucket-name}/*) 的 s3:PutObject 权限。例如：

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::{bucket-name}/*"
    }
  ]
}
```

- 创建名为 “imagebuilder” 的 SNS 主题，以接收来自 Image Build EC2 er 的任何提醒和通知。

使用 AMS SSP 在你的 AMS 账户 AWS Fargate 中配置 Amazon ECS

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中通过 AWS Fargate 功能访问 Amazon ECS。AWS Fargate 是一种可以与 Amazon ECS 配合使用的技术，无需管理服务器或亚马

迹 EC2 实例集群即可运行[容器 \(参见上面的容器 AWS \)](#)。使用 AWS Fargate，您无需再预置、配置或扩展虚拟机集群来运行容器。这样一来，您就无需再选择服务器类型、确定扩展集群的时间和优化集群打包。

要了解更多信息，请参阅上的 [Amazon ECS AWS Fargate](#)。

AWS Managed Services 常见问题解答中的 Fargate 上的 Amazon ECS

问：如何使用我的 AMS 账户请求访问 Fargate 上的 Amazon ECS？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Fargate 上的 Amazon ECS。此 RFC 将以下 IAM 角色配置到您的账

户：customer_ecs_fargate_console_role (如果没有提供 ECS 策略与 ECS 策略关联的现有 IAM 角

色) customer_ecs_fargate_events_service_role、customer_ecs_task_execution_service_role 和 AWSServiceRoleForApplicationAutoScaling_ECSService。在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问：使用我的 AMS 账户在 Fargate 上使用 Amazon ECS 有哪些限制？

- Amazon ECS 任务监控和日志记录被视为您的责任，因为容器级别的活动发生在虚拟机管理程序之上，并且日志记录功能受到 Fargate 上的 Amazon ECS 的限制。作为 Fargate 上的 Amazon ECS 用户，我们建议您采取必要步骤启用对您的 Amazon ECS 任务的登录功能。有关更多信息，请参阅[为容器启用 awslogs 日志驱动程序](#)。
- 容器级别的安全和恶意软件保护也被视为您的责任。Fargate 上的 Amazon ECS 不包括趋势科技或预先配置的网络安全组件。
- 此服务适用于多账号着陆区和单账号着陆区 AMS 账户。
- 由于创建 Route 53 私有托管区域需要更高的权限，因此默认情况下，自行配置角色限制了 Amazon ECS [服务发现](#)。要在服务上启用服务发现，请提交“管理”|“其他”|“其他”|“更新”更改类型。要提供为您的 Amazon ECS 服务启用服务发现所需的信息，请参阅[服务发现手册](#)。
- AMS 目前不管理或限制用于在 Amazon ECS Fargate 上部署到容器的映像。您将能够部署来自 Amazon ECR、Docker Hub 或任何其他私有镜像存储库的镜像。因此，我们建议不要部署公共镜像或任何不安全的镜像，因为它们可能会导致账户出现恶意活动。

问：在我的 AMS 账户中在 Fargate 上使用 Amazon ECS 有哪些先决条件或依赖关系？

- 以下是 Amazon ECS 对 Fargate 的依赖关系；但是，使用您的自配置角色启用这些服务无需执行任何其他操作：

- CloudWatch 日志
 - CloudWatch 事件
 - CloudWatch 警报
 - CodeDeploy
 - App Mesh
 - Cloud Map
 - Route 53
- 根据您的使用案例，以下是 Amazon ECS 所依赖的资源，并且在您的账户中使用 Fargate 上的 Amazon ECS 之前可能需要的资源：
- 要与 Amazon ECS 服务配合使用的安全组。您可以使用部署 | 高级堆栈组件 | 安全组 | 创建 (auto) (ct-3pc215bnwb6p7)，或者，如果您的安全组需要特殊规则，请使用部署 | 高级堆栈组件 | 安全组 | 创建 (需要审阅) (ct-1oxx2g2g2d7hc90)。注意：您在 Amazon ECS 上选择的安全组必须专门为 Amazon ECS 服务或集群所在的 Amazon ECS 创建。您可以在“使用 [Amazon ECS 进行设置](#)”和“[亚马逊弹性容器服务中的安全](#)”的“安全组”部分了解更多信息。
 - 应用程序负载均衡器 (ALB)、网络负载均衡器 (NLB)、用于任务间负载平衡的经典负载均衡器 (ELB)。
 - 的目标群体 ALBs.
 - 用于与 Amazon ECS 集群集成的应用程序网格资源（例如虚拟路由器、虚拟服务、虚拟节点）。
- 目前，在标准 AMS 变更类型之外创建时，AMS 无法自动降低与支持安全组权限相关的风险。我们建议您申请一个用于您的 Fargate 集群的特定安全组，以限制使用未指定用于 Amazon ECS 的安全组的可能性。

使用 AMS SSP 在你的 AMS 账户 AWS Fargate 中配置 Amazon EKS

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中通过 AWS Fargate 功能访问 Amazon EKS。AWS Fargate 是一种按需为容器提供大小合适的计算容量的技术（要了解容器，请参阅[什么是容器？](#)）。使用 AWS Fargate，您无需再预置、配置或扩展虚拟机组来运行容器。这样一来，您就无需再选择服务器类型、确定扩展节点组的时间和优化集群打包。

亚马逊 Elastic Kubernetes Service（亚马逊 EKS）使用使用 AWS Fargate Kubernetes 提供的上游可扩展模型 AWS 构建的控制器将 Kubernetes 与 Kubernetes 集成。这些控制器作为 Amazon EKS 管理的 Kubernetes 控制平面的一部分运行，负责将原生 Kubernetes pod 调度到 Fargate 上。除了若干转换和验证准入控制器外，Fargate 控制器还包括一个与默认 Kubernetes 调度器一起运行的新调度器。

当您启动满足 Fargate 上的运行条件的 Pod 时，集群中运行的 Fargate 控制器会识别、更新 Pod 并将其安排到 Fargate 上。

要了解更多信息，请参阅[AWS Fargate 现已正式上市的 Amazon EKS](#) 和 [Amazon EKS 安全最佳实践指南](#)（包括“建议”，例如“查看并撤消不必要的匿名访问权限”等）。

 Tip

AMS 有一个变更类型，即部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建 OpenID Connect 提供商 (ct-30ecvfi3tq4k3)，您可以将其与亚马逊 EKS 一起使用。有关示例，请参阅[身份和访问管理 \(IAM\) Management | 创建 OpenID Connect 提供商](#)。

AWS Managed Services 常见问题解答 AWS Fargate 中的亚马逊 EKS

问：如何使用我的 AMS 账户申请访问 Fargate 上的 Amazon EKS？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色。

- customer_eks_fargate_console_role.

在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

- 这些服务角色允许 Fargate 上的 Amazon EKS 代表您拨打其他 AWS 服务：

- customer_eks_pod_execution_role
- customer_eks_cluster_service_role

问：在我的 AMS 账户中在 Fargate 上使用 Amazon EKS 有哪些限制？

- AMS 不支持创建[托管或自行管理](#)的 EC2 节点组。如果您需要使用 EC2 工作节点，请联系您的 AMS 云服务交付经理 (CSDM) 或云架构师 (CA)。
- AMS 不包括趋势科技或容器映像的预配置网络安全组件。您需要管理自己的图像扫描服务，以便在部署之前检测恶意容器镜像。
- 由于相互依存关系，不支持 EKSCTL。CloudFormation
- 在创建集群期间，您有权禁用集群控制平面日志记录。有关更多信息，请参阅[Amazon EKS 控制面板日志记录](#)。我们建议您在创建集群时启用所有重要的 API、身份验证和审核日志。

- 在创建集群期间，Amazon EKS 集群的集群终端节点访问权限默认为公用；有关更多信息，请参阅 [Amazon EKS 集群终端节点访问控制](#)。我们建议将 Amazon EKS 终端节点设置为私有终端节点。如果需要终端节点才能进行公共访问，则最佳做法是仅针对特定 CIDR 范围将其设置为公用。
- AMS 没有办法强制和限制用于部署到 Amazon EKS Fargate 上的容器中的映像。您可以部署来自 Amazon ECR、Docker Hub 或任何其他私有镜像存储库的镜像。因此，部署可能对账户执行恶意活动的公共镜像存在风险。
- AMS 不支持通过云开发套件 (CDK) 或 CloudFormation Ingest 部署 EKS 集群。
- 您必须使用 [ct-3pc215bnwb6p7 部署 | 高级堆栈组件 | 安全组 | 在清单文件中创建和引用创建入口所需的安全组](#)。这是因为该角色customer-eks-alb-ingress-controller-role无权创建安全组。

问：在我的 AMS 账户中在 Fargate 上使用 Amazon EKS 有哪些先决条件或依赖关系？

要使用该服务，必须配置以下依赖关系：

- 要针对服务进行身份验证，aws-iam-authenticator必须同时安装 KUBECTL 和；有关更多信息，请参阅[管理集群身份验证](#)。
- Kubernetes 依赖一个叫做“服务账户”的概念。为了在 EKS 上使用 kubernetes 集群内部的服务账户功能，需要使用管理 | 其他 | 其他 | 更新 RFC，其中包含以下输入：
 - [必填] 亚马逊 EKS 集群名称
 - [必需] 将部署服务账户 (SA) 的 Amazon EKS 集群命名空间。
 - [必填] Amazon EKS 集群 SA 名称。
 - [必填] IAM 策略名称和 permissions/document 待关联。
 - [必需] 正在请求 IAM 角色名称。
 - [可选] OpenID Connect 提供商网址。有关更多信息，请参阅
 - [在集群上为服务账户启用 IAM 角色](#)
 - [为服务账号引入精细的 IAM 角色](#)
- 我们建议配置和监控 Config 规则
 - 公共集群终端节点
 - 已禁用 API 日志记录

您有责任监控和修正这些 Config 规则。

如果您想部署 [ALB 入口控制器](#)，请提交“[管理 | 其他 | 其他更新 RFC](#)”，以配置与 ALB Ingress Controller Pod 一起使用的必要的 IAM 角色。创建与 ALB Ingress Controller 关联的 IAM 资源需要以下输入（包括您的 RFC 中的这些内容）：

- [必填] 亚马逊 EKS 集群名称
- [可选] OpenID Connect 提供商网址
- [可选] 将部署应用程序负载均衡器 (ALB) 入口控制器服务的 Amazon EKS 集群命名空间。[默认：kube-system]
- [可选] Amazon EKS 集群服务账户 (SA) 名称。[默认：aws-load-balancer-controller]

如果要在集群中启用信封密钥加密（我们建议这样做），请在 RFC 的描述字段中提供 IDs 您打算使用的 KMS 密钥以添加服务（[管理 | 服务 | 自配置 AWS 服务 | 添加](#) (ct-1w8z66n899dct)。要了解有关信封加密的更多信息，请参阅 [Amazon EKS 使用 AWS KMS 为机密添加信封加密](#)。

使用 AMS SSP 在您的 AMS 账户中配置亚马逊 EMR

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon EMR 功能。亚马逊 EMR 是业界领先的云大数据平台，用于使用 Apache Spark、Apache Hive、Apache Flink、Apache Hudi 和 P HBase resto 等开源工具处理大量数据。借助 Amazon EMR，您可以以不到传统本地解决方案一半的成本运行 PB 级分析，速度比标准 Apache Spark 快 3 倍以上。对于短期运行的作业，您可以启动和关闭集群，并为使用的实例按秒付费。对于长时间运行的工作负载，您可以创建高度可用的集群，这些集群可以自动扩展以满足需求。

您可以在 AMS 多账户着陆区账户或单账户着陆区账户中创建一个或多个 Amazon EMR 集群实例，以支持临时和永久性 Amazon EMR 集群。您也可以启用 Kerberos 身份验证以启用对本地 Active Directory 域中的用户进行身份验证。

您可以在 Amazon EMR 集群中利用多个数据存储来支持特定于用例的 Hadoop 工具和库。可以使用 OnDemand 或竞价型实例创建 Amazon EMR 集群，并配置自动扩展以管理容量并降低成本。

可以将集群日志文件存档到 Amazon S3 存储桶中以进行日志记录和调试。您还可以访问托管在 Amazon EMR 集群中的网页界面，以支持 hadoop 管理要求或为客户提供笔记本体验。

要了解更多信息，请参阅 [Amazon EMR](#)。

AWS Managed Services 常见问题解答中的亚马逊 EMR

问：如何通过我的 AMS 账户申请访问亚马逊 EMR？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：

- customer_emr_cluster_instance_profile
- customer_emr_cluster_autoscaling_role
- customer_emr_console_role
- customer_emr_cluster_service_role

在您的账户中进行配置后，您必须在联合解决方案中加载 customer_emr_console_role。

问：在我的 AMS 账户中使用 Amazon EMR 有哪些限制？

通过 AWS 控制台在 EC2 集群上创建 Amazon EMR 时，我们建议您使用“创建集群-高级”选项。必须通过添加带有密钥“for-use-with-amazon-emr-managed-policies”且值为“true”的标签来创建 Amazon EMR 集群。在“安全”选项中选择以下配置：

- 为您的集群选择自定义角色：
 - EMR 角色：customer_emr_cluster_service_role
 - EC2 实例配置文件：customer_emr_cluster_instance_profile
 - Auto Scaling 角色：customer_emr_cluster_autoscaling_role
- EC2 安全组：
 - Master: ams-emr-master-security-group
 - 核心和任务：ams-emr-worker-security-group
 - 服务访问权限：ams-emr-serviceaccess-security-group

问：在我的 AMS 账户中使用 Amazon EMR 的先决条件或依赖条件是什么？

AMS 为 Amazon EMR 主节点、工作节点和服务节点创建默认安全组。

要用于 Amazon EMR 集群的启动模板和安全组必须具有标签密钥“for-use-with-amazon-”，值为“true emr-managed-policies”。

默认的 Amazon EMR 集群实例配置文件允许访问名称包含“emr”的 s3 存储桶和 dynamodb 表等资源。您可以申请其他 IAM 政策，以使用任何其他资源与 Amazon EMR 配合使用。以下资源 ARN 可以使用 customer_emr_cluster_instance_profile 用于亚马逊 EMR 任务：

- arn: aws: dynamodb: *: *: table/*emr*

- `arn: aws: kinesis: *: *: stream/*emr*`
- `arn: aws: sns: *: *: *emr*``arn: aws: sqs: *: *: *emr*`
- `arn: aws: sqs: *: *: *emr*`
- `arn: aws: sqs: *: *: AWS--* ElasticMapReduce`
- `arn: aws: sdb: *: *: domain: *emr*`
- `arn: aws: s3::: *emr*`

如果 Amazon EMR 集群需要 kerberos 身份验证：

- 提供用于每个 kerberized Amazon EMR 集群的领域名称和本地 Active Directory IP 地址。
- 基础架构要求：

多账户登录区 (MALZ)：提交 RFC 以在现有应用程序账户中创建新的托管应用程序账户或新 VPC。

单账户着陆区 (SALZ)：提交 RFC 以在您的 VPC 中创建新的子网。

- 在预置的 Active Directory 上为集群的领域配置传入信任。
- 提交 RFC 以在托管 AD 中为该领域配置 DNS 区域。
- 领域配置：

MALZ：提交管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC 以更新 VPC DHCP 选项设置为使用域名后缀的领域名称。

SALZ：提交管理 | 其他 | 其他 | 更新 (ct-0xdawir96cy7k) RFC 以生成新的亚马逊 EMR AMI，使用特定领域作为域名后缀。

要部署 Amazon EMR studio，该角色 `customer_emr_cluster_service_role` 必须具备亚马逊简单存储服务存储段的先决条件。要创建存储桶，请使用自动化 CT `ct-1a68ck03fn98r`（部署 | 高级堆栈组件 | S3 存储 | 创建）。当您使用此自动 CT 为 Amazon EMR 创建 Amazon S3 存储桶时，存储桶名称必须以前缀开头。 `customer-emr-` 而且，您必须在与 Amazon EMR AWS 集群相同的区域中创建存储桶。

使用 AMS SSP EventBridge 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊 EventBridge 功能。Amazon EventBridge 是一项无服务器事件总线服务，可以轻松地将您的应用程序与来自各种来源的数据连接起来。EventBridge 提供来自您自己的应用程序、Software-as-a-Service (SaaS) 应用程序

和 AWS 服务的实时数据流，并将这些数据路由到目标，例如 AWS Lambda。您可以设置路由规则来确定发送数据的目的地，以便构建能够实时响应所有数据源的应用程序架构。利用 EventBridge，您可以构建事件驱动的体系结构，这些体系结构是松散耦合的和分布式的。

要了解更多信息，请参阅 [Amazon EventBridge](#)。

EventBridge 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 EventBridge 中申请访问权限？

EventBridge 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：customer_eventbridge_role 和 customer_eventbridge_scheduler_execution_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

执行角色 customer_eventbridge_scheduler_execution_role 是一个 IAM 角色，EventBridge 日程安排器代替您与其他 AWS 服务角色进行交互。附加到此角色的权限策略授予 EventBridge 调度程序调用目标的访问权限。

Note

默认情况下，EventBridge 调度器使用 AWS 自有的密钥 EventBridge 对数据进行加密。要使用客户托管密钥对数据进行加密，请使用管理 | AWS 服务 | 自配置服务 | [添加 \(需要审核\) 更改类型 \(ct-3qe6io8t6jtny\)](#) 提交服务配置的 RFC。EventBridge

问：EventBridge 在我的 AMS 账户中使用有什么限制？

您必须提交 AMS RFCs 并创建以下资源：用于触发批处理作业的服务角色、SQS 队列 CodeBuild CodePipeline、和 SSM 命令。

问：在我的 AMS 账户 EventBridge 中使用的先决条件或依赖条件是什么？

在使用触发其他 EventBridge 资源（例如 Lambda、Amazon SNS、Amazon SQS 或亚马逊日志资源）之前，您必须使用部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建实体或策略（需要审查）更改类型 (ct-3dpd8m AWS dd9jn1r) 申请 EventBridge 服务角色。AWS Batch CloudWatch 指定在请求您的服务角色时要调用的服务。要了解调用目标所需的权限，请参阅 [使用基于资源的策略。EventBridge](#)

EventBridge 与 AWS CloudTrail 一项服务集成，该服务提供用户、角色或角色所执行操作 AWS 服务的记录 EventBridge。CloudTrail 必须启用并允许其将日志文件存储到 S3 存储桶中。注意：所有 AMS 账户均已 CloudTrail 启用，因此无需执行任何操作。

问：角色 `customer_eventbridge_scheduler_execution_role` 具有密钥的先决条件（如果用于加密，则为可选）。AWS Key Management Service 如何在静止/传输时采用 AWS KMS CMKs 数据加密？

默认情况下，S EventBridge scheduler 会加密其存储在 AWS 自有密钥下的事件元数据和消息数据（静态加密）。EventBridge 调度器还使用传输层安全 (TLS)（传输中的加密）对在 EventBridge 调度程序和其他服务之间传递的数据进行加密。

如果您的特定用例要求您控制和审核在 EventBridge 计划程序上保护您的数据的加密密钥，则可以使用客户托管密钥。

在使用 Amazon EventBridge 加入许可之前，您必须使用管理 AWS 服务 | 自行配置服务 | 添加（需要审核）更改类型申请 RFC。AWS KMS

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Forecast

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Forecast (Forecast) 功能。Amazon Forecast 是一项完全托管的服务，它使用机器学习来提供高度准确的预测。

Note

AWS 自 2024 年 7 月 29 日起，已关闭新买家访问 Amazon Forecast 的权限。Amazon Forecast 现有客户可以继续照常使用该服务。AWS 继续投资于 Amazon Forecast 的安全性、可用性和性能改进，但 AWS 不打算推出新功能。

如果你想使用 Amazon Forecast，请联系你的 CSDM，他们可以进一步指导你如何将你的 Amazon Forecast [使用转移到亚马逊 Can vas](#)。SageMaker

基于亚马逊使用的相同技术，Forecast 使用机器学习将时间序列数据与其他变量相结合以建立预测。Forecast 不需要任何机器学习经验即可开始使用。您只需要提供历史数据，以及您认为可能影响预测的任何其他数据。例如，对特定颜色的衬衫的需求可能会随着季节和商店位置的变化而变化。这种复杂的关系很难单独确定，但是机器学习非常适合识别这种关系。在您提供数据后，Forecast 将自动对其进行检查，确定哪些内容有意义，并生成一个预测模型，该模型能够做出比单独查看时间序列数据高出 50% 的预测准确性。

要了解更多信息，请参阅 [Amazon Forecast](#)。

AWS Managed Services 常见问题中的 Amazon Forecast

问：如何使用我的 AMS 账户申请访问 Forecast？

AWS Firewall Manager 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_forecast_admin_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Forecast 有哪些限制？

默认 S3 存储桶访问权限仅允许您访问命名模式为“customer-forecast-*”的存储桶。如果您对数据存储桶有自己的命名约定，请与您的云架构师 (CA) 讨论存储分区命名和相关访问权限设置。例如：

- 您可以定义您的特定的 Amazon Forecast 服务角色，命名为“AmazonForecast-ExecutionRole-”，并关联相应的 S3 存储桶访问权限。在 IAM 控制台中查看服务角色 AmazonForecast-ExecutionRole-Admin 和 IAM 策略-customer_forecast_default_s3_access_policy。
- 您可能需要将相关的 S3 存储桶访问权限关联到 IAM 联合角色中。在 IAM 控制台中查看 IAM 政策——customer_forecast_default_s3_access_policy。

问：在我的 AMS 账户中使用 Forecast 的先决条件或依赖条件是什么？

- 在使用 Forecast 之前，必须创建正确的 Amazon S3 存储桶。特别是，默认 S3 存储桶访问权限使用命名模式“customer-forecast-”
- 如果要在 S3 存储桶上使用除“customer-forecast-”之外的命名模式，则必须创建一个对存储桶具有 S3 访问权限的新服务角色：
 - 要创建一个命名为“AmazonForecast-ExecutionRole-{suffix}”的新服务角色。
 - 要创建的新 IAM 策略与 customer_forecast_default_s3_access_policy 类似，并将与新的服务角色和相关的联合管理员角色（例如“customer_forecast_admin_role”）相关联

问：在使用 Amazon Forecast 时，如何增强数据安全？

- 对于静态数据加密，您可以使用配置客户托管的 CMK AWS KMS 来保护 Amazon S3 服务上的数据存储：
 - 使用配置密钥在存储桶上启用默认加密，并将存储桶策略设置为在放置 AWS KMS 数据时接受数据加密。

- 启用 Amazon Forecast 服务角色 'AmazonForecast-ExecutionRole-*' 和联盟管理员角色 (例如 'customer_forecast_admin_role') 作为关键用户。AWS KMS
- 对于传输中的数据加密, 您可以设置 HTTPS 协议, 这是根据 Amazon S3 存储桶策略传输对象时所必需的。
- 对访问控制的进一步限制, 为 Amazon Forecast 服务角色 “AmazonForecast-ExecutionRole-*” 和管理员角色 (例如 “customer_forecast_admin_role”) 的已批准访问启用存储桶策略。

问: 使用 Amazon Forecast 时的最佳做法是什么?

- 在 Amazon Forecast 中使用 S3 存储桶时, 您应该充分了解自己的数据分类实践并规划相关的数据安全需求。
- 对于 Amazon S3 存储桶配置, 我们强烈建议您在 S3 存储桶策略中启用 HTTPS 强制执行。
- 您必须知道管理员角色 “customer_forecast_admin_role” 支持对亚马逊 S3 存储桶进行许可访问 (S3 对象 Get/Delete/Put), 命名为 “customer-forecast-*”。注意: 如果您需要对多个团队进行精细的访问控制, 请遵循以下做法:
 - 定义您的基于团队的访问权限 IAM 身份 (角色/用户), 对相关 Amazon S3 存储桶具有最低权限访问权限。
 - team/project 基于创建 AWS KMS CMKs 授予对应的 IAM 身份的适当访问权限。 (用户访问权限和 'AmazonForecast-ExecutionRole-{团队/项目}')。
 - 使用创建的设置 S3 存储桶默认加密 AWS KMS CMKs。
 - 在 S3 存储桶策略上使用 HTTPS 协议强制执行 S3 API 流量。
 - 对相关 IAM 身份 (用户访问权限和 “AmazonForecast-ExecutionRole-{team/project}”) 的已批准访问存储桶强制执行 S3 存储桶配置。
- 如果您想将 “customer_forecast_admin_role” 用于一般用途, 请考虑前面列出的保护 S3 存储桶的要点。

问: 有关 Amazon Forecast 的合规信息在哪里?

请参阅[AWS 服务合规计划](#)。

使用 AMS SSP FSx 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式, 直接在您的 AMS 托管账户中访问亚马逊 FSx 功能。Amazon FSx 提供完全托管的第三方文件系统。Amazon FSx 为您提供第三方文件系统的原生兼容性, 其功能集适用于基于 Windows 的存储、高性能计算 (HPC)、机器学习和电子设计自动化 (EDA) 等工作负

载。Amazon FSx 可自动执行耗时的管理任务，例如硬件配置、软件配置、修补和备份。Amazon FSx 将文件系统与云原生 AWS 服务集成，使其对更广泛的工作负载更加有用。

亚马逊 FSx 为您提供两种文件系统 FSx 供您选择：适用于基于 Windows 的应用程序的 Amazon Windows 文件服务器和适用于计算密集型工作负载的 Amazon FSx for Lustre。要了解更多信息，请参阅 [Amazon FSx](#)。

AWS Managed Services FSx 中的亚马逊常见问题解答

问：如何使用我的 AMS 账户申请访问亚马逊 FSx ？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问亚马逊 FSx。此 RFC 为您的账户配置以下 IAM 角色:customer_fsx_admin_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：FSx 在我的 AMS 账户中使用 Amazon 有哪些限制？

没有任何限制。该服务的全部功能都可用。

问：在我的 AMS 账户 FSx 中使用 Amazon 的先决条件或依赖条件是什么？

没有先决条件。但是，对于多可用区等高级配置，您必须安装和管理 DFS 复制和 DFS 命名空间服务。有关更多信息，请参阅[部署多可用区文件系统](#)。

问：如何将我的 Amazon FSx 文件系统与我的多账户 landing zone 托管 AD 集成？

创建亚马逊 FSx 文件系统时，您可以将您的 MALZ 托管 AD 指定为“AWS 托管的 Microsoft Active Directory”，用于 Windows 身份验证。有关更多信息，请参阅[将亚马逊 FSx 与微软 Active Directory Service 搭配使用](#)”

您还必须先将托管 AD 共享给应用程序账户。为此，请使用管理 | Directory Service | Directory Service | Directory | 共享目录更改类型 (ct-369odask0pd9w) 提交 RFC。

问：哪些用户属于 AWS 委派 FSx 管理员组？

只有 IT 文件服务器管理员。该组对所有文件共享都具有完全访问权限。

问：我是否应该使用在配置 FSx 系统时创建的默认文件共享（共享）？

不，我们不建议使用已配置的默认文件共享，即共享。它向所有人授予完全访问权限，这违反了最低权限原则。相反，可以创建更小的自定义文件共享，以满足您的业务需求。

问：如何为企业中的特定组织创建自定义文件共享？

有关创建自定义[文件共享](#)的说明，请参阅文件共享。使用最低权限原则限制对每个文件共享的访问权限。

使用 AMS SSP 在你的 AMS 账户中 FSx 为亚马逊配置 OpenZFS

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托 FSx 管账户中访问亚马逊 OpenZFS 功能。FSx for OpenZFS 是一项完全托管的文件存储服务，无需更改应用程序代码或数据管理方式，即可轻松地将本地 ZFS 或其他基于 Linux 的文件服务器中的数据移动到 AWS。它提供基于开源 OpenZFS 文件系统的高度可靠、可扩展、高性能和功能丰富的文件存储，提供 OpenZFS 文件系统熟悉的特性和功能，同时具有完全托管服务的敏捷性、可扩展性和简单性。AWS 对于构建云原生应用程序的开发人员，它提供了简单、高性能的存储，并具有丰富的数据处理功能。

FSx openZFS 文件系统可使用行业标准 NFS 协议 (v3、v4.0、v4.1、v4.2) 从 Linux、Windows 和 macOS 计算实例和容器中广泛访问。OpenZFS 由 AWS Graviton 处理器以及最新的 AWS 磁盘和网络技术 (包括 AWS 可扩展的可靠数据报网络和 AWS Nitro 系统) 提供支持，可提供高达 100 万个 IOPS，延迟 FSx 为数百微秒。凭借对即时 point-in-time 快照和数据克隆等 OpenZFS 功能的全面支持，FSx For OpenZFS 使您可以轻松地将本地文件服务器替换为提供熟悉文件系统功能的 AWS 存储，并且无需进行冗长的资格认证以及更改或重新架构现有应用程序或工具。而且，通过将 OpenZFS 数据管理功能的强大功能与最新 AWS 技术的高性能和成本效益相结合，for OpenZFS 使您能够构建和运行高性能、FSx 数据密集型应用程序。

作为一项完全托管 FSx 的服务，for OpenZFS 可以轻松启动、运行和扩展完全托管的文件系统 AWS，取代您在本地运行的文件服务器，同时有助于提供更好的灵活性和更低的成本。使用 f FSx or OpenZFS，您不必再担心设置和配置文件服务器和存储卷、复制数据、安装和修补文件服务器软件、检测和解决硬件故障以及手动执行备份。它还提供了与其他 AWS 服务的丰富集成，例如 AWS Identity and Access Management (IAM)、AWS Key Management Service (AWS KMS)、Amazon CloudWatch 和 AWS CloudTrail。

亚马逊 FSx 为您提供两种文件系统 FSx 供您选择：适用于基于 Windows 的应用程序的 Amazon Windows 文件服务器和适用于计算密集型工作负载的 Amazon fo FSx r Lustre。要了解更多信息，请参阅 [Amazon FSx](#)。

AWS Man FSx aged Services 常见问题解答中的亚马逊 OpenZFS

问：如何申请在我的 AMS 账户中使用 FSx OpenZFS 的访问权限？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8 FSx z66n899dct) 更改类型提交 RFC，请求访问亚马逊 OpenZFS。此 RFC 为您的账户配置以下 IAM 角色:customer_fsx_ontap_admin_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 FSx OpenZFS 有哪些限制？

替换 Amazon FSx 弹性网络接口 (ENIs) 上的安全组需要您提交“管理”|“其他”|“其他”|“更新”，RFCs 因为安全组是 AMS 环境的关键边界。这是唯一的限制。

问：在我的 AMS 账户中使用 FSx OpenZFS 有哪些先决条件或依赖关系？

没有先决条件。但是，您必须已[使用 AMS SSP FSx 在您的 AMS 账户中配置亚马逊](#)安装。

使用 AMS SSP 在您的 AMS 账户中 FSx 为 NetApp ONTAP 配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管 FSx 账户中访问 Amazon for NetApp ONTAP 功能。Amazon FSx for NetApp or ONTAP 是一项完全托管的服务，它基于广受欢迎的 ONTAP 文件系统提供高度可靠、可扩展、高性能和功能丰富的文件存储。NetApp 它提供了熟悉的特性、性能、功能和 APIs NetApp 文件系统，并具有完全托管的敏捷性、可扩展性和简单性 AWS 服务。

Amazon FSx for NetApp or ONTAP 提供功能丰富、快速且灵活的共享文件存储，可在本地或本地运行的 Linux、Windows 和 macOS 计算实例上广泛访问这些存储空间。AWS FSx for ONTAP 提供具有亚毫秒延迟的高性能 SSD 存储，您只需单击一下按钮即可快照、克隆和复制文件，从而可以快速轻松地管理数据。它还可以自动将您的数据分层到成本更低的弹性存储，从而无需预置或管理容量，并允许您实现工作负载的 SSD 性能级别，同时只需为一小部分数据支付 SSD 存储费用。它通过完全托管的备份提供高度可用和耐用的存储，并支持跨区域灾难恢复，并支持流行的数据安全和防病毒应用程序，使保护和保护数据变得更加容易。对于在本地使用 NetApp ONTAP 的客户 FSx 来说，for ONTAP 是将基于文件的应用程序从本地迁移、备份或突发到本地的理想解决方案，AWS 无需更改应用程序代码或数据管理方式。

作为一项完全托管的服务，Amazon FSx for NetApp ONTAP 可以轻松地在云中启动和扩展可靠、高性能和安全的共享文件存储。有了 Amazon FSx for NetApp ONTAP，您不必再担心设置和配置文件服务器和存储卷、复制数据、安装和修补文件服务器软件、检测和解决硬件故障、管理故障转移和故障恢复以及手动执行备份。它还提供了与其他 AWS 服务（例如 AWS Identity and Access Management Amazon WorkSpaces 和）的丰富集成 AWS CloudTrail。AWS Key Management Service

亚马逊 FSx 为您提供两种文件系统 FSx 供您选择：适用于基于 Windows 的应用程序的 Amazon Windows 文件服务器和适用于计算密集型工作负载的 Amazon for FSx Lustre。要了解更多信息，请参阅 [Amazon FSx](#)。

AWS Managed Services 常见问题解答中的亚马逊 NetApp ONTAP 版

问：如何使用我的 AMS 账户申请访问亚马逊 FSx NetApp ONTAP 版？

使用管理 | AWS 服务 | 自行配置服务 | 添加 (ct-1w8z66 NetApp n899dct) 更改类型提交 RFC，请求访问亚马逊 FSx ONTAP 版。此 RFC 为您的账户配置以下 IAM 角色:customer_fsx_ontap_admin_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon FSx for NetApp or ONTAP 有哪些限制？

将 Amazon 上的安全组替换 FSx 为 NetApp ONTAP 弹性网络接口 (ENIs) 需要您提交“管理 | 其他 | 其他 | 其他 | 更新”，RFCs 因为安全组是 AMS 环境的关键边界。这是唯一的限制。

问：在我的 AMS 账户中使用 Amazon FSx for NetApp ONTAP 有哪些先决条件或依赖关系？

没有先决条件。但是，您必须已[使用 AMS SSP FSx 在您的 AMS 账户中配置亚马逊](#)安装。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Inspector Classic

Note

终止支持通知：2026年5月20日，AWS 将终止对Amazon Inspector Classic的支持。2026 年 5 月 20 日之后，您将无法再访问亚马逊 Inspector Classic 控制台或亚马逊 Inspector Classic 资源。Amazon Inspector Classic 将不再适用于新账户和在过去六个月内未完成评估的账户。对于所有其他账户，访问权限将在 2026 年 5 月 20 日之前有效，之后您将无法再访问亚马逊 Inspector Classic 控制台或 Amazon Inspector Classic 资源。有关更多信息，请参阅 [Amazon Inspector Classic 终止支持](#)。

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Inspector Classic 功能。Amazon Inspector Classic 是一项自动安全评估服务，可帮助提高部署在其上的应用程序的安全性和合规性 AWS。Amazon Inspector Classic 会自动评估应用程序的漏洞、漏洞以及与最佳实践的偏差。执行评估后，Amazon Inspector Classic 会生成一份按严重程度排列优先顺序的安全发现的详细清单。这些发现可以直接查看，也可以作为详细评估报告的一部分进行审查，这些报告可通过 Amazon Inspector Classic 控制台或 API 获得。要了解更多信息，请参阅 [Amazon Inspector 经典版](#)。

AWS Managed Services 常见问题中的亚马逊 Inspector

问：如何使用我的 AMS 账户申请访问 Amazon Inspector Classic？

使用管理 | AWS 服务 | 自行配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Amazon Inspector Classic。此 RFC 为您的账户customer_inspector_admin_role配置 IAM 角

色。该角色包括 AWS 托管 AmazonInspectorFullAccess 策略。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Inspector Classic 有哪些限制？

没有任何限制。Amazon Inspector Classic 的全部功能可在你的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Inspector Classic 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 Amazon Inspector Classic 没有任何先决条件或依赖关系。

在 AMS 中使用全新 Amazon Inspector

现在，你可以在你的 AMS 账户中使用新的 Amazon Inspector。

对于 Amazon Inspector Classic `AmazonInspectorFullAccess`，必须使用 `customer-inspector-admin-role-ssm-inspector-agent-policy` 和。但是，SSPS 角色已更新 `customer-inspector-admin-role`，现在包括一个新增 `policyAmazonInspector2FullAccess` 角色。这项新政策允许使用新版本的 Amazon Inspector 的 API 权限。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Kendra

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Kendra 功能。Amazon Kendra 是一项智能搜索服务，它使用自然语言处理和高级机器学习算法，从您的数据中返回搜索问题的具体答案。与传统的基于关键字的搜索不同，Amazon Kendra 使用其语义和上下文理解功能来确定文档是否与搜索查询相关。Amazon Kendra 会返回问题的具体答案，因此您的体验接近于与人类专家互动。Amazon Kendra 具有高度的可扩展性，能够满足性能需求，与 Amazon S3 和 Amazon Lex 等其他 AWS 服务紧密集成，并提供企业级安全性。要了解更多信息，请参阅 [Amazon Kendra](#)。

AWS Managed Services 常见问题解答中的亚马逊 Kendra

问：如何使用我的 AMS 账户申请访问亚马逊 Kendra？

要申请访问 Amazon Inspector Classic，请使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-3qe6io8t6jtny) 更改类型提交 RFC。此 RFC 为您的账户 `customer_kendra_console_role` 配置 IAM 角色。在您的账户中配置后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Kendra 有哪些限制？

没有任何限制。Amazon Kendra 的全部功能可在您的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Kendra 的先决条件或依赖条件是什么？

开始使用 Amazon Kendra 没有任何先决条件或依赖关系。但是，根据您的具体用例，您可能需要访问其他 AWS 服务。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Kinesis Data Streams

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Kinesis Data Streams (KDS) 功能。Amazon Kinesis Data Streams 是一项高度可扩展、耐用的实时数据流服务。KDS 每秒可以持续捕获来自成千上万个来源（例如网站点击流、数据库事件流、财务交易、社交媒体源、IT 日志和位置跟踪事件）的千兆字节数据。收集的数据可在毫秒内获得，以实现实时分析用例，例如实时仪表板、实时异常检测、动态定价等。要了解更多信息，请参阅 [Amazon Kinesis Data Streams](#)。

AWS Managed Services 中的 Kinesis Data Streams 常见问题解答

常见问题和答案：

问：如何通过我的 AMS 账户申请访问亚马逊 Kinesis Data Streams？

通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC，请求访问亚马逊 Kinesis Data Streams。此 RFC 为您的账户配置以下 IAM 角色:customer_kinesis_data_streaming_user_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Kinesis Data Streams 有哪些限制？

没有任何限制。Amazon Kinesis Data Streams 的全部功能可在你的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Kinesis Data Streams 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 Amazon Kinesis Data Streams 没有任何先决条件或依赖关系。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Kinesis Video Streams

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Kinesis Video Streams (KVS) 功能。Amazon Kinesis Video Streams 可帮助您安全地将视频从联网设备流式传输 AWS 到用于分析、机器学习 (ML)、播放和其他处理的目的。Kinesis Video Streams 可自动配置并弹性扩展从数百万台设备摄取流视频数据所需的所有基础架构。它还可以持久地存储、加密和索引直播中的视频数据，并允许您通过访问数据。easy-to-use APIs Kinesis Video Streams 使您能够播放用于直播和点播观看的视频，并通过与 Amazon Rekognition Video 以及 Apache 和 OpenCV MxNet 等

TensorFlow机器学习框架的库集成，快速构建利用计算机视觉和视频分析的应用程序。要了解更多信息，请参阅 [Amazon Kinesis Video Streams](#)。

AWS Managed Services 中的亚马逊 Kinesis Video Streams 常见问题解答

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 Kinesis Video Streams Amazon Kinesis Video Streams？

使用管理 AWS | 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC，请求访问亚马逊 Kinesis Video Streams。此 RFC 为您的账户配置以下 IAM 角色:customer_kinesis_video_streaming_user_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Kinesis Video Streams 有哪些限制？

没有任何限制。Amazon Kinesis Video Streams 的全部功能可在你的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Amazon Kinesis Video Streams 有哪些先决条件或依赖关系？

在你的 AMS 账户中使用 Amazon Kinesis Video Streams 没有先决条件或依赖关系。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Lex

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Lex 功能。Amazon Lex 是一项使用语音和文本在任何应用程序中构建对话界面的服务。Amazon Lex 提供高级深度学习功能，包括用于将语音转换为文本的自动语音识别 (ASR) 和用于识别文本意图的自然语言理解 (NLU)，使您能够构建具有高度吸引力的用户体验和逼真的对话互动的应用程序。借助 Amazon Lex，任何开发者都可以使用支持 Amazon Alexa 的深度学习技术，使您能够快速轻松地构建复杂的自然语言、对话机器人或聊天机器人。要了解更多信息，请参阅 [Amazon Lex](#)。

AWS Managed Services 中的亚马逊 Lex 常见问题解答

常见问题和答案：

问：如何使用我的 AMS 账户申请访问 Amazon Lex？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_lex_author_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Lex 有哪些限制？

为了防止对 AMS 基础设施进行任何修改，Amazon Lex 与 Lambda 的集成仅限于没有“AMS-”前缀的 Lambda 函数。

问：在我的 AMS 账户中使用 Amazon Lex 有哪些先决条件或依赖条件？

在您的 AMS 账户中使用 Amazon Lex 没有任何先决条件或依赖关系。

使用 AMS SSP 在您的 AMS 账户中配置亚马逊 MQ

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon MQ 功能。Amazon MQ 是一项适用于 Apache ActiveMQ 的托管消息代理服务，可帮助您在云中设置和操作消息代理。消息代理允许不同的软件系统（通常使用不同的编程语言和不同的平台）来通信和交换信息。Amazon MQ 通过管理流行的开源消息代理 ActiveMQ 的配置、设置和维护来减轻您的运营负担。将您当前的应用程序连接到 Amazon MQ 使用行业标准 APIs 和消息传递协议，包括 JMS、NMS、AMQP、STOMP、MQTT 和 WebSocket。使用标准意味着，在大多数情况下，迁移到 AWS 时无需重写任何消息传递代码。要了解更多信息，请参阅[什么是 Amazon MQ](#)？

AWS Managed Services 常见问题解答中的亚马逊 MQ

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 MQ？

在您的 AMS 账户中使用亚马逊 MQ 的过程分为两步：

1. 配置亚马逊 MQ 代理。为此，请通过包含亚马逊 MQ Broker 的 RFC 提交 CFN 模板，其中包含部署 | Ingestion | Stack CloudFormation from template | 创建更改类型 (ct-36cn2avfrj9v)，或者使用管理层 | 其他 | 其他 | 创建更改类型 (ct-1e1xtak34nx76) 更改类型提交 RFC，请求配置亚马逊 MQ Broker 已存入您的账户。
2. 访问亚马逊 MQ 控制台。配置亚马逊 MQ Broker 后，使用管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC，即可访问亚马逊 MQ 控制台。此 RFC 为您的账户配置以下 IAM 角色:customer_mq_console_role。

在您的账户中配置该角色后，您必须将其加入您的联合解决方案中。

问：在我的 AMS 账户中使用 Amazon MQ 有哪些限制？

Amazon MQ 的全部功能可在您的 AMS 账户中使用；但是，由于需要提升权限，因此无法通过该政策配置亚马逊 MQ Broker。有关如何在您的账户中配置 Amazon MQ 经纪商的详细信息，请参阅上文。

问：在我的 AMS 账户中使用 Amazon MQ 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 Amazon MQ 没有任何先决条件或依赖关系。

使用 AMS SSP 在你的 AMS 账户中为 Apache Flink 配置亚马逊托管服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问适用于 Apache Flink 的亚马逊托管服务功能。适用于 Apache Flink 的托管服务是分析流数据、获得切实可行的见解以及实时响应业务和客户需求的最简单方法。适用于 Apache Flink 的 Amazon 托管服务降低了构建、管理流应用程序以及与其他 AWS 服务集成的复杂性。SQL 用户可以使用模板和交互式 SQL 编辑器轻松查询流数据或构建整个流应用程序。Java 开发人员可以使用开源 Java 库和 AWS 集成快速构建复杂的流媒体应用程序，以实时转换和分析数据。适用于 Apache Flink 的 Amazon 托管服务负责处理持续运行实时应用程序所需的一切，并自动扩展以匹配传入数据的数量和吞吐量。使用适用于 Apache Flink 的亚马逊托管服务，您只需为流媒体应用程序消耗的资源付费。没有最低费用或安装成本。要了解更多信息，请参阅适用于 [Apache Flink 的亚马逊托管服务](#)。

AWS Managed Services 常见问题解答中的 Apache Flink 托管服务

常见问题和答案：

问：如何使用我的 AMS 账户申请访问适用于 Apache Flink 的亚马逊托管服务？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角

色:customer_kinesis_analytics_application_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用适用于 Apache Flink 的亚马逊托管服务有哪些限制？

- 配置仅限于没有“AMS-”或“MC-”前缀的资源，以防止对 AMS 基础设施进行任何修改。
- 删除或创建新 Kinesis Data Streams 或 Firehose 的权限已从该政策中删除。我们还有另一项允许这样做的政策。

问：在我的 AMS 账户中使用 Amazon Kinesis Data Streams 有哪些先决条件或依赖关系？

有几个依赖关系：

- 适用于 Apache Flink 的亚马逊托管服务要求在使用适用于 Apache Flink 的托管服务配置应用程序之前，必须先创建 Kinesis Data Streams 或 Firehose。
- 基于资源的策略权限应指明特定的输入数据源。

使用 AMS SSP 在你的 AMS 账户中为 Apache Kafka 配置亚马逊托管流媒体 Kafka

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问适用于 Apache Kafka 的亚马逊托管流媒体（亚马逊 MSK）功能。适用于 Apache Kafka 的 Amazon Managed Streaming 是一项完全 AWS 托管的流数据服务，可让您轻松构建和运行使用 Apache Kafka 处理流数据的应用程序，而无需成为 Apache Kafka 集群操作专家。Amazon MSK 为您管理 Apache Kafka 集群和 Apache 节点的配置、配置和维护。ZooKeeper 亚马逊 MSK 还在控制台中显示了 Apache Kafka 的关键性能指标。

AWS

Amazon MSK 为您的 Apache Kafka 集群提供多个级别的安全保护，包括 VPC 网络隔离、用于控制平面 API 授权的 AWS IAM、静态加密、传输中的 TLS 加密、基于 TLS 的证书身份验证、受保护的身份验证。SASL/SCRAM AWS Secrets Manager 要了解更多信息，请参阅 [Amazon MSK](#)。

AWS Managed Services 常见问题解答中的亚马逊 MSK

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 MSK？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 策略和角色：

- customer-msk-admin-policy.json
- AmazonMSKFullAccess
- customer-msk-admin-role.json

在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：使用 Amazon MSK 有哪些限制？

要让 Amazon MSK 将代理日志传送到您配置的目标，请确保将 AmazonMSKFullAccess 策略附加到您的 IAM 角色。因此，完全访问权限已经到位。

问：使用 Amazon MSK 的先决条件或依赖条件是什么？

在创建 MSK 集群之前，您必须拥有一个 VPC 并在该 VPC 内拥有子网。默认情况下，AMS 在 [创建 AMS VPC](#) 时会将其包括在内。

要了解亚马逊 MSK 的限制，请参阅 [亚马逊 MSK 限制](#)。

使用 AMS SSP 在您的 AMS 账户中为 Prometheus 配置亚马逊托管服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问适用于 Prometheus 的亚马逊托管服务 (AMP) 功能。Amazon Managed Service for Prometheus 是一项面向容器指标的无服务器 Prometheus 兼容监控服务，有助于更轻松地实现对容器环境的大规模监控。借助 Amazon Managed Service for Prometheus，您可以使用目前所用的开源 Prometheus 数据模型和查询语言来监控容器化工作负载的性能，还可以享受更高的可扩展性、可用性和安全性，而无需管理底层基础设施。

Amazon Prometheus 托管服务会随着工作负载的扩大和缩小规模而自动扩展操作指标的摄取、存储和查询。它与 AWS 安全服务集成，可以快速、安全地访问数据。有关更多信息，请参阅[什么是 Prometheus 的亚马逊托管服务？](#)

AWS Managed Services 常见问题解答中的亚马逊 Prometheus 托管服务

常见问题和答案：

问：如何使用我的 AMS 账户申请访问适用于 Prometheus 的亚马逊 Prometheus 托管服务？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer-prometheus-console-role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该customer-prometheus-console-role角色。

问：在我的 AMS 账户中使用适用于 Prometheus 的亚马逊 Prometheus 托管服务有哪些限制？

支持所有功能。

问：在我的 AMS 账户中使用适用于 Prometheus 的亚马逊 Prometheus 托管服务有哪些先决条件或依赖关系？

开始使用适用于 Prometheus 的亚马逊托管服务没有任何先决条件或依赖关系。但是，根据您的具体用例，您可能需要访问其他 AWS 服务。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Personalize

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Personalize 功能。Amazon Personalize 是一项机器学习服务，可让开发人员轻松为使用其应用程序的客户创建个性化推荐。

机器学习越来越多地用于通过提供个性化的产品和内容推荐、量身定制的搜索结果和有针对性的营销促销来提高客户参与度。但是，由于复杂性，开发制作这些复杂的推荐系统所必需的机器学习能力已超出了当今大多数组织的能力。Amazon Personalize 允许以前没有机器学习经验的开发者使用经过多年在 Amazon.com 上使用而完善的机器学习技术，轻松地在其应用程序中构建复杂的个性化功能。

借助 Amazon Personalize，您可以提供来自应用程序的活动流（点击量、页面浏览量、注册次数、购买次数等）以及您想要推荐的商品（例如文章、产品、视频或音乐）的清单。您也可以选择向 Amazon Personalize 提供来自用户的其他人口统计信息，例如年龄或地理位置。Amazon Personalize 将处理和检查数据，确定有意义的内容，选择正确的算法，并训练和优化针对您的数据定制的个性化模型。Amazon Personalize 分析的所有数据都是保密和安全的，并且仅用于您的定制推荐。您可以通过简单的 API 调用开始提供个性化推荐。您只需按实际用量付费，没有最低费用，也没有预先承诺。

要了解更多信息，请参阅 [Amazon Personalize](#)。

AWS Managed Services 常见问题解答中的亚马逊个性化

问：如何使用我的 AMS 账户申请访问 Amazon Personalize？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny)

更改类型来请求访问权限，您需要指定哪个 S3 存储桶包含用于个

性化生成推荐的数据。AWS 此 RFC 为您的账户配置以下 IAM 角

色：customer_personalize_console_role 和 customer_personalize_service_role

- 在您的账户中配置 customer_personalize_console_role 完毕后，您必须在联合解决方案中加入该角色。您也可以将附加 customer_personalize_console_policy 到除之外的其他现有角色 Customer_ReadOnly_Role。
- 向您的账户提供后，您可以在创建新的数据集组时参考其 ARN。customer_personalize_service_role

此时，AMS Operations 还将在您的账户中部署此服务角

色：aws_code_pipeline_service_role_policy。

问：在我的 AMS 账户中使用 Amazon Personalize 有哪些限制？

Amazon Personalize 配置仅限于没有“ams-”或“mc-”前缀的资源，以防止对 AMS 基础设施进行任何修改。

问：在我的 AMS 账户中使用 Amazon Personalize 有哪些先决条件或依赖条件？

- 如果存储数据的 S3 存储桶已加密，则必须提供 KMS 密钥 ID，这样我们就可以允许 Amazon Personalize 使用的角色解密该存储桶。

Amazon Personalize 不支持默认 KMS S3 密钥。如果需要使用 KMS，请创建一个自定义密钥，然后打开 RFC，并使用更改类型 KMS Key | Create（需要查看），向其添加以下策略：

JSON

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy-3",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}
```

- 必须使用以下存储桶策略创建 S3 存储桶。为此，请提交 RFC，更改类型为 S3 存储 | 创建策略。该政策允许 Amazon Personalize 访问数据；该存储桶将包含供亚马逊个性化使用的数据。

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PersonalizeS3BucketAccessPolicy",
  "Statement": [
    {
      "Sid": "PersonalizeS3BucketAccessPolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "personalize.amazonaws.com"
      },
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
      ]
    }
  ]
}
```

```
}
```

使用 AMS SSP QuickSight 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 QuickSight 功能。QuickSight 是一项快速、基于云的商业智能服务，可为组织中的每个人提供见解。作为一项完全托管的服务，QuickSight 您可以轻松创建和发布包含机器学习 (ML) 见解的交互式仪表板。要了解更多信息，请参阅 [Amazon QuickSight](#)。

QuickSight 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 QuickSight 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_quicksight_console_admin_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：QuickSight 在我的 AMS 账户中使用有什么限制？

- AWS 由于 IAM 策略依赖关系，您 QuickSight 无法访问上的资源设置。但是，AMS 团队会根据您启用服务的请求为您启用每项资源。
- 此模式不支持个人用户和群组的资源访问权限，因为此功能允许用户更改可能危及 AMS 基础设施的 IAM 权限。
- 由于更改 IAM 对象涉及风险，QuickSight 因此不支持从内部邀请 IAM 身份。
- QuickSight 服务提供两个版本：企业版和标准版。两者都提供了 AMS 支持的单点登录 (SSO) 选项。但是，企业版可以选择 QuickSight 与活动目录 (AD) 集成。QuickSight 由于 AMS 账户结构与信任要求不兼容，在 AMS 上不支持与 AD 集成。QuickSight

问：在我的 AMS 账户 QuickSight 中使用的先决条件或依赖条件是什么？

- 当 AMS 收到要添加的 RFC 时 QuickSight，您会收到一份服务请求，要求您提供更多信息；请向他们提供以下信息：
 - QuickSight 账户名（例如，*CustomerName*-quicksight
 - QuickSight 版本（标准版与企业版）

- 启用 QuickSight 服务的 AWS 区域 (默认为您的 AMS AWS 区域) 。
- QuickSight 账户的通知电子邮件地址。
- (可选) 要分析的数据文件所在的 S3 存储桶。
- 连接 IDs 的 VPC 和子网 QuickSight 支持添加 VPC 连接的功能，该功能可在账户内 QuickSight 和资源之间实现私有连接。

AMS 操作员代表您执行注册流程并配置两个 QuickSight 功能：

- [自动发现](#)数据源。
- [VPC 连接](#)。

 Note

这些操作需要由 AMS 操作员执行，因为在登录过程中需要提升的 IAM 和 VPC 权限。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Rekognition

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Rekognition 功能。Amazon Rekognition 使用久经考验、高度可扩展的深度学习技术，无需机器学习专业知识即可轻松地将图像和视频分析添加到您的应用程序中。借助 Amazon Rekognition，您可以识别图像和视频中的物体、人物、文本、场景和活动，还可以检测任何不当内容。Amazon Rekognition 还提供高度准确的面部分析和面部搜索功能，您可以使用这些功能来检测、分析和比较人脸，用于各种用户验证、人数统计和公共安全用例。

借助 Amazon Rekognition 自定义标签，您可以识别图像中特定于您的业务需求的对象和场景。例如，您可以构建模型来对装配线上的特定机器零件进行分类或检测不健康的工厂。Amazon Rekognition Custom Labels 为您处理模型开发的繁重工作，因此无需任何机器学习经验。您只需要提供要识别的物体或场景的图像，剩下的交给服务即可。

要了解更多信息，请参阅[亚马逊 Rekognition](#)。

AWS Managed Services 常见问题解答中的亚马逊 Rekognition

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 Rekognition？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_rekognition_console_role & customer_rekognition_service_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Rekognition 有哪些限制？

亚马逊 Rekognition 的全部功能可通过亚马逊 Rekognition 自行配置服务角色获得。

问：在我的 AMS 账户中使用 Amazon Rekognition 有哪些先决条件或依赖关系？

如果您使用为亚马逊 Rekognition Video 流处理器或数据流提供源流视频的 Kinesis Video Streams 作为向 Kinesis Data Streams 写入数据的目标，请在创建 RFC 时向 AMS 提供。kinesisStreamName

使用 AMS SSP 在你的 AMS 账户中配置 SageMaker Amazon AI

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 SageMaker Amazon AI 功能。SageMaker AI 为每位开发人员和数据科学家提供了快速构建、训练和部署机器学习模型的能力。Amazon SageMaker AI 是一项完全托管的服务，涵盖了整个机器学习工作流程，包括标记和准备数据、选择算法、训练模型、调整和优化模型以进行部署、做出预测和采取行动。您的模型能够以更少的工作量和更低的成本更快地投入生产。要了解更多信息，请参阅 [Amazon SageMaker AI](#)。

SageMaker AWS Managed Services 中的人工智能常见问题

常见问题和答案：

问：如何使用我的 AMS 账户申请访问 SageMaker AI？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：customer_sagemaker_admin_role和服务角色AmazonSageMaker-ExecutionRole-Admin。在您的账户中配置 SageMaker AI 后，您必须在联合解决方案中加入该customer_sagemaker_admin_role角色。您无法直接访问服务角色；SageMaker AI 服务在执行各种操作时使用该角色，如下所述：[传递角色](#)。

问：在我的 AMS 账户中使用 SageMaker AI 有哪些限制？

- AMS Amazon A SageMaker I IAM 角色不支持以下用例：
 - SageMaker 目前不支持 AI Studio。
 - SageMaker 不支持 AI Ground Truth 来管理私人工，因为此功能需要过于宽松地访问 Amazon Cognito 资源。如果需要管理私人工，则可以申请一个具有 A SageMaker I 和 Amazon Cognito

权限相结合的自定义 IAM 角色。否则，我们建议使用公共劳动力（由 Amazon Mechanical Turk 提供支持）或 AWS Marketplace 服务提供商进行数据标记。

- 创建 VPC 终端节点以支持对 SageMaker AI 服务的 API 调用（aws.sagemaker. {区域}.notebook, com.amazonaws. {region}.sagemaker.api & com.amazonaws. 不支持 {region}.sagemaker.runtime），因为权限不能仅限于人工智能相关的服务。SageMaker 要支持此用例，请提交[管理 | 其他 | 其他 RFC](#) 以创建相关的 VPC 终端节点。
- SageMaker 不支持 AI 端点自动缩放，因为 SageMaker AI 需要任何 (“*”) 资源的 DeleteAlarm 权限。要支持端点自动缩放，请提交[“管理 | 其他 | 其他 | 其他 RFC”](#) 来为 SageMaker AI 终端节点设置自动缩放。

问：在我的 AMS 账户中使用 SageMaker AI 的先决条件或依赖条件是什么？

- 以下用例需要在使用前进行特殊配置：
 - 如果要使用 S3 存储桶来存储模型工件和数据，则必须使用[部署 | 高级堆栈组件 | S3 存储 | 创建 RFC](#) 请求一个以所需关键字（”、SageMaker “Sagemaker”、“sagemaker” 或 “aws-glue”）命名的 S3 存储桶。
 - 如果要使用弹性文件存储 (EFS)，则必须在同一个子网中配置 EFS 存储，并且必须得到安全组的允许。
 - 如果其他资源需要直接访问 SageMaker AI 服务（笔记本、API、运行时等），则必须通过以下方式请求配置：
 - 提交 RFC 以为终端节点创建安全组（[部署 | 高级堆栈组件 | 安全组 | 创建 \(auto\)](#)）。
 - 提交[管理 | 其他 | 其他 | 创建 RFC](#) 以设置相关的 VPC 终端节点。

问：对于 **customer_sagemaker_admin_role** 可以直接访问的资源，支持的命名约定有哪些？（以下内容适用于更新和删除权限；如果您需要其他支持的资源命名约定，请联系 AMS Cloud Architect 进行咨询。）

- 资源：传递 AmazonSageMaker-ExecutionRole-* 角色
 - 权限：SageMaker AI 自行配置的服务角色支持您使用 SageMaker AI 服务角色 (AmazonSageMaker-ExecutionRole-*) 和 AWS Glue AWS RoboMaker、和。AWS Step Functions
- 资源：Secrets Manager 上的 AWS 秘密
 - 权限：使用 AmazonSageMaker-* 前缀描述、创建、获取、更新密钥。
 - 权限：当 SageMaker 资源标签设置为时，描述、获取机密 true。

- 资源：存储库开启 AWS CodeCommit
 - 权限：创建/删除带AmazonSageMaker-*前缀的仓库。
 - 权限：在带有以下前缀的存储库 Pull/Push 上使用 Git *sagemaker*、*SageMaker*、和。*Sagemaker*
- 资源：Amazon ECR (亚马逊弹性容器注册表) 存储库
 - 权限：权限：使用以下资源命名约定，设置、删除存储库策略和上传容器镜像*sagemaker*。
- 资源：亚马逊 S3 存储桶
 - 权限：当资源具有以下前缀时，获取、放置、删除对象、中止分段上传 S3 对象：*SageMaker*、*Sagemaker*和。*sagemaker* aws-glue
 - 权限：当SageMaker标签设置为时获取 S3 对象true。
- 资源：Amazon CloudWatch 日志组
 - 权限：创建日志组或流、放置日志事件、列出、更新、创建、删除带以下前缀的日志传送：/aws/sagemaker/*。
- 资源：Amazon CloudWatch 指标
 - 权限：使用以下前缀时放入指标数据：AWS/SageMaker、AWS/SageMaker/、aws/SageMaker、aws/SageMaker/、aws/sagemakeraws/sagemaker/、和/aws/sagemaker/。。
- 资源：Amazon CloudWatch 控制面板
 - 权限:使用以下前缀时的 Create/Delete 仪表板:customer_*
- 资源：Amazon SNS (简单通知服务) 主题
 - 权限：使用以下前缀时 Subscribe/Create 的主题：*sagemaker**SageMaker*、和。*Sagemaker*

问：AmazonSageMakerFullAccess和有什么区别customer_sagemaker_admin_role？

customer_sagemaker_admin_role与customer_sagemaker_admin_policy提供的权限几乎相同，唯一的 AmazonSageMakerFullAccess 不同是：

- 连接 Amazon Cognito 和 AWS Glue 资源的权限。AWS RoboMaker
- SageMaker AI 端点自动缩放。您必须通过管理 | 高级堆栈组件 | 身份和访问管理 (IAM) Management | 更新实体或策略 (需要审查) 更改类型 (ct-27tuth19k52b4) 提交 RFC 才能临时或永久提升自动扩展权限，因为自动扩展需要对服务的许可访问权限。CloudWatch

问：如何在静态数据加密中采用 AWS KMS 客户托管密钥？

您必须确保已在客户托管密钥上正确设置密钥策略，以便相关的 IAM 用户或角色可以使用这些密钥。有关更多信息，请参阅[AWS KMS 密钥策略文档](#)。

使用 AMS SSP 在您的 AMS 账户中配置 Amazon 简单电子邮件服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊简单电子邮件服务 (Amazon SES) 功能。Amazon Simple Email Service 是一项基于云的电子邮件发送服务，旨在帮助数字营销人员和应用程序开发人员发送营销、通知和交易电子邮件。

您可以使用 SMTP 接口或其中一个接口将 Amazon SES 直接集成 AWS SDKs 到您的现有应用程序中。您还可以将 Amazon SES 的电子邮件发送功能集成到您已经使用的软件中，例如票务系统和电子邮件客户端。

要了解更多信息，请参阅 [Amazon 简单电子邮件服务](#)。

AWS Managed Services 中的亚马逊 SES 常见问题解答

问：如何使用我的 AMS 账户申请访问 Amazon SES？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Amazon SES。此 RFC 为您的账户配置以下 IAM 角色:customer_ses_admin_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon SES 有哪些先决条件或依赖条件？

- 您必须配置 S3 存储桶策略以允许 Amazon SES 向存储桶发布事件。
- 您必须使用默认 (S AWS ES) 或配置 CMK 密钥，以允许 Amazon SES 加密电子邮件并将事件推送到属于该账户的其他服务资源，例如 Amazon S3、Amazon SNS、Lambda 和 Firehose。

问：在我的 AMS 账户中使用 Amazon SES 有哪些限制？

您必须筹集 RFCs 才能创建以下资源：

- PutEvents 有权访问 Kinesis Firehose 直播的 SMTP 用户和 IAM 服务角色。
- 您必须使用 AMS 更改类型创建 S3 存储桶、Firehose 流、SNS 主题等新 AWS 资源，这样您的 Amazon SES 规则和配置集的目标才能使用这些资源。
- SMTP 凭证。要申请新的 SMTP 凭证，请使用更改类型（管理 | 其他 | 其他 | 创建）。AMS 会为您创建凭证并将其添加到 Secrets Manager 中。

使用 AMS SSP 在您的 AMS 账户中配置 Amazon 简单工作流程服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问亚马逊简单工作流程服务 (Amazon SWF) Simple Workflow Service 功能。Amazon Simple Workflow Service 可帮助开发人员构建、运行和扩展具有并行或顺序步骤的后台作业。您可以将 Amazon SWF 视为云端完全托管的状态跟踪器和任务协调器。如果您的应用程序的步骤需要超过 500 毫秒才能完成，则需要跟踪处理状态，或者在任务失败时需要恢复或重试，Amazon SWF 可以为您提供帮助。要了解更多信息，请参阅 [Amazon 简单工作流程服务](#)。

AWS Managed Services 常见问题解答中的亚马逊 SWF

常见问题和答案：

问：如何使用我的 AMS 账户申请访问亚马逊 SWF？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_swf_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon SWF 有哪些限制？

Lambda InvokeFunction 权限已包含在该服务中，但是，添加到所有 AMS customer_deny_policy 客户角色的 AMS 明确拒绝访问 AMS Lambda 函数和 AMS 拥有的资源。要在 Amazon SWF 中标记或取消标记资源，请提交“管理 | 其他 | 其他更改类型”。

问：在我的 AMS 账户中使用 Amazon SWF 有哪些先决条件或依赖条件？

Amazon SWF 依赖于该 AWS Lambda 服务，因此，该角色提供了调用 Lambda 的权限，并且无需其他权限即可从亚马逊 SWF 调用 Lambda。否则，使用 Amazon SWF 没有任何先决条件。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Textract

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Textract 功能。Amazon Textract 是一项完全托管的机器学习服务，可自动从扫描的文档中提取打印的文本、手写和其他数据，这些数据超出了简单的光学字符识别 (OCR) 范围，可以识别、理解和提取表单和表格中的数据。要了解更多信息，请参阅 [Amazon Textract](#)。

AWS Managed Services 常见问题解答中的亚马逊 Textract

常见问题和答案：

问：如何申请在我的 AMS 账户中设置亚马逊 Textract？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：

customer_textract_console_role、customer_textract_human_review_execution_role、和 customer_ec2_textract_instance_profile。在您的账户中配置该角色后，您必须在联合解决方案 customer_textract_console_role 中加入该角色。

问：在我的 AMS 账户中使用亚马逊 Textract 有哪些限制？

在您的 AMS 账户中使用亚马逊 Textract 没有任何限制。

问：在我的 AMS 账户中使用 Amazon Textract 有哪些先决条件或依赖条件？

您必须通过提交 RFC 部署 | 高级堆栈组件 | S3 存储 | 创建 (ct-1a68ck03fn98r) 来请求创建 S3 存储桶。

使用 AMS SSP 在你的 AMS 账户中配置 Amazon Transcribe

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Amazon Transcribe 功能。Amazon Transcribe 是一项完全托管且持续训练的自动语音识别服务，可自动从音频文件生成带有时间戳的文本脚本。借助 Amazon Transcribe，开发人员可以轻松地为 speech-to-text 应用程序添加功能。计算机几乎不可能搜索和分析音频数据。因此，录制的语音需要先转换为文本，然后才能用于应用程序。从历史上看，客户必须与转录提供商合作，这些提供商要求他们签订昂贵的合同，并且很难集成到他们的技术堆栈中来完成这项任务。这些提供商中有许多使用过时的技术，无法很好地适应不同的场景，例如联络中心常见的低保真电话音频，这会导致准确性差。

Amazon Transcribe 使用一种称为自动语音识别 (ASR) 的深度学习过程来快速准确地将语音转换为文本。Amazon Transcribe 可用于转录客户服务电话、自动添加隐藏式字幕和字幕，以及生成媒体资产的元数据以创建完全可搜索的档案。您可以使用 Amazon Transcribe Medical 为临床文档应用程序添加医疗 speech-to-text 功能。要了解更多信息，请参阅 [Amazon Transcribe](#)。

AWS Managed Services 中的亚马逊转录常见问题解答

常见问题和答案：

问：如何申请在我的 AMS 账户中设置 Amazon Transcribe？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：customer_transcribe_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Amazon Transcribe 有哪些限制？

使用 transcribe 时，您必须使用 “customer-transcribe*” 作为存储桶的前缀，除非 RA 和另有说明。

您无法在 Amazon 转录中创建 IAM 角色。

您不能使用服务托管 S3 存储桶存储默认 SSP 中的输出数据（如果需要，请联系您的账户 CA）。

如果您想使用不属于 AMS 命名空间的客户管理的 KMS 密钥，则必须提交“风险接受”。

问：在我的 AMS 账户中使用 Amazon Transcribe 有哪些先决条件或依赖条件？

S3 必须有权访问名为“客户转录*”的存储桶。如果您的 S3 存储桶使用 KMS 密钥加密，则需要使用 KMS 才能使用 Amazon Transcribe。如果存储桶不需要加密，则可以删除“KMStranscribeAllow”。

使用 AMS SSP WorkSpaces 在您的 AMS 账户中配置亚马逊

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 WorkSpaces 功能。

WorkSpaces 允许你为用户配置基于云的虚拟 Microsoft Windows 或 Amazon Linux 桌面，称为 WorkSpaces。WorkSpaces 无需购买和部署硬件或安装复杂的软件。您可以根据需求的变更，快速添加或删除用户。用户使用 WorkSpaces 支持的设备上的客户端应用程序或者（对于 Windows，则使用 Web 浏览器）进行访问 WorkSpaces，然后使用现有的本地 Active Directory (AD) 凭据登录。

要了解更多信息，请参阅 [Amazon WorkSpaces](#)。

WorkSpaces 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何在 AMS 账户 WorkSpaces 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_workspaces_console_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：WorkSpaces 在我的 AMS 账户中使用有什么限制？

Amazon WorkSpaces 自行配置的服务角色提供了工作空间的全部功能。

问：在我的 AMS 账户 WorkSpaces 中使用的先决条件或依赖条件是什么？

- WorkSpaces 受 AWS 区域限制；因此，AD Connector 必须配置在托管 WorkSpaces 实例的同一 AWS 区域。

客户可以使用以下两种方法之一 WorkSpaces 连接到客户 AD：

1. 使用 AD 连接器代理对本地 Active Directory 服务的身份验证（首选）：

在将您的 WorkSpaces 实例与本地目录服务集成之前，在您的 AMS 账户中配置 Active Directory (AD) 连接器。AD Connector 充当您的现有 AD 用户（来自您的域）的代理，让他们 WorkSpaces 使用现有本地 AD 凭据进行连接。这是首选，因为 WorkSpaces 它们可以直接加入客户的本地域，该域既充当资源林，又充当用户林，从而增强了客户方面的控制权。

有关更多信息，请参阅[部署 Amazon 的最佳实践 WorkSpaces（场景 1）](#)。

2. 将 AD Connector 与 AWS 微软 AD、共享服务 VPC 以及对本地的单向信任一起使用：

您还可以先建立从 AMS 管理的 AD 到您的本地 AD 的单向传出信任，从而使用本地目录对用户进行身份验证。WorkSpaces 将使用 AD Connector 加入 AMS 管理的 AD。WorkSpaces 然后，访问权限将通过 AMS 托管的 AD 委派给 WorkSpaces 实例，无需与您的本地环境建立双向信任。在这种情况下，用户林将位于客户 AD 中，资源林将位于 AMS 管理的 AD 中（可以通过 RFC 请求对 AMS 管理的 AD 进行更改）。请注意，WorkSpaces VPC 和运行 AMS 托管 AD 的 MALZ 共享服务 VPC 之间的连接是通过 Transit Gateway 建立的。

有关更多信息，请参阅[部署 Amazon 的最佳实践 WorkSpaces（场景 6）](#)。

 Note

可以通过提交“管理 | 其他 | 其他 | 其他 | 创建更改类型 RFC”来配置 AD Connector，其中包含先决条件 AD 配置的详细信息；有关更多信息，请参阅[创建 AD 连接器](#)。如果使用方法 2 在 AMS 管理的 AD 中创建资源林，请通过运行 AMS 管理的 AD 在 AMS 共享服务账户中提交另一个管理 | 其他 | 其他 | 创建更改类型 RFC。

使用 AMS SSP 在您的 AMS 账户中配置 AMS 代码服务

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 AMS Code 服务功能。AMS Code 服务是 AWS 代码管理服务的专有捆绑包，详见下文。您可以选择使用 AMS Code 服务在 AMS 中部署所有服务，也可以在 AMS 中单独部署这些服务。

AMS 代码服务包括以下服务：

- AWS CodeCommit：一种完全托管的[源代码控制](#)服务，用于托管基于 Git 的安全存储库。它使团队可以在安全且高度可扩展的生态系统中协作处理代码。CodeCommit 无需操作自己的源代码控制

系统或担心扩展其基础架构。您可以使用 CodeCommit 将源代码中的内容安全地存储到二进制文件中，并且它可与您现有的 Git 工具无缝协作。要了解更多信息，请参阅 [AWS CodeCommit](#)。

要将其独立于 AMS Code 服务部署到您的 AMS 账户中，请参阅[使用 AMS SSP AWS CodeCommit 在您的 AMS 账户中进行配置](#)。

- AWS CodeBuild：一种完全托管的持续集成服务，用于编译源代码、运行测试和生成随时可以部署的软件包。使用 CodeBuild，您无需预置、管理和扩展自己的构建服务器。CodeBuild 持续扩展并同时处理多个构建，因此您的构建不会在队列中等待。您可以使用预先打包的构建环境快速开始，也可以创建使用您自己的构建工具的自定义构建环境。使用 CodeBuild，按分钟计费所使用的计算资源。要了解更多信息，请参阅 [AWS CodeBuild](#)。

要将其独立于 AMS Code 服务部署到您的 AMS 账户中，请参阅[使用 AMS SSP AWS CodeBuild 在您的 AMS 账户中进行配置](#)。

- AWS CodeDeploy：一项完全托管的部署服务，可自动将软件部署到各种计算服务，例如 Amazon EC2 和您的本地服务器。AWS CodeDeploy 帮助您快速发布新功能，帮助您避免应用程序部署期间的停机，并处理更新应用程序的复杂性。您可以使用 AWS CodeDeploy 自动化软件部署，无需进行容易出错的手动操作。该服务可根据您的部署需求进行扩展。要了解更多信息，请参阅 [AWS CodeDeploy](#)。

要将其独立于 AMS Code 服务部署到您的 AMS 账户中，请参阅[使用 AMS SSP AWS CodeDeploy 在您的 AMS 账户中进行预配置](#)。

- AWS CodePipeline：一项完全托管的[持续交付](#)服务，可帮助您实现发布管道的自动化，从而实现快速可靠的应用程序和基础设施更新。CodePipeline 每次发生代码更改时，都会根据您的发布模型自动执行发布过程的构建、测试和部署阶段。这让您可以快速而可靠地交付各种功能和更新。您可以轻松地 AWS CodePipeline 与第三方服务集成，例如 GitHub 或与您自己的自定义插件集成。使用 AWS CodePipeline，您只需为实际用量付费。无前期费用，无长期承诺。要了解更多信息，请参阅 [AWS CodePipeline](#)。

要将其独立于 AMS Code 服务部署到您的 AMS 账户中，请参阅[使用 AMS SSP AWS CodePipeline 在您的 AMS 账户中进行预配置](#)。

AWS Managed Services 常见问题解答中的 AMS 代码服务

问：如何使用我的 AMS 账户申请访问 AMS Code 服务？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_code_suite_console_role。在您的账户中配置后，您必须在联合解决方案中加入该角色。此时，AMS Operation

`customer_codebuild_service_role`s 还将在您的账户中为 CodeDeploy 和 `aws_code_pipeline_service_role` 服务部署 CodeBuild、CodePipeline 服务角色。`customer_codedeploy_service_role` 如果需要其他 IAM 权限，请提交 AMS 服务请求。`customer_codebuild_service_role`

Note

您也可以单独添加这些服务；有关信息，请分别参见[使用 AMS SSP AWS CodeBuild 在您的 AMS 账户中进行配置](#)、[使用 AMS SSP AWS CodeDeploy 在您的 AMS 账户中进行预配置](#)、[使用 AMS SSP AWS CodePipeline 在您的 AMS 账户中进行预配置](#)、和。

问：在我的 AMS 账户中使用 AMS 代码服务有哪些限制？

- AWS CodeCommit：如果具有创建 SNS 主题的相关权限，CodeCommit 则开启的触发器功能已禁用。直接进行身份验证受到限制；用户应使用 Cre CodeCommit dential Helper 进行身份验证。某些 KMS 命令也受到限制：`kms:加密`、`kms:解密`、`kms:ReEncrypt`、`kms:GenereteDataKey`、`kms:GenerateDataKeyWithoutPlaintext`、和 `kms: DescribeKey`
- CodeBuild：对于 AWS CodeBuild 控制台管理员访问权限，权限在资源级别受到限制；例如，对特定资源的 CloudWatch 操作受到限制，`iam:PassRole` 权限受到控制。
- CodeDeploy：目前仅 CodeDeploy 支持在 Amazon EC2 /本地部署。不支持通过 CodeDeploy ECS 和 Lambda 进行部署。
- CodePipeline: CodePipeline 功能、阶段和提供者仅限于以下内容：
 - 部署阶段：亚马逊 S3 和 AWS CodeDeploy
 - 来源阶段：Amazon S3、AWS CodeCommit、Bit Bucket 和 GitHub
 - 建造阶段：AWS CodeBuild 还有 Jenkins
 - 批准阶段：亚马逊 SNS
 - 测试阶段：AWS CodeBuild、Jenkins、、Ghost Inspector UI 测试、Micro Focus Loa StormRunner d、Runscope BlazeMeter
 - 调用阶段：Step Functions 和 Lambda

Note

AMS Operations `customer_code_pipeline_lambda_policy` 在您的账户中部署；它必须与 Lambda 调用阶段的 Lambda 执行角色相关联。提供您想要添加此策略的 Lambda `service/execution` 角色名称。如果没有自定义 Lambda `service/execution` 角色，则 AMS

会创建一个名为的新角色`customer_code_pipeline_lambda_execution_role`，该角色是和的 `customer_lambda_basic_execution_role`副本。`customer_code_pipeline_lambda_policy`

问：在我的 AMS 账户中使用 AMS Code 服务的先决条件或依赖条件是什么？

- CodeCommit：如果 S3 存储桶使用 AWS KMS 密钥加密，AWS KMS 则必须使用 AWS CodeCommit S3 和。
- CodeBuild：如果定义的 AWS CodeBuild 服务角色需要其他 IAM 权限，请通过 AMS 服务请求请求这些权限。
- CodeDeploy：无。
- CodePipeline：无。AWS 支持的服务 AWS CodeDeploy—AWS CodeCommit AWS CodeBuild、— 必须在发布之前或同时启动。CodePipeline但是，这是由 AMS 工程师完成的。

使用 AMS SSP AWS Amplify 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Amplify 功能。AWS Amplify 这是一个完整的解决方案，允许前端 Web 和移动开发人员轻松构建、连接和托管全栈应用程序。随着用例的演变，Amplify 可以灵活地利用 AWS 服务的广度。Amplify 提供用于构建全栈 iOS、安卓、Flutter、Web 和 React Native 应用程序的产品。要了解更多信息，请参阅[AWS Amplify](#)。

AWS Amplify 在 AWS Managed Services 常见问题中

常见问题和答案：

问：AWS Amplify 如何申请在我的 AMS 账户中进行设置？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:`customer_amplify_console_role`. 配置到您的账户后，您必须在联合解决方案中加入该角色。

此外，您必须提供风险接受，因为您 AWS Amplify 拥有基础架构变更权限。为此，请与您的云服务交付经理 (CSDM) 合作。

问：AWS Amplify 在我的 AMS 账户中使用有什么限制？

使用 Amplify 时，您必须使用 '`amplify*`' 作为存储桶的前缀，除非 RA 和另有说明。

问：在我的 AMS 账户 AWS Amplify 中使用的先决条件或依赖条件是什么？

在您的 AMS 账户 AWS Amplify 中使用没有任何先决条件。

仅限 Malz 环境：Amplify 的默认载入角色是“customer_amplify_console_role”。要使用自定义角色，请先部署 IAM 实体。然后，再创建一个 RFC，将您的自定义角色添加到应用程序帐户的服务控制策略允许列表中。

使用 AMS SSP 进行配置 AWS AppSync

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS AppSync 功能。AWS AppSync 允许您创建灵活的 API 来安全地访问、操作和合并来自一个或多个数据源的数据，从而简化应用程序开发。AWS AppSync 是一项托管服务，它使用 GraphQL 让应用程序可以轻松地准确获取所需的数据。

借助 AWS AppSync，您可以在一系列数据源（例如 NoSQL 数据存储、关系数据库、HTTP APIs 和自定义数据源）上构建可扩展的应用程序，包括那些需要实时更新的应用程序。AWS Lambda 对于移动和 Web 应用程序，AWS AppSync 还可在设备离线时提供本地数据访问权限，并在设备重新联机时提供可自定义冲突解决方案的数据同步。要了解更多信息，请参阅[AWS AppSync](#)。

AWS AppSync 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何使用我的 AMS 账户申请访问权限 AWS AppSync？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角

色：customer_appsync_service_role 和 customer_appsync_author_role。在您的账户中配置后，您必须在联合解决方案 customer_appsync_author_role 中加载。

问：使用有哪些限制 AWS AppSync？

- 在客户上 AppSync 创建数据源时，需要指定先前创建的服务角色，不允许创建新角色，因此会返回访问被拒绝的消息
- AppSync 角色配置为限制对包含“AMS-”或“MC-”前缀的资源的权限，以防止对 AMS 基础设施进行任何修改。

问：使用的先决条件或依赖关系 AWS AppSync 是什么？

该服务允许将多个其他服务用作数据源，因此使用这些服务的基本权限包含在服务角色 (customer_appsync_service_role) 中，但在使用服务时必须手动选择服务角色。

使用 AMS SSP AWS App Mesh 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS App Mesh 功能。AWS App Mesh 提供应用程序级联网，使您的服务可以轻松地在多种类型的计算基础设施之间相互通信。App Mesh 标准化了您的服务通信方式，为您提供 end-to-end 可视性并确保应用程序的高可用性。

AWS App Mesh 通过为跨多种类型的计算基础设施构建的服务提供一致的可见性和网络流量控制，使服务运行变得更加容易。App Mesh 无需更新应用程序代码，即可更改监控数据的收集方式或服务间流量的路由方式。App Mesh 将每项服务配置为导出监控数据，并在整个应用程序中实现一致的通信控制逻辑。这样可以轻松快速查明错误的确切位置，并在出现故障或需要部署代码更改时自动重新路由网络流量。要了解更多信息，请参阅[AWS App Mesh](#)。

AWS App Mesh 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何使用我的 AMS 账户申请访问权限 AWS App Mesh ？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_app_mesh_console_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：使用有哪些限制 AWS App Mesh ？

的全部功能可在您 AWS App Mesh 的 AMS 账户中使用。

问：使用的先决条件或依赖关系 AWS App Mesh 是什么？

您的 AMS 账户 AWS App Mesh 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Audit Manager 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Audit Manager 功能。Audit Manager 可帮助您持续审计 AWS 使用情况，以简化评估风险以及对法规和行业标准的合规性的方式。Audit Manager 可自动收集证据，以便更轻松地评估您的策略、过程和活动是否有效运行。当需要进行审计时，Audit Manager 可以帮助您管理利益相关者对控制措施的审查，并帮助您以更少的手动工作来生成可供审计的报告。要了解更多信息，请参阅 Audit [Manager](#)。

AWS Audit Manager 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS Audit Manager 的 AMS 账户？

您可以通过提交 AWS 服务 RFC 管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 来申请访问权限。此 RFC 在您的账户中配置以下 IAM 角色:customer-audit-manager-admin-Role. 在您的账户中配置后，您必须在联合解决方案中加入该角色。

问：使用有什么限制 AWS Audit Manager？

在您的 AMS 账户 AWS Audit Manager 中使用没有任何限制。提供了 AWS Audit Manager 的全部功能。

问：使用的先决条件或依赖关系 AWS Audit Manager是什么？

1. 您需要向 AMS 提供您 reports/assessments 要存放的 s3 存储桶。
2. 如果您想使用该服务进行加密，则需要向 AMS 提供要使用的 KMS CMK ARN。
3. 如果您想向某个主题发送 SNS 通知，则必须提供该主题的名称或 arn。
4. (可选) 如果您想在 Audit Manager 中启用 Organizations 作为多账户登录区域的一部分，并且想要委托管理员帐户，则还有一个额外的先决条件：在 RFC (管理 | AWS 服务 | 兼容服务 | 添加) 的描述字段中，提及您要在 Audit Manager 设置中使用委派管理员帐户，并提供以下详细信息：
 - KMS CMK ARN (最初用于设置 Audit Manager)
 - Audit Manager 可以用作此多账户登录区域一部分的委托管理员账户 ID (可以是 MALZ 应用程序帐户)

使用 AMS SSP AWS Batch 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Batch 功能。AWS Batch 使开发人员、科学家和工程师能够轻松高效地运行成千上万的批量计算作业 AWS。AWS Batch 根据提交的批处理作业的容量和特定资源要求，动态配置计算资源的最佳数量和类型 (例如 CPU 或内存优化型实例)。有了它 AWS Batch，您无需安装和管理用于运行作业的批处理计算软件或服务集群，这样您就可以专注于分析结果和解决问题。要了解更多信息，请参阅[AWS Batch](#)。

AWS Batch 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS Batch 的 AMS 账户？

1. 要申请访问权限 AWS Batch，请提交 RFC 管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct)。此 RFC 在您的账户中配置了以下 IAM 角色和策略：

IAM 角色：

- customer_batch_console_role
- customer_batch_ecs_instance_role
- customer_batch_events_service_role
- customer_batch_service_role
- customer_batch_ecs_task_role

策略：

- customer_batch_console_role_policy
- customer_batch_service_role_policy
- customer_batch_events_service_role_policy

2. 在您的账户中配置后，您必须在联合解决方案customer_batch_console_role中加入该角色。

问：使用有什么限制 AWS Batch？

创建计算环境时，应将 EC2 实例标记为“customer_batch”或“customer_batch”。如果未标记实例，则在任务完成时不会批量终止实例。

问：使用的先决条件或依赖关系 AWS Batch是什么？

您的 AMS 账户 AWS Batch 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Certificate Manager 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接在您的 AMS 托管账户中访问 AWS Certificate Manager (ACM) 功能。AWS Certificate Manager 是一项服务，允许您预置、管理和部署用于服务和内部连接资源的公共和私有安全套接字 Layer/Transport 层安全 (SSL/TLS) 证书。AWS SSL/TLS 证书用于保护网络通信并通过互联网确定网站的身份以及私有网络上的资源。AWS Certificate Manager 消除了购买、上传和续订 SSL/TLS 证书的耗时手动流程。

借助 AWS Certificate Manager，您可以申请证书，将其部署到集成 ACM 的 AWS 资源（例如弹性负载均衡器、Amazon CloudFront 分配）和 API APIs Gateway 上，然后让我们来 AWS Certificate Manager 处理证书续订。它还使您能够为内部资源创建私有证书，并集中管理证书生命周期。通过预配置的 AWS Certificate Manager 用于集成 ACM 的服务的公有和私有证书是免费的。您只需为运行应用程序而创建的 AWS 资源付费。使用 [AWS 私有证书颁发机构](#)，您按月支付操作费用 AWS 私有 CA 和您颁发的私有证书的费用。要了解更多信息，请参阅 [AWS Certificate Manager - AWS 文档](#)。

AWS Managed Services 中的 ACM 常见问题解答

常见问题和答案：

问：如何在 AMS 账户 AWS Certificate Manager 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_acm_create_role. 您可以使用此角色来创建和管理 ACM 证书。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

即使您尚未添加 IAM 角色，也可以使用以下更改类型创建 AC customer_acm_create_role M 证书：

- [ACM | 创建公共证书](#)
- [ACM | 创建私有证书](#)
- [ACM 证书及其他 SANs | 创建](#)

问：使用有哪些限制 AWS Certificate Manager？

您必须向 AMS 提交更改申请 (RFC) 才能删除或修改现有证书，因为这些操作需要完全的管理员访问权限（使用管理 | 其他 | 其他 | 更新更改类型 (ct-0xdawir96cy7k)。请注意，IAM 策略不能根据标签名称（mc*、ams* 等）排除权限。证书不产生费用，因此删除未使用的证书对时间不敏感。

问：使用 Certificate Manager 的先决条件或依赖条件是什么？

现有的公有 DNS 名称和创建 DNS 别名记录的访问权限，但这些记录无需托管在托管账户中。

使用 AMS SSP AWS 私有证书颁发机构 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS 私有证书颁发机构 功能。私有证书用于识别和保护私有网络上互联资源之间的通信，例如服务器、移动设备和物联网设备和应用程序。AWS 私有 CA 是一项托管私有 CA 服务，可帮助您轻松安全地管理私有证书的生命周期。

AWS 私有 CA 为您提供高度可用的私有 CA 服务，无需支付运营自己的私有 CA 的前期投资和持续维护成本。AWS 私有 CA 将 ACM 的证书管理功能扩展到私有证书，使您能够集中创建和管理公有和私有证书。您可以使用 AWS 管理控制台或 ACM API 轻松地为您 AWS 资源创建和部署私有证书。对于 EC2 实例、容器、物联网设备和本地资源，您可以轻松创建和跟踪私有证书，并使用自己的客户端自动化代码进行部署。对于需要自定义证书生命周期、密钥算法或资源名称的应用程序，您还可以灵活地创建私有证书并自行管理这些证书。要了解更多信息，请参阅[AWS 私有 CA](#)。

AWS 私有 CA 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何使用我的 AMS 账户申请访问权限 AWS 私有 CA ？

通过提交 AWS 服务 RFC (管理 | 服务 | 兼容 AWS 服务) 来申请访问权限。通过此 RFC，将在您的账户中配置以下 IAM 角色：。customer_acm_pca_role在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：使用有哪些限制 AWS 私有 CA ？

目前，AWS Resource Access Manager (AWS RAM) 不能用于共享您的 AWS 私有 CA 跨账户。

问：使用的先决条件或依赖关系 AWS 私有 CA是什么？

1. 如果您计划创建 CRL，则需要一个 S3 存储桶来存储它。AWS 私有 CA 自动将 CRL 存入您指定的 Amazon S3 存储桶中，并定期对其进行更新。在设置 CRL 之前，S3 存储桶必须具有以下存储桶策略。要继续处理此请求，请按如下方式使用 ct-0fpjlx808sh2 (管理 | 高级堆栈组件 | S3 存储 | 更新策略) 创建 RFC：

- 提供 S3 存储桶名称或 ARN。
- 将以下策略复制到 RFC 上，并bucket-name替换为所需的 S3 存储桶名称。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "acm-pca.amazonaws.com"
      }
    }
  ]
}
```

```

    },
    "Action":[
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
    ],
    "Resource":[
        "arn:aws:s3:::bucket-name/*",
        "arn:aws:s3:::bucket-name"
    ]
}
]
}

```

2. 如果上述 S3 存储桶已加密，则服务主体 `acm-pca.amazonaws.com` 需要解密权限。要继续处理此请求，请按如下方式使用 `ct-3ovo7px2vsa6n`（[管理](#) | [高级堆栈组件](#) | [KMS 密钥](#) | [更新](#)）创建 RFC：

- 提供必须更新策略的 KMS 密钥 ARN。
- 将以下策略复制到 RFC 上，并 `bucket-name` 替换为所需的 S3 存储桶名称。

```

{
  "Sid":"Allow ACM-PCA use of the key",
  "Effect":"Allow",
  "Principal":{
    "Service":"acm-pca.amazonaws.com"
  },
  "Action":[
    "kms:GenerateDataKey",
    "kms:Decrypt"
  ],
  "Resource": "*",
  "Condition":{"
    "StringLike":{"
      "kms:EncryptionContext:aws:s3:arn":[
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
        "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
        "arn:aws:s3:::bucket_name/audit-report/*",
        "arn:aws:s3:::bucket_name/crl/*"
      ]
    }
  }
}

```

```
}  
}
```

3. AWS 私有 CA CRLs 不支持 S3 设置“阻止通过新的访问控制列表 (ACLs) 授予的对存储桶和对象的公开访问权限”。您必须对 S3 账户和存储桶禁用此设置才能允许写入，CRLs 如[如何安全地创建和存储 ACM Private CA 的 CRL 中所述](#)。如果您想禁用，请使用 ct-0xdawir96cy7k (管理 | 其他 | 其他 | 更新) 创建一个新的 RFC 并附上风险接受书。AWS 私有 CA 如果您对风险接受有任何疑问，请联系您的云架构师。

使用 AMS SSP AWS CloudEndure 在您的 AMS 账户中进行配置

Note

成功推出后 AWS Application Migration Service，CloudEndure 迁移服务现已在所有 AWS 地区停用。我们建议客户使用 AWS Application Migration Service 升降和转移到 GovCloud 区域和商业区域的迁移。有关信息，请参阅[什么是 AWS Application Migration Service？](#)。

如果您想使用 AWS Application Migration Service，请联系您的 CA，以便他们为您提供指导。

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CloudEndure 功能。AWS CloudEndure 迁移可简化、加快和自动化从物理、虚拟和基于云的基础架构向的大规模迁移。AWS CloudEndure 灾难恢复 (DR) 可防止任何威胁（包括勒索软件和服务器损坏）造成的停机和数据丢失。

AWS CloudEndure 在 AWS Managed Services 常见问题中

问：如何申请访问我 CloudEndure 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 将以下 IAM 用户配置到您的账户:customer_cloud_endure_user。在您的账户中配置访问密钥和密钥后，将在 Secrets Manager 中共享该用户的访问密钥和 AWS 密钥。

这些策略也已配置到账

户：customer_cloud_endure_policy和。customer_cloud_endure_deny_policy

此外，您必须提供风险承受能力，因为用于应用程序集成的 CloudEndure 灾难恢复解决方案具有基础架构变更权限。为此，请与您的云服务交付经理 (CSDM) 合作。

问：CloudEndure 在我的 AMS 账户中使用有什么限制？

云端忍受复制和转换实例只能在您指定的子网中启动。

问：在我的 AMS 账户 CloudEndure 中使用的先决条件或依赖条件是什么？通过 RFC 双向通信共享以下内容：

- 要启动的复制和转换实例的 VPC 子网详细信息。
- 如果 EBS 卷已加密，则为 KMS 密钥亚马逊资源名称 (ARN)。

使用 AMS SSP AWS CloudHSM 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CloudHSM 功能。AWS CloudHSM 通过在 AWS 云中使用专用的硬件安全模块 (HSM) 实例，帮助您满足企业、合同和监管机构对数据安全的合规性要求。AWS 和 AWS Marketplace 合作伙伴提供了各种解决方案来保护 AWS 平台内的敏感数据，但是对于某些受合同或监管要求约束的管理加密密钥的应用程序和数据，可能需要额外的保护。AWS CloudHSM 补充现有的数据保护解决方案，并允许您保护其中的加密密钥 HSMs，这些密钥是按照政府安全密钥管理标准设计和验证的。AWS CloudHSM 允许您以只有您才能访问的方式安全地生成、存储和管理用于数据加密的加密密钥。要了解更多信息，请参阅[AWS CloudHSM](#)。

AWS CloudHSM 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS CloudHSM 的 AMS 账户？

在您的 AMS 账户中使用分为两个步骤：

1. 请求集 AWS CloudHSM 群。为此，请提交 RFC，其中包含管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型。请包括以下详细信息：
 - AWS 区域。
 - 与您提交的 RFC 属于同一账户的 VPC ID/ARN. Provide a VPC ID/VPC ARN.
 - 为集群指定至少两个可用区。
 - 将连接到 HSM 集群的亚马逊 EC2 实例 ID。
2. 访问控制 AWS CloudHSM 台。为此，请使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC。此 RFC 为您的账户配置以下 IAM 角色:customer_cloudhsm_console_role.

在您的账户中配置该角色后，您必须将其加入您的联合解决方案中。

问：AWS CloudHSM 在我的 AMS 账户中使用有什么限制？

访问 AWS CloudHSM 控制台不允许您创建、终止或恢复集群。要做这些事情，请提交“管理 | 其他 | 其他 | 创建变更类型 (ct-1e1xtak34nx76)”变更类型。

问：在我的 AMS 账户 AWS CloudHSM 中使用的先决条件或依赖条件是什么？

您必须允许 TCP 流量使用端口 2225 通过 VPC 内的客户端 Amazon EC2 实例，或者要访问 HSM 集群的本地服务器使用 Direct Connect VPN。AWS CloudHSM 依赖于 Amazon EC2 来提供安全组和网络接口。对于日志监控或审计，HSM 依赖 CloudTrail（AWS API 操作）和 CloudWatch 日志来处理所有本地 HSM 设备活动。

问：谁将对 AWS CloudHSM 客户端和相关软件库进行更新？

您负责应用库和客户端更新。您需要监视 [CloudHSM 版本历史记录页面上的版本](#)，然后使用 [CloudHSM 客户端升级](#)来应用更新。

Note

HSM 设备的软件补丁始终由该 AWS CloudHSM 服务自动应用。

使用 AMS SSP AWS CodeBuild 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CodeBuild 功能。AWS CodeBuild 是一项完全托管的持续集成服务，用于编译源代码、运行测试和生成随时可以部署的软件包。使用 CodeBuild，您无需预置、管理和扩展自己的构建服务器。CodeBuild 持续扩展并同时处理多个构建，因此您的构建不会排队等待。您可以使用预先打包的构建环境快速开始，也可以创建使用您自己的构建工具的自定义构建环境。使用 CodeBuild，按分钟计费所使用的计算资源。要了解更多信息，请参阅[AWS CodeBuild](#)。

Note

要加载 CodeCommit、CodeBuild CodeDeploy、和 CodePipeline 使用单个 RFC，请提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型并请求三项服务：和。CodeBuild CodeDeploy CodePipeline然后，所有三个角色、customer_codebuild_service_rolecustomer_codedeploy_service_role、和aws_code_pipeline_service_role都将在您的账户中配置。在您的账户中进行配置后，您必须在联合解决方案中加入该角色。

CodeBuild 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS CodeBuild 的 AMS 账户？

AWS CodeBuild 在您的 AMS 账户中使用分为两个步骤：

1. 预置构建流程以与 AWS S3 存储桶、Amazon CloudWatch 和日志组进行协调 CodeBuild Service Role
2. 请求访问控制 CodeBuild 台

您可以通过管理 | AWS 服务 | 自配服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC，请求在您的 AMS 账户中同时设置两者。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：AWS CodeBuild 在我的 AMS 账户中使用有什么限制？

对于 AWS CodeBuild 控制台管理员的访问权限，权限受资源级别的限制；例如，对特定资源的 CloudWatch 操作受到限制，iam:PassRole 权限受到控制。

问：在我的 AMS 账户 CodeBuild 中使用的先决条件或依赖条件是什么？

如果定义的 AWS CodeBuild 服务角色需要其他 IAM 权限，请通过 AMS 服务请求进行申请。

使用 AMS SSP AWS CodeCommit 在您的 AMS 账户中进行配置

Note

AWS 自 2024 年 7 月 25 日 AWS CodeCommit 起，已关闭新客户访问权限。AWS CodeCommit 现有客户可以继续照常使用该服务。AWS 继续投资于安全性、可用性和性能改进 AWS CodeCommit，但我们不打算引入新功能。

要将 AWS CodeCommit Git 存储库迁移到其他 Git 提供商，请联系您的云架构师 (CA) 寻求指导。有关迁移 Git 存储库的更多信息，请参阅[如何将您的 AWS CodeCommit 存储库迁移到其他 Git 提供商](#)。

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CodeCommit 功能。AWS CodeCommit 是一项完全托管的[源代码控制](#)服务，用于托管基于 Git 的安全存储库。它可以帮助

团队在安全且高度可扩展的生态系统中协作处理代码。CodeCommit 无需操作自己的源代码控制系统或担心扩展其基础架构。您可以使用 CodeCommit 安全地存储从源代码到二进制文件的所有内容，并且它可以与现有 Git 工具无缝协作。要了解更多信息，请参阅[AWS CodeCommit](#)。

Note

要加载 CodeCommit、CodeBuild CodeDeploy、和 CodePipeline 使用单个 RFC，请提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型并请求三项服务：和。CodeBuild CodeDeploy CodePipeline 然后，所有三个角色、customer_codebuild_service_role、customer_codedeploy_service_role、和 aws_code_pipeline_service_role 都将在您的账户中配置。在您的账户中进行配置后，您必须在联合解决方案中加入该角色。

CodeCommit 在 AWS Managed Services 常见问题中

问：如何申请访问我 CodeCommit 的 AMS 账户？

AWS CodeCommit 可以通过提交两个 AWS 服务 RFCs、控制台访问和数据访问权限来请求控制台和数据访问角色：

- AWS CodeCommit 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：customer_codecommit_console_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

数据访问（例如训练和实体列表）要求每个数据源分别 CTs 指定 S3 数据源（必填）、输出存储桶（必填）和 KMS（可选）。只要所有数据源都被授予访问角色，就不会限制创建 AWS CodeCommit 就业机会。要申请数据访问权限，请向管理层 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 提交 RFC。

问：AWS CodeCommit 在我的 AMS 账户中使用有什么限制？

如果具有创建 SNS 主题的相关权限，CodeCommit 则会禁用开启的触发器功能。直接进行身份验证受到限制，用户应使用 Cre CodeCommit dential Helper 进行身份验证。某些 KMS 命令也受到限制：kms:Encryptkms:Decryptkms:ReEncrypt、kms:GenereteDataKey、kms:GenerateDataKey和kms:DescribeKey。

问：在我的 AMS 账户 AWS CodeCommit 中使用的先决条件或依赖条件是什么？

如果使用 KMS 密钥加密 S3 存储桶，则必须使用 AWS CodeCommit S3 和 KMS。

使用 AMS SSP AWS CodeDeploy 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CodeDeploy 功能。AWS CodeDeploy 是一项完全托管的部署服务，可自动将软件部署到各种计算服务，例如 Amazon EC2、AWS Fargate、AWS Lambda、和您的本地服务器。AWS CodeDeploy 帮助您快速发布新功能，帮助您避免应用程序部署期间的停机，并处理更新应用程序的复杂性。您可以使用 AWS CodeDeploy 自动化软件部署，无需进行容易出错的手动操作。该服务可根据您的部署需求进行扩展。要了解更多信息，请参阅[AWS CodeDeploy](#)。

Note

要加载 CodeCommit、CodeBuild、CodeDeploy、和 CodePipeline 使用单个 RFC，请提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型并请求三项服务：和。CodeBuild、CodeDeploy、CodePipeline。然后，所有三个角色、customer_codebuild_service_role、customer_codedeploy_service_role、和aws_code_pipeline_service_role都将在您的账户中配置。在您的账户中进行配置后，您必须在联合解决方案中加入该角色。

CodeDeploy 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 CodeDeploy 中申请访问权限？

CodeDeploy 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：customer_codedeploy_console_role和。customer_codedeploy_service_role在您的账户中配置该角色后，您必须在联合解决方案中加入该customer_codedeploy_console_role角色。

问：CodeDeploy 在我的 AMS 账户中使用有什么限制？

目前，我们仅支持计算平台 — Amazon EC2 /on-Premises。Blue/Green 不支持部署。

问：在我的 AMS 账户 CodeDeploy 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 CodeDeploy 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS CodePipeline 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS CodePipeline 功能。AWS CodePipeline 是一项完全托管的[持续交付](#)服务，可帮助您实现发布管道的自动化，从而实现快速可靠的应用程序和基础架构更新。CodePipeline 每次发生代码更改时，都会根据您的发布模型自动执行发布过程的构建、测试和部署阶段。这让您可以快速而可靠地交付各种功能和更新。您可以轻松地 AWS CodePipeline 与第三方服务集成，例如 GitHub 或与您自己的自定义插件集成。使用 AWS CodePipeline，您只需为实际用量付费。无前期费用，无长期承诺。要了解更多信息，请参阅[AWS CodePipeline](#)。

Note

要加载 CodeCommit、CodeBuild CodeDeploy、和 CodePipeline 使用单个 RFC，请提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型并请求三项服务：和。CodeBuild CodeDeploy CodePipeline然后，所有三个角色、customer_codebuild_service_rolecustomer_codedeploy_service_role、和aws_code_pipeline_service_role都将在您的账户中配置。在您的账户中进行配置后，您必须在联合解决方案中加入该角色。

CodePipeline 在 AMS 中，不支持源阶段的“Amazon Ev CloudWatch ents”，因为它需要更高的权限才能创建服务角色和策略，从而绕过最低权限模型和 AMS 变更管理流程。

CodePipeline 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 CodePipeline 中申请访问权限？

CodePipeline 通过在相关账户customer_code_pipeline_console_role中提交服务请求来请求访问权限。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

此时，AMS Operations 还将在您的账户中部署此服务角

色：aws_code_pipeline_service_role_policy。

问：CodePipeline 在我的 AMS 账户中使用有什么限制？

是的。CodePipeline 功能、阶段和提供者仅限于以下内容：

1. 部署阶段：仅限于 Amazon S3，以及 AWS CodeDeploy
2. 来源阶段：仅限于 Amazon S3 AWS CodeCommit、BitBucket、和 GitHub
3. 建造阶段：仅限于 AWS CodeBuild，而且 Jenkins

4. 批准阶段：仅限于亚马逊 SNS
5. 测试阶段：仅限于 Jenkins AWS CodeBuild、Ghost Inspector 用户界面测试、Micro Focus StormRunner 加载和 Runscope API 监控 BlazeMeter
6. 调用阶段：仅限于 Step Functions 和 Lambda

Note

AMS 操作将在您的账户 `customer_code_pipeline_lambda_policy` 中部署；它必须与 Lambda 调用阶段的 Lambda 执行角色相关联。请提供您想要添加此策略的 Lambda service/execution 角色名称。如果没有自定义 Lambda service/execution 角色，AMS 将创建一个名为的新角色 `customer_code_pipeline_lambda_execution_role`，该角色将作为副 `customer_lambda_basic_execution_role` 本。 `customer_code_pipeline_lambda_policy`

问：在我的 AMS 账户 CodePipeline 中使用的先决条件或依赖条件是什么？

AWS 支持的服务 AWS CodeCommit AWS CodeDeploy 必须在发布之前或同时启动 CodePipeline。
AWS CodeBuild

使用 AMS SSP AWS Compute Optimizer 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Compute Optimizer 功能。AWS Compute Optimizer 使用机器学习来分析历史利用率指标，为您的工作负载推荐最佳 AWS 计算资源，从而降低成本并提高性能。过度配置计算 (Amazon EC2 和 ASGs) 可能会导致不必要的基础设施成本，而计算配置不足会导致应用程序性能不佳。Compute Optimizer 可帮助您根据使用率数据选择最佳的亚马逊 EC2 实例类型，包括属于 Amazon A EC2 uto Scaling 组的实例类型。要了解更多信息，请参阅[AWS Compute Optimizer](#)。

AWS 托管服务中的 Compute Optimizer 常见问题解答

问：如何使用我的 AMS 账户申请访问 Compute Optimizer？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色: `customer_compute_optimizer_readonly_role`。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Compute Optimizer 有哪些限制？

没有任何限制。的全部功能可在您 AWS Compute Optimizer 的 AMS 账户中使用。

问：在我的 AMS 账户中使用 Compute Optimizer 有哪些先决条件或依赖关系？

- 您必须提交 RFC (管理 | 其他 | 其他 | 更新)，授权 AMS Ops 在账户中启用该服务。在部署期间，将创建一个服务关联角色 (SLR)，以允许收集指标和生成报告。单反相机标有“AWSServiceRoleForComputeOptimizer”。有关更多信息，请参阅[使用服务相关角色 AWS Compute Optimizer](#)
- CloudWatch 必须为以下指标启用指标：
 - CPU 利用率：实例上正在使用的已分配的 Amazon EC2 计算单元的百分比。该指标确定了在选定实例上运行应用程序所需的处理能力。
 - 内存利用率：在采样期间以某种方式使用的内存量。该指标用于确定在选定实例上运行应用程序所需的内存。仅针对安装了统一 CloudWatch 代理的资源分析内存利用率。有关更多信息，请参阅使用 CloudWatch 代理启用内存利用率 (第 10 页)。
 - 网络输入：实例在所有网络接口上接收的字节数。该指标用于识别单个实例的传入网络流量。
 - 网络输出：实例在所有网络接口上发送的字节数。该指标用于识别来自单个实例的传出网络流量。
 - 本地磁盘 input/output (I/O)：本地磁盘的 input/output 操作次数。该指标用于识别实例根卷的性能

使用 AMS SSP AWS DataSync 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS DataSync 功能。AWS DataSync 在本地存储和亚马逊 S3、Amazon Elastic File System (亚马逊弹性文件系统) 或亚马逊之间在线移动大量数据 FSx。与数据传输相关的手动任务可能会减慢迁移速度并给 IT 运营带来负担。DataSync 消除或自动处理其中的许多任务，包括编写拷贝作业脚本、安排和监控传输、验证数据以及优化网络利用率。DataSync 软件代理连接到您的网络文件系统 (NFS) 和服务器消息块 (SMB) 存储，因此您无需修改应用程序。DataSync 可以通过 Internet 或 AWS Direct Connect 链接传输数百 TB 和数百万个文件，速度比开源工具快 10 倍。您可以使用将活动数据集或存档迁移 DataSync 到云端 AWS，将数据传输到云端以便及时进行分析和处理，或者将数据复制到云端以 AWS 实现业务连续性。

要了解更多信息，请参阅[AWS DataSync](#)。

DataSync 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 DataSync 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_datasync_console_role.

在您的账户中配置后，您必须在联合解决方案中加入角色。

用于流式传输任务 CloudWatch 日志的日志组是“/aws/datasync”。

问：DataSync 在我的 AMS 账户中使用有什么限制？

的全部功能可在您 AWS DataSync 的 AMS 账户中使用。

问：在我的 AMS 账户 DataSync 中使用的先决条件或依赖条件是什么？

- 与将使用 DataSync 服务角色 `customer_datasync_service_role` 执行的 DataSync 任务关联的所有 S3 存储桶都需要 Amazon S3 ARNs（Amazon 资源名称）。
- 在使用 VPC 终端节点之前，必须使用管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型的 RFC 请求 DataSync 代理的 VPC 终端节点和安全组。
- AWS DataSync 代理作为设备在 AMS 中运行。该服务已对 AWS DataSync 代理进行修补和更新；有关详细信息，请参阅[AWS DataSync 常见问题解答](#)。
- 要启动 AWS DataSync 代理，请提交带有管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型的 RFC，请求部署代理。提供 AWS DataSync Amazon EC2 AMI ID、实例类型、子网、安全组；并引用现有的 Amazon EC2 密钥对或请求创建新的密钥对。

Note

AMS 代表客户手动配置 AWS DataSync 代理，并且不需要在 Amazon AWS DataSync AMI 上进行 WIGS 摄取流程。EC2

使用 AMS SSP AWS Device Farm 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Device Farm 功能。AWS Device Farm 是一项应用程序测试服务，可让您通过在各种桌面浏览器和真实移动设备上测试 Web 和移动应用程序来提高其质量，而无需预置和管理任何测试基础架构。该服务使您能够在多个桌面浏览器或真实设备上同时运行测试，以加快测试套件的执行速度，并生成视频和日志以帮助快速识别应用程序存在的问题。

要了解更多信息，请参阅[AWS Device Farm](#)。

AWS Device Farm 在 AWS Managed Services 常见问题中

问：如何申请访问我 AWS Device Farm 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_devicefarm_role.

在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问：AWS Device Farm 在我的 AMS 账户中使用有什么限制？

除了在“名称”标签中使用 AMS 命名空间外，还提供对该 AWS Device Farm 服务的完全访问权限。

问：在我的 AMS 账户 AWS Device Farm 中使用的先决条件或依赖条件是什么？

无。

使用 AMS SSP AWS Elastic Disaster Recovery 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elastic Disaster Recovery 功能。AWS Elastic Disaster Recovery 使用经济实惠的存储、最少的计算和恢复，快速、可靠地 point-in-time 恢复本地和基于云的应用程序，最大限度地减少停机时间和数据丢失。当您使用 AWS Elastic Disaster Recovery 复制在支持的操作系统上运行的本地应用程序或基于云的应用程序时，可以提高 IT 弹性。使用 AWS 管理控制台 来配置复制和启动设置、监控数据复制以及启动用于演练或恢复的实例。

要了解更多信息，请参阅[AWS Elastic Disaster Recovery](#)。

AWS Elastic Disaster Recovery 在 AWS Managed Services 常见问题中

问：如何申请访问我 AWS Elastic Disaster Recovery 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_drs_console_role.

在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：AWS Elastic Disaster Recovery 在我的 AMS 账户中使用有什么限制？

在您的 AMS 账户 AWS Elastic Disaster Recovery 中使用没有任何限制。

问：在我的 AMS 账户 AWS Elastic Disaster Recovery 中使用的先决条件或依赖条件是什么？

- 访问控制台角色后，您必须初始化 Elastic 灾难恢复服务，以便在账户中创建所需的 IAM 角色。

- 您必须提交更改类型管理 | 应用程序 | IAM 实例配置文件 | 创建 (需要审查) 更改类型 `ct-0ixp4ch2tiu04` RFC 才能创建实例配置文件的克隆并附加策略。 `customer-mc-ec2-instance-profile AWSElasticDisasterRecoveryEc2InstancePolicy` 您必须指定要将新策略附加到哪些计算机。
- 如果实例未使用默认实例配置文件，则 AMS `AWSElasticDisasterRecoveryEc2InstancePolicy` 可以通过自动化进行连接。
- 您必须使用客户拥有的 KMS 密钥进行跨账户恢复。必须按照策略更新源账户的 KMS 密钥以允许目标账户访问。有关更多信息，请参阅[与目标账户共享 EBS 加密密钥](#)。
- 如果您不想切换角色进行查看，则必须更新 KMS 密钥策略以允许 `customer_drs_console_role` 查看策略。
- 对于跨账户、跨区域灾难恢复，AMS 必须将源账户和目标账户设置为可信账户，并通过部署[故障恢复和大小合适的角色AWS](#)。 CloudFormation

使用 AMS SSP AWS Elemental MediaConvert 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaConvert 功能。AWS Elemental MediaConvert 是一种基于文件的视频转码服务，具有广播级功能。它使您能够创建 video-on-demand (VOD) 内容，用于大规模广播和多屏传送。该服务将高级视频和音频功能与简单的 Web 服务界面和 pay-as-you-go 定价相结合。借 AWS Elemental MediaConvert 助，您可以专注于提供引人入胜的媒体体验，而不必担心构建和运营自己的视频处理基础设施的复杂性。

要了解更多信息，请参阅[AWS Elemental MediaConvert](#)。

MediaConvert 在 AWS Managed Services 常见问题中

问：如何申请访问我 MediaConvert 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色: `customer_mediaconvert_author_role`. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

将提供第二个角色 `customer_MediaConvert_Default_Role`，该角色用于从源 S3 存储桶读取数据并将输出写入目标 S3 存储桶，还用于在需要数字版权管理 (DRM) 时调用 API 网关。MediaConvert

问：MediaConvert 在我的 AMS 账户中使用有什么限制？

在 AMS MediaConvert 中使用没有任何限制。

问：在我的 AMS 账户 MediaConvert 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaConvert 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Elemental MediaLive 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaLive 功能。AWS Elemental MediaLive 是一项广播级的直播视频处理服务。它使您能够创建高质量的视频流，以传送到广播电视和联网的多屏设备，例如联网设备、平板电脑 TVs、智能手机和机顶盒。该服务的工作原理是对您的直播视频流进行实时编码，获取较大的实时视频源，然后将其压缩成较小的版本以分发给您的观众。借助高级广播功能 AWS Elemental MediaLive、高可用性和定价，您可以轻松地直播活动和全天候频道设置直播。pay-as-you-go AWS Elemental MediaLive 让您专注于为观众创造引人入胜的实时视频体验，而无需复杂地构建和运营广播级视频处理基础架构。

要了解更多信息，请参阅[AWS Elemental MediaLive](#)。

MediaLive 在 AWS Managed Services 常见问题中

问：如何申请访问我 MediaLive 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_medialive_author_role。

作为本 RFC 的一部分，第二个角色将部署到您的账户；

该customer_medialive_service_role角色可以分配给您的媒体直播频道和输入，以便与其他服务 (例如 Amazon S3 和 CloudWatch 日志) 进行交互。MediaStore

在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问：MediaLive 在我的 AMS 账户中使用有什么限制？

在 AMS MediaLive 中使用没有任何限制。

问：在我的 AMS 账户 MediaLive 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaLive 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Elemental MediaPackage 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaPackage 功能。AWS Elemental MediaPackage 可靠地准备和保护您的视频，以便通过互联网传输。通过单个

视频输入，AWS Elemental MediaPackage 创建格式化为可在联网手机 TVs、计算机、平板电脑和游戏机上播放的视频流。它可以轻松地让观众实现流行的视频功能（重播、暂停、倒带等），就像上面常见的功能一样。DVRs AWS Elemental MediaPackage 还可以使用数字版权管理 (DRM) 保护您的内容。AWS Elemental MediaPackage 根据加载量自动缩放，因此您的观众将始终获得出色的体验，而不必事先准确预测所需的容量。

要了解更多信息，请参阅[AWS Elemental MediaPackage](#)。

MediaPackage 在 AWS Managed Services 常见问题中

问：如何在 AMS 账户 AWS Elemental MediaPackage 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_mediapackage_author_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

将提供第二个角色customer_mediapackage_service_role，可以将其分配给您的媒体直播频道和输入，以便与其他服务（例如 S3 和 Secrets Manager）进行交互。

问：MediaPackage 在我的 AMS 账户中使用有什么限制？

在 AMS MediaPackage 中使用没有任何限制。

问：在我的 AMS 账户 MediaPackage 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaPackage 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Elemental MediaStore 在您的 AMS 账户中进行配置

Note

经过仔细考虑，决定停产 MediaStore，AWS 自2025年11月13日起生效。如果您是活跃客户 MediaStore，则可以照常使用 MediaStore，直到 2025 年 11 月 13 日该服务的支持将终止。在此日期之后，您将无法再使用本服务提供的 MediaStore 任何功能。

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaStore 功能。AWS Elemental MediaStore 是一项针对媒体进行了优化的 AWS 存储服务。它为您提供交付直播视频内容所需的性能、一致性和低延迟。AWS Elemental MediaStore 在您的视频工作流程中充当原始

存储。其高性能功能可满足最苛刻的媒体交付工作负载的需求，再加上长期且经济实惠的存储。要了解更多信息，请参阅[AWS Elemental MediaStore](#)。

MediaStore 在 AWS Managed Services 常见问题中

问：如何申请访问我 MediaStore 的 AMS 账户？

MediaStore 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_mediastore_author_role. 作为本 RFC 的一部分，将在您的账户中部署第二个角色：MediaStoreAccessLogs角色，如果您选择启用该功能 CloudWatch，则 MediaStore 服务使用该角色来登录活动。在您的账户中配置角色后，您必须在联合解决方案中加入角色。

此时，AMS 运营部门还将在您的账户中部署此服务角色：aws_code_pipeline_service_role_policy。

问：MediaStore 在我的 AMS 账户中使用有什么限制？

在 AMS MediaStore 中使用没有任何限制。

问：在我的 AMS 账户 MediaStore 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaStore 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Elemental MediaTailor 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Elemental MediaTailor 功能。AWS Elemental MediaTailor 允许视频提供商在不牺牲广播 quality-of-service级别的情况下将单独定向的广告插入到其视频流中。这样 AWS Elemental MediaTailor，您的直播或点播视频的观众都会收到一个将您的内容与针对他们的个性化广告相结合的直播。但是，与其他个性化广告解决方案不同，AWS Elemental MediaTailor 您的整个视频流（视频和广告）都以广播级的视频质量投放，以改善观众的体验。AWS Elemental MediaTailor 提供基于客户端和服务端广告投放指标的自动报告，以准确衡量广告展示次数和观众行为。您可以轻松地通过意想不到的高需求观看活动获利，而无需支付任何前期费用。AWS Elemental MediaTailor它还可以提高广告投放率，帮助您从每个视频中获得更多收益，并且可以与更多种类的内容交付网络、广告决策服务器和客户端设备配合使用。

要了解更多信息，请参阅[AWS Elemental MediaTailor](#)。

MediaTailor 在 AWS Managed Services 常见问题中

问：如何申请访问我 MediaTailor 的 AMS 账户？

MediaTailor 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer-mediatailor-role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：MediaTailor 在我的 AMS 账户中使用有什么限制？

在 AMS MediaTailor 中使用没有任何限制。

问：在我的 AMS 账户 MediaTailor 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 MediaTailor 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Global Accelerator 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问全球加速器功能。Global Accelerator 是一项网络层服务，您可以在其中创建加速器以提高全球受众使用的互联网应用程序的可用性和性能。要了解更多信息，请参阅[全球加速器](#)。

AWS Managed Services 中的全球加速器常见问题解答

常见问题和答案：

问：如何申请在我的 AMS 账户中设置全球加速器？

通过提交 AWS 服务 RFC (管理 | 服务 | 自配 AWS 服务) 来请求访问权限。通过此 RFC，将在您的账户中配置以下 IAM 角色：。customer_global_accelerator_console_role在您的账户中配置控制台角色后，您必须在联合解决方案中加入控制台角色。

问：在我的 AMS 账户中使用全球加速器有哪些限制？

Global Accelerator 是一项全球服务，支持 AWS 区域[表中列出的多个AWS 区域](#)的终端节点。

问：在我的 AMS 账户中使用全球加速器的先决条件或依赖条件是什么？

使用全球加速器设置加速器时，可以将静态 IP 地址关联到一个或多个 AWS 区域的区域终端节点。对于标准加速器，终端节点是网络负载均衡器、应用程序负载均衡器、Amazon EC2 实例或弹性 IP 地址。对于自定义路由加速器，终端节点是具有一个或多个 EC2 实例的虚拟私有云 (VPC) 子网。

使用 AMS SSP AWS Glue 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Glue 功能。AWS Glue 是一项完全托管的提取、转换和加载 (ETL) 服务，可帮助您准备和加载数据以进行分析。只需在中单

击几下即可创建和运行 ETL 作业。AWS 管理控制台您指 AWS Glue 向存储在上的数据 AWS，AWS Glue 发现您的数据并将关联的元数据（例如表定义和架构）存储在中 AWS Glue Data Catalog。对您的数据进行编目后，即可立即搜索和查询，并可用于 ETL 操作。要了解更多信息，请参阅[AWS Glue](#)。

AWS Glue 在 AWS Managed Services 常见问题中

常见问题和答案：

问：AWS Glue 如何申请在我的 AMS 账户中进行设置？

AWS Glue 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：

- `customer_glue_console_role`
- `customer_glue_service_role`

前面的角色包括以下附加策略：

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

在您的账户中配置角色后，您必须将其加入您的联合解决方案中。

要访问爬虫、作业和开发终端节点（特定用例所需的角色），请使用部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建实体或策略 (ct-3dpd8mdd9jn1r) 提交 RFC。

问：AWS Glue 在我的 AMS 账户中使用有什么限制？

没有任何限制。的全部功能可在您 AWS Glue 的 AMS 账户中使用。要获得可以创作和测试 ETL 脚本的交互式环境，请使用 AWS Glue Studio 上的笔记本。AWS Glue Interactive Sessions 和 Job Notebook 是无服务器功能，您可以在中 AWS Glue 使用这些功能，也可以利用 AWS Glue 服务角色。
AWS Glue

AWS Glue 2.0 之前版本：AWS Glue 笔记本是一种非托管资源，可在账户中启动 Amazon EC2 实例。最佳做法是启动您自己的 Amazon EC2 实例并安装支持笔记本环境和开发所需的软件。有关更多信息，请参阅[教程：设置本地 Apache Zeppelin 笔记本来测试和调试 ETL 脚本以及使用开发端点开发脚本](#)。

问：在我的 AMS 账户 AWS Glue 中使用的先决条件或依赖条件是什么？

AWS Glue 依赖于 Amazon S3 CloudWatch、和 CloudWatch 日志。传递依赖关系因数据源和可能与之交互的其他 AWS Glue 服务功能而异（例如：Amazon Redshift、Amazon RDS、Athena）。

使用 AMS SSP AWS Lake Formation 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Lake Formation 功能。AWS Lake Formation 是一项服务，可让您在几天之内轻松设置安全的数据湖。数据湖是一种集中的、策管的、安全存储库，用于存储所有数据，包括原始形式和准备进行分析的形式。数据湖能够打破数据孤岛，将不同类型的分析结合起来，获得信息并指导更好的业务决策。

使用 Lake Formation 创建数据湖很简单，以及要应用的数据访问和安全策略。然后，Lake Formation 可帮助您从数据库和对象存储收集和编目数据，将数据移动到新的 Amazon S3 数据湖，使用机器学习算法清理和分类数据，安全访问敏感数据。您的用户可以访问集中式数据目录（有关详细信息，请参阅[AWS Glue 常见问题解答](#)），该目录描述了可用数据集及其适当用法。然后，您的用户将这些数据集与他们选择的分析和机器学习服务结合起来，例如[亚马逊 Redshift](#)、[Amazon Athena](#) 和（测试版）[适用于 Apache Spark 的 Amazon EMR](#)。Lake Formation 建立在中提供的功能之上[AWS Glue](#)。

要了解更多信息，请参阅[AWS Lake Formation](#)。

AWS 托管服务中的 Lake Formation 常见问题解答

问：如何申请访问我 AWS Lake Formation 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_lakeformation_data_analyst_role. 在您的账户中配置角色后，您必须在联合解决方案中加入角色。

此外，以下两个角色是可选的：

- customer_lakeformation_admin_role
- customer_lakeformation_workflow_role

要获得管理员权限，您可以选择将该角色customer_lakeformation_admin_role作为相同 SSP 更改类型（ct-3qe6io8t6jtny）的一部分加入。

如果要在 AWS Lake Formation 控制台中创建蓝图，则需要提交管理 | 其他 | 其他 RFC (ct-1e1xtak34nx76) 来部署。customer_lakeformation_workflow_role在 RFC 中，如果创建蓝图时存储桶是源，则必须提供 S3 存储桶名称。如果蓝图类型为 AWS CloudTrail Classic Load Balancer 日志或应用程序负载均衡器日志，则 S3 存储桶适用。

问：AWS Lake Formation 在我的 AMS 账户中使用有什么限制？

Lake Formation 的全部功能已在 AMS 中提供。

问：在我的 AMS 账户 AWS Lake Formation 中使用的先决条件或依赖条件是什么？

Lake Formation 与该 AWS Glue 服务集成，因此 AWS Glue 用户只能访问他们拥有 Lake Formation 权限的数据库和表。此外，AWS Athena 和 Amazon Redshift 用户只能查询他们拥有 Lake Formation 权限 AWS Glue 的数据库和表。

使用 AMS SSP AWS Lambda 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Lambda 功能。AWS Lambda 允许您在不预置或管理服务器的情况下运行代码。您只需为所消耗的计算时间付费，当您的代码未运行时不收取任何费用。借助 Lambda，您几乎可以为任何类型的应用程序或后端服务运行代码，所有这些都无需任何管理。上传您的代码，Lambda 会处理运行和扩展代码所需的一切，使其具有高可用性。您可以将代码设置为从其他 AWS 服务自动触发，或者直接从任何 Web 或移动应用程序调用。要了解更多信息，请参阅[AWS Lambda](#)。

AWS Managed Services 中的 Lambda 常见问题解答

问：如何在 AMS 账户 AWS Lambda 中申请访问权限？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角

色：customer_lambda_admin_role和。customer_lambda_basic_execution_role在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问：AWS Lambda 在我的 AMS 账户中使用有什么限制？

- Lambda 函数旨在由事件源调用。有关可用作 Lambda 事件源的服务列表，请参阅[与其他服务 AWS Lambda 一起使用](#)。目前，并非所有这些服务都在 AMS 账户中可用。如果您需要的服务不可用，请与您的 AMS CSDM 合作提交例外申请。
- 默认情况下，AMS 为您提供包
含AWSLambdaBasicExecutionRole和AWSXrayWriteOnlyAccess权限的基本 Lambda 初始角色；有关信息，请参阅[AWS Lambda 初始](#)角色。如果您需要其他权限，例如能够在您的 AMS VPC 中配置 Lambda 函数，请使用管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) (ct-3qe6io8t6jtny) 更改类型提交 RFC。

问：在我的 AMS 账户 AWS Lambda 中使用的先决条件或依赖条件是什么？

开始时没有先决条件或依赖关系 AWS Lambda；但是，根据您的具体用例，您可能需要访问其他 AWS 服务才能创建事件源，或者您的函数需要额外的权限才能执行各种操作。如果需要其他权限，请使用管理 | AWS 服务 | 自配置服务 | 添加 (需要审核) 更改类型 (ct-3qe6io8t6jtny) 提交 RFC。

问：要在我的任何账户中运行 Lambda 函数，我需要做什么？

要在核心账户中部署 Lambda 函数，请使用以下指南：

- 确保已加载 SSP f AWS Lambda or。
- 只要您的 AMS 资源受到保护且合规，AMS 职责下没有禁止这种部署的具体限制。
- 如果您希望 AMS 创建 Lambda 函数，则必须首先使用所提供的 SSP 角色。AWS Lambda 然后，如果您仍希望 AMS 协助部署或支持该功能，请联系您的 CA 并启动超出范围 (OOS) 流程。

使用 AMS SSP AWS License Manager 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS License Manager 功能。AWS License Manager 与 AWS 服务集成，通过单 AWS 一账户简化多个 AWS 账户、IT 目录和本地许可证的管理。AWS License Manager 允许管理员创建模拟其许可协议条款的自定义许可规则，然后在 Amazon 实例启动时强制执行这些规则 EC2。中的规则 AWS License Manager 使您能够通过实际阻止实例启动或将违规行为通知管理员来限制许可违规行为。要了解更多信息，请参阅[AWS License Manager](#)。

AWS Managed Services 中的许可证管理器常见问题解答

常见问题和答案：

问：AWS License Manager 如何申请在我的 AMS 账户中进行设置？

AWS License Manager 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_license_manager_role。在您的账户中配置 License Manager IAM 角色后，您必须在联合身份验证解决方案中加入该角色。

问：AWS License Manager 在我的 AMS 账户中使用有什么限制？

您可以将规则与 AMIs 您自己的 AWS License Manager 规则相关联（在“我拥有”下筛选）。如果您选择强制与 AMI 建立限制关联（例如：只能支持此 AMI 的 100 个 vCPU）并耗尽限制，则未来使用该 AMI 的启动将被阻止，并返回一条错误消息，指出“没有可用许可证”。这是本服务的预期行为（不允许许可证耗尽）。如果您已用尽限制，但需要再次启动 AMI，则必须修改中配置的规则 AWS License Manager。

问：在我的 AMS 账户 AWS License Manager 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS License Manager 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Migration Hub 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Migration Hub 功能。AWS Migration Hub 提供了一个位置，您可以在其中跟踪跨多个解决方案 AWS 和合作伙伴解决方案的应用程序迁移进度。使用 Migration Hub，您可以选择最适合自己需求的迁移工具 AWS 和合作伙伴，同时可以查看整个应用程序组合的迁移状态。Migration Hub 还提供各个应用程序的关键指标和进度，无论使用何种工具进行迁移。这使您可以快速获取所有迁移的进度更新，轻松识别和解决任何问题，并减少在迁移项目上花费的总体时间和精力。要了解更多信息，请参阅[AWS Migration Hub](#)。

AWS Managed Services 中的迁移中心常见问题解答

常见问题和答案：

问：如何使用我的 AMS 账户申请访问 Migration Hub？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Migration Hub。此 RFC 为您的账户配置以下 IAM 角色:customer_migrationhub_author_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：Migration Hub 有哪些限制？

无。

问：启用 Migration Hub 的先决条件是什么？

在您的 AMS 账户中开始使用 Migration Hub 不需要任何先决条件。但是，在管理服务期间，可能需要在 Migration Hub 之外的权限，例如向 Amazon S3 写入上传服务器信息的权限。

使用 AMS SSP AWS Outposts 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Outposts 功能。AWS Outposts 是一项完全托管的服务，可将 AWS 基础架构 APIs、AWS 服务和工具扩展到几乎任何数据中心、托管空间或本地设施，以提供一致的混合体验。AWS Outposts 适用于需要低延迟访问本地系统、本地数据处理或本地数据存储的工作负载。要了解更多信息，请参阅[AWS Outposts](#)。

AWS Outposts 在 AWS Managed Services 常见问题中

常见问题和答案：

问：AWS Outposts 如何申请在我的 AMS 账户中进行设置？

AWS Outposts 通过使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_outposts_role. 在您的账户中配置该角色后，您必须将其加入您的联合解决方案中。

问：AWS Outposts 在我的 AMS 账户中使用有什么限制？

在您的 AMS 账户 AWS Outposts 中使用没有任何限制。

问：在我的 AMS 账户 AWS Outposts 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS Outposts 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Resilience Hub 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Resilience Hub 功能。AWS Resilience Hub 帮助您主动准备并保护 AWS 应用程序免受中断。Resilience Hub 提供弹性评估和验证，可集成到您的软件开发生命周期中，以发现弹性弱点。Resilience Hub 可帮助您估算您的应用程序能否满足恢复时间目标 (RTO) 和恢复点目标 (RPO) 目标，并在问题发布到生产环境之前帮助解决问题。将 AWS 应用程序部署到生产环境后，您可以使用 Resilience Hub 继续跟踪应用程序的弹性状况。如果发生中断，Resilience Hub 会向操作员发送通知，要求其启动相关的恢复流程。

AWS Resilience Hub 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何在 AMS 账户 AWS Resilience Hub 中申请访问权限？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问弹性中心。此 RFC 为您的账户配置以下 IAM 角色和策略：

IAM 角色

- customer_resiliencehub_console_role
- customer_resiliencehub_service_role

策略

- customer_resiliencehub_console_policy
- customer_resiliencehub_service_policy

在您的账户中配置该角色后，您必须在联合解决方案 `customer_resiliencehub_console_role` 中加入该角色。

问：AWS Resilience Hub 在我的 AMS 账户中使用有什么限制？

没有任何限制。Resilience Hub 的全部功能可在您的 AMS 账户中使用。

问：在我的 AMS 账户 AWS Resilience Hub 中使用的先决条件或依赖条件是什么？

在您的 AMS 账户中使用 Resilience Hub 没有任何先决条件或依赖关系。

使用 AMS SSP AWS Secrets Manager 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Secrets Manager 功能。AWS Secrets Manager 帮助您保护访问应用程序、服务和 IT 资源所需的机密。该服务使您能够在数据库凭证、API 密钥和其他密钥的整个生命周期中轻松轮换、管理和检索它们。用户和应用程序通过调用 Secrets Manager 来检索机密 APIs，无需以纯文本格式对敏感信息进行硬编码。Secrets Manager 使用 Amazon RDS、Amazon Redshift 和 Amazon DocumentDB 的内置集成提供密钥轮换。此外，该服务还可扩展到其他类型的机密，包括 API 密钥和 OAuth 令牌。要了解更多信息，请参阅[AWS Secrets Manager](#)。

Note

默认情况下，AMS 操作员可以访问使用账户默认密 AWS KMS 钥 (CMK) 加密的机密。AWS Secrets Manager 如果您希望 AMS Operations 无法访问您的机密，请使用自定义 CMK，其中包含一个 AWS Key Management Service (AWS KMS) 密钥策略，该策略定义了与存储在密钥中的数据相应的权限。

AWS 托管服务中的 Secrets Manager 常见问题解答

问：如何申请访问我 AWS Secrets Manager 的 AMS 账户？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-3qe6io8t6jtny) 更改类型提交 RFC，请求访问 Secrets Manager。此 RFC 为您的账户配置以下 IAM 角色：`customer_secrets_manager_console_role`和。`customer-rotate-secrets-lambda-role`用作管理员角色来配置和管理密钥，并用作轮换密钥。`customer-rotate-secrets-lambda-role`的 Lambda 函数的 Lambda 执行角色。`customer_secrets_manager_console_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该 `customer_secrets_manager_console_role` 角色。

问：AWS Secrets Manager 在我的 AMS 账户中使用有什么限制？

的全部功能均可在您的 AWS Secrets Manager 的 AMS 账户中使用，同时还提供自动轮换密钥的功能。但是，请注意，不支持使用“创建新的 Lambda 函数来执行轮换”来设置轮换，因为它需要更高的权限才能创建 CloudFormation 堆栈（IAM 角色和 Lambda 函数创建），从而绕过变更管理流程。AMS Advanced 仅支持“使用现有 Lambda 函数执行轮换”，在这种模式下，您可以使用 Lambda SSP 管理员角色管理您的 Lambda 函数以轮换密钥。AWS AMS Advanced 不会创建或管理 Lambda 来轮换密钥。

问：在我的 AMS 账户 AWS Secrets Manager 中使用的先决条件或依赖条件是什么？

以下命名空间保留给 AMS 使用，不能作为直接访问的一部分使用：AWS Secrets Manager

- arn: aws: secretsmanager: *: *: secret: ams-shared/*
- arn: aws: secretsmanager: *: *: secret: customershared/*
- arn: aws: secretsmanager: *: *: secret: ams/*

使用 Secrets Manager (AMS SSP) 共享密钥

以 RFC、服务请求或事件报告的纯文本形式与 AMS 共享机密会导致信息泄露事件，AMS 会从案例中删除这些信息，并要求您重新生成密钥。

您可以在这个命名空间下使用 [AWS Secrets Manager](#)(Secrets Manager) customer-shared。

使用 Secrets Manager 共享密钥常见问题解答

问：必须使用 Secrets Manager 共享哪种类型的机密？

一些示例包括用于创建 VPN 的预共享密钥、身份验证密钥（IAM、SSH）、许可证密钥和密码等机密密钥。

问：如何使用 Secrets Manager 与 AMS 共享密钥？

1. 使用您的联合访问权限和相应的角色登录 AWS 管理控制台：

对于 SALZ 来说，Customer_ReadOnly_Role

对于 MALZ 来说，AWSManagedServicesChangeManagementRole。

2. 导航到[AWS Secrets Manager 控制台](#)，然后单击“存储新密钥”。
3. 选择其他密钥类型。

4. 以纯文本形式输入密钥值并使用默认 KMS 加密。单击下一步。
5. 输入密钥名称和描述，名称始终以 customers hared/开头。例如，客户共享 /mykey2022。单击下一步。
6. 禁用自动轮换，单击“下一步”。
7. 查看并单击“存储”以保存密钥。
8. 通过服务请求、RFC 或事件报告回复我们并提供机密名称，以便我们识别和检索机密。

问：使用 Secrets Manager 共享密钥需要什么权限？

SALZ：查找customer_secrets_manager_shared_policy托管 IAM 策略并验证策略文档是否与以下创建步骤中附加的策略文档相同。确认该策略已附加到以下 IAM 角色：Customer_ReadOnly_Role。

MALZ：验证AMSSecretsManagerSharedPolicy，是否已附加到允许您在ams-shared命名空间中GetSecretValue执行操作的AWSManagedServicesChangeManagementRole角色。

示例：

```
{
  "Action": "secretsmanager:*",
  "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  ],
  "Effect": "Allow",
  "Sid": "AllowAccessToSharedNameSpaces"
}
```

Note

当您添加为自助服务配置服务时 AWS Secrets Manager，将授予必要的权限。

使用 AMS SSP AWS Security Hub CSPM 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Security Hub CSPM 功能。AWS Security Hub CSPM 让您全面了解自己的安全状态以及您对安全行业标准 AWS 和最佳实践的遵守情况。Security Hub 集中处理来自 AWS 账户、服务和支持的第三方合作伙伴的安全和合规调查

结果并确定其优先级，以帮助您分析安全趋势并确定优先级最高的安全问题。要了解更多信息，请参阅[AWS Security Hub CSPM](#)。

AWS 托管服务中的 Security Hub 常见问题解答

问：如何申请访问我 AWS Security Hub CSPM 的 AMS 账户？

通过管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC 来申请 Security Hub 的访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_securityhub_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 Security Hub 有哪些限制？

存档功能已被视为潜在的安全和操作风险，并且作为自配置服务安全角色的一部分受到限制。

问：在我的 AMS 账户 AWS Security Hub CSPM 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS Security Hub CSPM 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Service Catalog AppRegistry 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AppRegistry 功能。AppRegistry 支持从中心位置进行应用程序搜索、报告和管理操作。构建者很少在单个 AWS 账户中创建应用程序。它们通常按生命周期阶段（例如开发、测试和生产）来分隔应用程序资源。AppRegistry 允许您对您定义的 AWS 账户中的所有资源集进行分组和查看。

使用 AppRegistry，您可以存储您的 AWS 应用程序、与您的应用程序关联的资源集合以及应用程序属性组。要了解更多信息，请参阅[什么是 AppRegistry](#)。

常见问题：AWS Service Catalog AppRegistry 在 AMS 中

问：如何申请访问我 AWS Service Catalog AppRegistry 的 AMS 账户？

AppRegistry 通过使用管理 | AWS 服务 | 自配置服务 | 添加（需要审核）(ct-3qe6io8t6jtny) 更改类型提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer-appregistry-console-role. 在您的账户中配置后，您必须在联合解决方案中加入该角色。

问：AWS Service Catalog AppRegistry 在我的 AMS 账户中使用有什么限制？

除了在 'Name' 标签中使用 AMS 命名空间外，还提供对该 AppRegistry 服务的完全访问权限。

问：在我的 AMS 账户 AWS Service Catalog AppRegistry 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AppRegistry 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Shield Advanced 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Shield Advanced 功能。AWS Shield Advanced 是一项托管的分布式拒绝服务 (DDoS) 保护服务，可保护正在运行的应用程序 AWS。Shield Advanced 提供不间断检测和自动内联缓解措施，可最大限度地减少应用程序停机时间和延迟，因此无需与 Su AWS pport 合作即可从 S 保护中受益。DDoS 有两个等级 AWS Shield —— 标准和高级；AMS 提供 Shield Advanced。要了解更多信息，请参阅 [Shield Advanced](#)。

所有 AWS 客户均可享受自动保护 AWS Shield Standard，无需支付额外费用。AWS Shield Standard 抵御针对您的网站或应用程序的最常见、最常发生的网络和传输层 DDoS 攻击。当您 AWS Shield Standard 与 Amazon CloudFront 和 Amazon Route 53 配合使用时，您将获得针对所有已知基础设施（第 3 层和第 4 层）攻击的全面可用性保护。

要获得更高级别的保护，抵御针对在亚马逊弹性计算云 (Amazon EC2)、Elastic Load Balancing (ELB) CloudFront AWS Global Accelerator、亚马逊和亚马逊 Route 53 资源上运行的应用程序的攻击，您可以订阅。AWS Shield Advanced

除了随 AWS Shield Standard 附的网络和传输层保护外，还 AWS Shield Advanced 提供了针对大型复杂的 DDoS 攻击的额外检测和缓解措施、近乎实时的攻击可见性以及与 AWS WAF Web 应用程序防火墙的集成。AWS Shield Advanced 还允许你全天候访问 AWS Shield 响应小组 (SRT)，并防止亚马逊弹性计算云 (亚马逊)、弹性负载均衡（弹性负载均衡 EC2）、亚马逊和亚马逊 CloudFront 亚马逊 Route 53 费用中与 DDoS 相关的峰值。AWS Global Accelerator

AWS Managed Services 常见问题解答中的 Shield Ad

问：如何在我的 AMS 账户中申请访问 Shield Advanced？

使用管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型提交 RFC，请求访问 Shield Advanced。此 RFC 为您的账户配置以下 IAM 角色：customer_shield_role 和。aws_drt_shield_role 在您的账户中配置角色后，您必须在联合解决方案中加入角色。

将角色部署到您的账户后，您可以使用在 customer_shield_role 您的账户 AWS Shield Advanced 中确认订阅。

Note

请注意，使用需要支付月费和一年的使用期限 AWS Shield Advanced。此外，AWS Shield Advanced 在 AMS 中使用会授权 AMS 升级到 AWS Shield (SRT)，后者可以在分布式拒绝服

务 (S AWS WAF) 事件升级期间更改您的 Web 应用程序防火墙 (DDoS) 规则。这些变更将与 AMS 协调进行。

问：在我的 AMS 账户中使用 Shield Advanced 有哪些限制？

尽管不是限制，但你应该明白，使用 Shield Advanced 会部署 `aws_drt_shield_role`，这允许 AWS Shield 队伍 (SRT) 在 S 事件升级 DDoS 期间对 AMS 账户内的 AWS WAF 规则进行紧急更改。AMS 建议这样做是为了最快地修复 DDoS 攻击，并且会在 AMS 升级到 SRT 之后发生。

问：在我的 AMS 账户中使用 Shield Advanced 有哪些先决条件或依赖关系？

在您的 AMS 账户中使用 Shield Advanced 没有任何先决条件或依赖关系。

使用 AMS SSP AWS Snowball Edge 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 Snowball Edge 功能。Snowball Edge 是一种 PB 级的数据传输解决方案，它使用专为安全设计的设备将大量数据传输到云端和从云端传出。AWS Snowball Edge 解决了大规模数据传输的常见挑战，包括高昂的网络成本、较长的传输时间和安全问题。您可以使用 Snowball Edge 迁移分析数据、基因组学数据、视频库、图像存储库、备份，并存档部分数据中心关闭、磁带更换或应用程序迁移项目。使用 Snowball Edge 传输数据既简单、快速、更安全，而且只需通过高速互联网传输数据的成本的五分之一。

使用 Snowball Edge，您无需编写任何代码或购买任何硬件即可传输数据。首先使用 AWS 管理控制台为 Snowball [创建导入任务](#)，Snowball 设备将自动发送给您。设备到达后，将设备连接到您的本地网络，下载并运行 Snowball Client (“客户端”) 以建立连接，然后使用客户端选择要传输到设备的文件目录。然后，客户端会加密文件并将其高速传输到设备。转移完成并准备退回设备后，电子墨水的运输标签会自动更新，您可以通过亚马逊简单通知服务 (Amazon SNS) Simple Notification Service、短信或直接在控制台中跟踪任务状态。要了解更多信息，请参阅 [AWS Snowball Edge](#)。

AWS Managed Services 常见问题中的 Snowball Edge

常见问题和答案：

问：如何申请访问我 AWS Snowball Edge 的 AMS 账户？

在 AMS 中实施 Snowball Edge 分为两个步骤：

1. 提交管理 | 其他 | 其他 | 创建 (ct-1e1xtak34nx76) 更改类型，然后为你的 AMS 账户申请 Snowball Edge 的服务角色。

2. 通过提交管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 来请求用户访问权限。此 RFC 为您的账户配置以下 IAM 角色：
色：`customer_snowball_console_role`、`customer_snowball_export_role`、
和。`customer_snowball_import_role`在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：AWS Snowball Edge 在我的 AMS 账户中使用有什么限制？

的全部功能可在您 AWS Snowball Edge 的 AMS 账户中使用。

问：在我的 AMS 账户 AWS Snowball Edge 中使用的先决条件或依赖条件是什么？

您必须拥有如上所述的服务角色帐户。

使用 AMS SSP AWS Step Functions 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Step Functions 功能。AWS Step Functions 是一项 Web 服务，使您能够使用可视化工作流程来协调分布式应用程序和微服务的组件。您可通过能执行离散函数（或称为任务）的各单独组件构建应用程序，这样您能够快速扩展和更改应用程序。Step Functions 提供了一种可靠的方法来协调组件并逐步执行应用程序的函数。Step Functions 提供了一个图形控制台，可将应用程序的组件可视化为一组步骤。它会自动触发和跟踪每个步骤，并在出现错误时重试，因此您的应用程序每次都能按预期按顺序运行。Step Functions 会记录每个步骤的状态，这样在出现错误时，您就能够迅速诊断并调试问题。要了解更多信息，请参阅[AWS Step Functions](#)。

AWS 托管服务常见问题解答中的 Step Functions

常见问题和答案：

问：如何在 AMS 账户 AWS Step Functions 中申请访问权限？

AWS Step Functions 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色：`customer_step_functions_role`。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：AWS Step Functions 在我的 AMS 账户中使用有什么限制？

的全部功能可在您 AWS Step Functions 的 AMS 账户中使用。

问：在我的 AMS 账户 AWS Step Functions 中使用的先决条件或依赖条件是什么？

在运行时，Step Functions 使用的角色必须有权访问步进函数所使用的服务。例如，步进函数可能依赖于 Lambda 函数。创作步骤函数的人很可能同时创建 Lambda 函数，并且还必须请求访问该服务。

使用 AMS SSP 在您的 AMS 账户中配置 AWS Systems Manager 参数存储

使用 AMS 自助配置 (SSP) 模式直接在您的 AMS 托管账户中访问 AWS Systems Manager 参数存储功能。AWS Systems Manager Parameter Store 为配置数据管理和密钥管理提供安全的分层存储。也可以将密码、数据库字符串和许可证代码等数据存储为参数值。可以将值存储为纯文本或加密数据。然后，可以使用创建参数时指定的唯一名称来引用对应值。Parameter Store 具有高度的可扩展性、可用性和耐用性，由 AWS 云端提供支持。要了解更多信息，请参阅[AWS Systems Manager 参数存储](#)。

Note

如果您想要一个具有生命周期管理功能的专用密钥存储库，请使用[使用 AMS SSP AWS Secrets Manager 在您的 AMS 账户中进行配置](#)而不是参数存储。Secrets Manager 允许您自动轮换密钥，从而帮助您满足安全和合规要求。Secrets Manager 在 Amazon RDS 上为 MySQL、PostgreSQL 和 Amazon Aurora 提供了内置集成，可通过自定义 Lambda 函数将其扩展到其他类型的机密。

AWS Systems Manager AWS Managed Services 中的参数存储常见问题

常见问题和答案：

问：如何在我的 AMS 账户中请求访问 Systems Manager 参数存储区？

通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请对 AWS Systems Manager 参数存储的访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_systemsmanager_parameterstore_console_role。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 P AWS Systems Manager Parameter Store 有哪些限制？

您需要使用 AWS 托管密钥；创建自定义 KMS 密钥的访问权限受到限制。但是，如果需要自定义密钥，请提交 RFC 以使用此 IAM 角色的部署 | 高级堆栈组件 | KMS 密钥 | 创建更改类型 (ct-1d84keiri1jhg) 作为和参数的值来创建客户管理的密钥 (CMK)。customer_systemsmanager_parameterstore_console_role
IAMPrincipalsRequiringDecryptPermissions
IAMPrincipalsRequiringEncryptPermissionsPrincipal创建 KMS 密钥后，您可以使用它创建安全字符串。

问：在我的 AMS 账户中使用 P AWS Systems Manager Parameter Store 有哪些先决条件或依赖关系？

没有先决条件；但是，SSM Parameter Store 依赖 KMS 来创建安全字符串，因此您可以加密和解密存储在参数存储中的值。

使用 AMS SSP 在您的 AMS AWS Systems Manager 账户中配置自动化

使用 AMS 自助服务配置 (SSP) 模式，直接在您的 AMS 托管账户中访问 AWS Systems Manager 自动化功能。AWS Systems Manager 自动化使用运行手册、操作和服务配额简化了 Amazon Elastic Compute Cloud 实例和其他 AWS 资源的常见维护和部署任务。它使您能够大规模构建、执行和监控自动化。Systems Manager Automation 是一种系统管理器文档，它定义了系统管理器对您的托管实例执行的操作。一本运行手册，用于执行常见的维护和部署任务，例如在托管实例中运行命令或自动化脚本。Systems Manager 包括一些功能，可帮助您使用亚马逊弹性计算云标签定位大量实例，以及帮助您根据定义的限制推出更改的速度控制。运行手册是使用 JavaScript 对象表示法 (JSON) 或 YAML 编写的。但是，通过使用 Systems Manager 自动化中的文档生成器，您可以创建运行手册，而无需使用本机 JSON 或 YAML 创作。或者，您可以使用 Systems Manager 提供的运行手册，其中包含适合您需求的预定义步骤。要了解更多信息，请参阅 AWS Systems Manager 文档中的[使用运行手册](#)。

Note

尽管 Systems Manager Automation 支持 20 种可在运行手册中使用的操作类型，但在创作要在 AMS 高级账户中使用的运行手册时，您可以使用的操作数量有限。同样，系统管理器提供的运行手册数量有限，既可以直接使用，也可以从自己的运行手册中使用。有关详细信息，请参阅以下常见问题解答中的限制。

AWS Systems Manager AWS Managed Services 中的自动化常见问题解答

常见问题和答案：

问：如何通过我的 AMS 账户申请访问 Systems Manager Automation？

通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请 AWS Systems Manager 自动化的访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_systemsmanager_automation_console_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：在我的 AMS 账户中使用 AWS Systems Manager 自动化有什么限制？

您需要编写运行手册，只有在托管实例中运行命令 and/or 脚本时，Systems Manager 支持的操作有限。下文概述了可供您执行的操作以及任何限制。

AWS Systems Manager 自动化限制

操作	说明	限制
aws : assertAwsResource财产 —	断言 AWS 资源状态或事件状态	仅限 EC2 实例
aw: aws: branch —	运行条件自动化步骤	没有限制
AWS: 创建标签 —	为 AWS 资源创建标签	仅适用于您撰写的 SSM 自动化运行手册
AWS: 执行自动化 —	运行另一个自动化	只有您撰写的自动化运行手册
aws: 执行脚本 —	运行脚本	唯一不对任何服务进行任何 API 调用的脚本
aws: 暂停 —	暂停自动化	没有限制
aws: runCommand	在托管实例上运行命令	仅使用系统管理器提供的文档 — AWS RunShellScript 和 AWS-RunPowerShellScript
aws: sleep —	延迟自动化	没有限制
aws: waitForAws ResourceP roperty —	等待 AWS 资源属性	仅限 EC2 实例

您也可以选择使用 Systems Manager 控制台中的“运行命令”功能直接RunPowerShellScript 使用 Systems Manager 提供的运行手册 AWS RunShellScript 和 AWS 运行手册运行命令或脚本。您还可以将这些运行手册嵌套在运行手册中，以满足额外的 and/or 后期验证或任何复杂的自动化逻辑。

该角色遵循最低权限原则，仅提供创作、执行和检索旨在在托管实例中执行命令 and/or 脚本的 runbook 的执行详细信息所需的权限。它不为 AWS Systems Manager 服务提供的任何其他功能提供权限。虽然该功能允许您编写自动化运行手册，但不能将运行手册的执行定向 AMS 拥有的资源。

问：在我的 AMS 账户中使用 AWS Systems Manager 自动化的先决条件或依赖条件是什么？

没有先决条件；但是，在编写运行手册时，必须确保 and/or 遵守内部流程合规性控制。我们还建议在根据生产资源执行运行手册之前，对其进行全面测试。

问：Systems Manager 策略 `customer_systemsmanager_automation_policy` 能否附加到其他 IAM 角色？

不可以，与其他启用自行配置的服务不同，此策略只能分配给已配置的默认角色。 `customer_systemsmanager_automation_console_role`

与其他 SSP 角色的策略不同，此 SSM SSP 策略不能与其他自定义 IAM 角色共享，因为此 AMS 服务仅用于在托管实例中运行命令或自动化脚本。如果允许将这些权限附加到其他自定义 IAM 角色（可能具有其他服务的权限），则允许的操作范围可能会扩展到托管服务，并可能降低您账户的安全状况。

要根据我们的 AMS 技术标准评估任何变更请求 (RFCs)，请与您各自的云架构师或服务交付经理合作，请参阅 [RFC 安全审查](#)。

Note

AWS Systems Manager 允许您使用与您的帐户共享的运行手册。我们建议您在使用共享运行手册时谨慎行事并进行尽职调查，并确保在执行运行手册之前查看内容以了解 `command/scripts` 其运行情况。有关详细信息，请参阅 [共享 SSM 文档的最佳实践](#)。

使用 AMS SSP AWS Transfer Family 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接在您的 AMS 托管账户中访问 AWS Transfer Family (Transfer Family) 功能。AWS Transfer Family 是一项完全托管的 AWS 服务，允许您通过安全文件传输协议 (SFTP) 将文件传输到亚马逊简单存储服务 (Amazon S3) Simple S3 Service 存储和传出亚马逊简单存储服务 (Amazon S3) 存储。SFTP 也称为安全外壳 (SSH) 文件传输协议。SFTP 用于不同行业的数据交换工作流程，例如金融服务、医疗保健、广告和零售等。

使用 AWS SFTP，您 AWS 无需运行任何服务器基础架构即可访问 SFTP 服务器。您可以使用此服务将基于 SFTP 的工作流程迁移到，AWS 同时保持最终用户的客户端和配置不变。首先将您的主机名与 SFTP 服务器端点相关联，然后添加您的用户并为其配置适当的访问级别。完成后，将直接从您的 AWS SFTP 服务器端点处理用户的传输请求。要了解更多信息 [AWS Transfer for SFTP](#)，另请参阅 [创建支持 SFTP 的服务器](#)。

AWS Transfer for SFTP 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何申请访问我 AWS Transfer for SFTP 的 AMS 账户？

AWS Transfer for SFTP 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。通过此 RFC，将在您的账户中配置以下 IAM 角色和策略：

- `customer_transfer_author_role`。此角色旨在让您通过控制台管理 SFTP 服务。
- `customer_transfer_sftp_server_logging_role`。此角色旨在附加到 SFTP 服务器上。它允许 SFTP 服务器提取日志。CloudWatch
- `customer_transfer_sftp_user_role`。此角色旨在附加到 SFTP 用户身上。它允许 SFTP 用户与 S3 存储桶进行交互。
- `policy_customer_transfer_scope_down_policy`。此策略是一项范围缩小策略，可应用于 SFTP 用户，将他们对 S3 存储桶的访问权限限制为其主文件夹。
- `customer_transfer_sftp_efs_user_role`。此角色旨在附加到 SFTP 用户身上。它允许 SFTP 用户与 EFS 文件系统进行交互。

在您的账户中配置角色后，您必须在联合解决方案中加入角色。

问：AWS Transfer for SFTP 在我的 AMS 账户中使用有什么限制？

AWS SFTP 配置的传输仅限于没有“AMS-”或“MC-”前缀的资源，以防止对 AMS 基础设施进行任何修改。

问：在我的 AMS 账户 AWS Transfer for SFTP 中使用的先决条件或依赖条件是什么？

- 在创建服务器和用户之前，您必须拥有名称包含关键字“transf AWS Transfer for SFTP er”的 Amazon S3 存储桶。
- 要使用“客户识别提供商”，您必须部署 API Gateway、Lambda 函数和您的用户存储库（AD、Secrets Manager 等）。有关更多信息，请参阅[启用密码身份验证以 AWS Transfer for SFTP 使用 AWS Secrets Manager 和使用身份提供商](#)。

使用 AMS SSP AWS Transit Gateway 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Transit Gateway 功能。AWS Transit Gateway 是一项服务，可让您将 Amazon Virtual Private Cloud (VPCs) 和本地网络连接到单个网关。随着运行的工作负载数量的增加 AWS，您需要能够跨多个账户和 Amazon 扩展您的网络，VPCs 以跟上增长的步伐。如今，您可以使用对等互连连接成对的 A VPCs mazon。但是，如果无法集中管理 point-to-point 连接策略 VPCs，则管理许多 Amazon 的连接可能在运营上成本高昂且繁

琐。要实现本地连接，您需要将 AWS VPN 连接到每个 Amazon VPC。此解决方案的构建可能非常耗时，而且在数量 VPCs 增加到数百个时也难以管理。要了解更多信息，请参阅[AWS Transit Gateway](#)。

AWS Transit Gateway 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何在 AMS 账户 AWS Transit Gateway 中申请访问权限？

AWS Transit Gateway 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_tgw_console_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：AWS Transit Gateway 在我的 AMS 账户中使用有什么限制？

除了 Trans AWS Transit Gateway it Gateway 路由的路线表修改外，您的 AMS 单账户着陆区账户中提供了全部功能。通过提交管理 | 其他 | 其他 | 创建更改类型 (ct-1e1xtak34nx76) 来请求更改路由表。

Note

此服务仅支持单账户着陆区 (SALZ)，不支持多账户着陆区 (MALZ)。

问：在我的 AMS 账户 AWS Transit Gateway 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS Transit Gateway 中没有必备条件或依赖项可供使用。

使用 AMS SSP 在您的 AMS 账户中配置 AWS WAF -Web 应用程序防火墙

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS WAF 功能。AWS WAF 是一种 Web 应用程序防火墙 (AWS WAF)，可帮助保护您的 Web 应用程序免受常见 Web 漏洞的侵害，这些漏洞可能会影响应用程序可用性、危及安全性或消耗过多资源。AWS WAF 通过定义可自定义的 Web 安全规则，您可以控制允许或阻止哪些流量进入您的 Web 应用程序。您可以使用 AWS WAF 创建阻止常见攻击模式（例如 SQL 注入或跨站点脚本）的自定义规则；以及专为您特定应用程序设计的规则。

要了解更多信息，请参阅 [AWS WAF -Web 应用程序防火墙](#)。

AMS 不支持监控（CloudWatch 警报/事件/彩信提醒）。AWS WAF 由于的性质 AWS WAF，您必须为应用程序创建自定义规则；如果没有应用程序的上下文，AMS 无法为您量化和创建警报。要了解更多信息，请参阅 [AWS WAF -Web 应用程序防火墙](#)。

AWS WAF 在 AWS Managed Services 常见问题中

常见问题和答案：

问：AWS WAF 如何申请在我的 AMS 账户中进行设置？

AWS WAF 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_waf_role. 在您的账户中配置 | AWS WAF AM 角色后，您必须在联合身份验证解决方案中加入该角色。

问：使用有什么限制 AWS WAF？

配置权限后，您将拥有的全部功能。AWS WAF

问：使用的先决条件或依赖关系 AWS WAF是什么？

您的 AMS 账户 AWS WAF 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS Well-Architected Tool 在您的 AMS 账户中进行预配置

使用 AMS 自助服务配置 (SSP) 模式直接访问您的 AMS 托管账户中的 AWS Well-Architected Tool 功能。AWS Well-Architected Tool 可帮助您查看工作负载的状态，并将其与最新的 AWS 架构最佳实践进行比较。该工具基于Well-Architect [AWS ed Framework](#)，旨在帮助云架构师构建安全、高性能、弹性和高效的应用基础架构。该框架为您评估架构提供了一种一致的方法，已在 AWS 解决方案架构团队进行的数万次工作负载审查中使用，并提供了指导以帮助实施可随着时间的推移随应用程序需求而扩展的设计。要了解更多信息，请参阅[AWS Well-Architected Tool](#)。

AWS WA Tool 在 AWS Managed Services 常见问题中

常见问题和答案：

问：如何在 AMS 账户 AWS Well-Architected Tool 中申请访问权限？

AWS Well-Architected Tool 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_well_architected_tool_console_admin_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

问：AWS Well-Architected Tool 在我的 AMS 账户中使用有什么限制？

的全部功能可在您 AWS Well-Architected Tool 的 AMS 账户中使用。

问：在我的 AMS 账户 AWS Well-Architected Tool 中使用的先决条件或依赖条件是什么？

您的 AMS 账户 AWS Well-Architected Tool 中没有必备条件或依赖项可供使用。

使用 AMS SSP AWS X-Ray 在您的 AMS 账户中进行配置

使用 AMS 自助服务配置 (SSP) 模式直接在您的 AMS 托管账户中访问 AWS X-Ray (X-Ray) 功能。AWS X-Ray 帮助开发人员分析和调试生产型分布式应用程序，例如使用微服务架构构建的应用程序。借助 X-Ray，您可以了解您的应用程序及其底层服务的性能，从而识别和排除性能问题和错误的根本原因。X-Ray 提供请求在应用程序中传输时的 end-to-end 视图，并显示应用程序底层组件的地图。您可以使用 X-Ray 分析开发和生产中的应用程序，从简单的三层应用程序到由数千个服务组成的复杂微服务应用程序。要了解更多信息，请参阅[AWS X-Ray](#)。

AWS 托管服务中的 X-Ray 常见问题解答

常见问题和答案：

问：如何申请访问我 AWS X-Ray 的 AMS 账户？

通过提交管理 | AWS 服务 | 自配置服务 | 添加 (ct-1w8z66n899dct) 更改类型来申请访问权限。此 RFC 为您的账户配置以下 IAM 角色:customer_xray_console_role. 在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。此外，您必须拥有将数据从您的 Amazon EC2 实例推送customer_xray_daemon_write_instance_profile到 X-Ray 的权限。此实例配置文件是在您收到时创建的customer_xray_console_role。

您可以向 AMS Operations 提交服务请求以将其分配给现有实例配置文件，也可以使用 AMS Operations 为您启用 X-Ray 时创建的实例配置文件。customer_xray_daemon_write_policy

问：AWS X-Ray 在我的 AMS 账户中使用有什么限制？

除了使用 KM AWS X-Ray S 密钥 (KMS 密 AWS 钥) 进行加密外，您的 AMS 账户中还提供的所有功能。AWS X-Ray 默认情况下会加密所有跟踪数据。默认情况下，X-Ray 对静态跟踪和相关数据进行加密。如果您需要使用密钥加密静态数据，则可以选择由托管的 KMS 密钥 (aws/xray) 或 KMS 客户 AWS 管理的密钥。对于用于 X-Ray 加密的 KMS 客户管理密钥，请提交管理 | 其他 | 其他 | 创建更改类型 (ct-1e1xtak34nx76)。

问：在我的 AMS 账户 AWS X-Ray 中使用的先决条件或依赖条件是什么？

AWS X-Ray 依赖于 Amazon S3 和 CloudWatch 日志，它们已在 AMS 账户中实现。CloudWatch 传递依赖关系因数据源和功能可能与之交互的其他 AWS 服务 AWS X-Ray (例如 Amazon Redshift、Amazon RDS、Athena) 而异。

使用 AMS SSP Import/Export 在您的 AMS 账户中配置虚拟机

使用 AMS 自助配置 (SSP) 模式 Import/Export capabilities 直接在您的 AMS 托管账户中访问虚拟机。通过虚拟机，Import/Export 您可以轻松地将虚拟机映像从现有环境导入到 Amazon EC2 实例，然后将其导出回本地环境。该产品允许您将虚拟机 EC2 作为 ready-to-use 实例引入 Amazon，从而利用您为满足 IT 安全、配置管理和合规要求而构建的虚拟机的现有投资。您还可以将导入的实例导回本地虚拟化基础架构，从而可以在 IT 基础架构中部署工作负载。要了解更多信息，请参阅[虚拟机导入/导出](#)。

AWS Managed Services Import/Export 中的虚拟机常见问题

常见问题和答案：

问：如何使用我的 AMS 账户申请虚拟机的 Import/Export 访问权限？

Import/Export 通过管理 | AWS 服务 | 自配置服务 | 添加更改类型 (ct-1w8z66n899dct) 提交 RFC 来请求访问虚拟机。此 RFC 为您的账户提供以下 IAM 策略:customer_vmimport_policy。在您的账户中配置该角色后，您必须在联合解决方案中加入该角色。

服务需要一个额外的角色，即虚拟机 Import/Export 服务角色，才能在您的账户中执行操作。

问：Import/Export 在我的 AMS 账户中使用 VM 有哪些限制？

- AMS VM Import/Export 中均提供导入自定义机器映像和数据量的功能。但是，对 S3 的权限范围已缩小，将操作限制为 customer-vmimport-* 在与名称相匹配的存储桶上，从而限制对账户内信息的访问。
- AMS 虚拟机导入/导出支持图像和快照导入。但是，由于安全措施，实例导入和实例导出功能不可用。
- 此外，为了降低导出受限和敏感数据的风险，导出功能已被禁用。

问：在我的 AMS 账户 Import/Export 中使用 VM 有哪些先决条件或依赖关系？

- 您必须提供支持的磁盘映像才能导入到 AWS 环境中。有关信息，请参阅[虚拟机 Import/Export 要求](#)。
- Import/Export 无法通过 AWS 控制台访问虚拟机。您必须通过 AWS CLI、AWS Tools for PowerShell、或访问此服务 AWS SDKs。或者，您可以通过提交更改类型 ct-117rmp64d5mnb：部署 | 高级堆栈组件 | 身份和访问管理 (IAM) Management | 创建实例配置文件来请求实例配置文件。EC2 此实例配置文件允许工具从实例执行命令。

客户管理模式

AWS Managed Services (AMS) 客户管理模式提供了一种灵活且可以根据您的要求进行调整的管理模型。这可以被视为 AMS 无法为您运行的服务和应用程序的备用选项。AMS 不运营托管在此模式下创建的账户中的基础设施。但是，您可以在此模式下利用集中式多账户管理。在此模式下，可以利用以下多账户登录区域功能：

- 自动账户部署
- 通过网络账户中的 Transit Gateway 进行连接
- AMS Config 规则库
- 将日志副本存储在登录账户中
- 将客户管理的 Guard Duty 警报汇总到安全账户
- 整合账单
- 启用自定义服务控制策略。

例如：如果您想在 Ubuntu Pro 上运行工作负载，而该操作系统不是 AMS 管理的操作系统，则可以使用客户管理的账户来托管。您还可以通过客户托管账户整合工作负载，以利用通过在 AWS 组织之间共享而获得的预留 Instances/Sharing 计划的批量折扣。

开始使用客户管理模式

AMS 客户管理模式可通过特殊的多账户 landing zone 应用程序账户获得。

有关详细信息，包括如何创建客户托管应用程序帐户，请参阅[客户管理的应用程序帐户](#)。

AMS 和 AWS Service Catalog

AWS Managed Services (AMS) 中的 Service Catalog 允许组织创建和管理 AWS 信息技术 (IT) 服务的目录，并允许 IT 管理员创建、管理和向其账户中的最终用户分发经批准的产品目录，然后他们可以在个性化的服务门户中访问所需的产品。管理员可以控制哪些用户有权访问每种产品，以强制遵守组织业务政策。管理员还可以设置角色，这样最终用户只需要访问 Service Catalog 的 IAM 访问权限即可部署已批准的资源。Service Catalog 使您的组织能够从更高的灵活性和更低的成本中受益，因为最终用户只能从您控制的目录中查找和发布他们需要的产品。

Service Catalog 为您提供 AMS 变更申请 (RFC) 流程的替代方案，用于在您的 AMS 托管账户中配置和更新资源。AMS 为通过 Service Catalog 配置的所有基础设施资源管理大规模运行 AWS 所需的所

有基础设施运营任务，包括安全、合规、配置、可用性、补丁、监控、警报、报告、事件响应和成本优化。在您的 AMS 托管账户中使用 Service Catalog 可为您提供一种集中管理常用部署的 IT 服务的机制，并帮助您实现一致的治理，同时使用户能够快速将他们需要的经批准的 IT 服务部署到其托管环境中。

Service Catalog 入门

要开始使用 AMS 中的 Service Catalog，请通过 AMS 控制台提交服务请求以请求访问服务目录。提交请求后，将向您的账户部署三个 IAM 角色以及一个包含调用 AMS 的 CloudFormation 宏的 AMS 托管堆栈 Transform（如前所述），以便我们可以在系统中注册产品，并对通过 Service Catalog 配置的基础设施执行操作。部署的三个 IAM 角色包括 IT 管理员以服务目录管理员的身份管理产品的角色；一个供应用程序所有者和最终用户配置、启动和管理产品的角色；以及一个用作启动约束的角色，用于定义 Service Catalog 在启动或更新产品时将使用的权限。

开始之前 AMS 中的 Service Catalog

Service Catalog 是否会取代现有的 AMS 变更申请 (RFC) 流程？

在启用了 Service Catalog 的账户中，它将充当变更管理系统，您可以在其中通过预定义的产品目录在 AMS 账户中配置和更新 IT 服务；AMS 将提供默认 portfolio/product 目录，您的 IT 管理员可以创建和配置自己的目录。Service Catalog 只会确认通过 Service Catalog 置备的堆栈。同样，通过 Service Catalog 提供的服务也无法通过 AMS RFC 流程进行修改，因为在 Service Catalog 之外的修改会使堆栈偏离经批准的产品配置。

我能否在 AMS 控制台中查看通过服务目录配置的堆栈？

是。您可以在 AMS 控制台中查看通过服务目录配置的所有堆栈。通过服务目录配置的堆栈可通过“SC-”的堆栈 ID 轻松识别。尽管可以在 AMS 控制台中查看堆栈，但您将无法通过 AMS RFC 流程进行更新。对 AMS 变更管理系统 (RFCs) 的访问仅限于访问请求、补丁编排和备份 RFCs。

如果我通过 Service Catalog 配置 and/or 更新堆栈，AMS 控制台中是否会有相应的 RFC？

AMS 控制台中唯一会显示的 RFC 是在最初配置堆栈时向 AMS 注册堆栈的 RFC。此 RFC 由 AMS 验证流程自动归档，该流程是在通过 Service Catalog 启动堆栈时触发的。所有其他配置和更改都直接在 Service Catalog 中进行跟踪，也可以在服务目录控制台中查看。此外，您还可以使用 Service Catalog 中的预配置产品计划功能来查看在置备或更新产品之前将对资源所做的更改列表。

在我的 AMS 托管账户中配置产品时，我需要做任何具体的事情吗？

是。在 AMS 账户中配置的所有 Service Catalog 产品都必须在定义该产品的 CFN 模板中包含以下 JSON 行：


```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

在您的 AMS 托管账户中配置资源之前，这段 CloudFormation 代码会触发所需的 AMS 验证。您有责任将此行代码作为产品定义的一部分。如果不包括在内，则配置将失败并显示以下错误消息：“无法创建产品。此账户由 AMS 管理。AMS 账户中的所有商品的模板中都必须有 AMS Transform 代码。”

在发布时，是否有任何不 and/or 限于 AMS 客户的 Service Catalog 功能？

是的，以下 SC 功能在首次发布时不适用于 AMS 客户：

- 通过 Service Catalog 创建账户
- 能够通过 Service Catalog 在 AMS 管理的账户中启动所有 AWS 服务。AWS 服务的可用性仅限于 AMS 支持的服务（托管和自行配置）。有关 AMS 支持的服务的更多信息，请参阅 AMS 服务说明。
- Service Catalog IT 服务管理器 (ITSM) 连接器无法与 AMS 事件报告和服务请求进行通信。
- 无需修改即可利用 Service Catalog 快速入门和参考架构。请记住，AMS 账户的 Service Catalog 产品必须包含以下一行 JSON 代码：

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

在 CNF 模板中。请注意，此行不是典型的 AWS CloudFormation 模板的一部分，必须明确添加。

- AMS 目前不支持 Terraform 来配置 Service Catalog 产品。
- AMS 不支持 AWS CFN 堆栈集。
- 您无法创建自定义 IAM 角色。
- 服务操作仅限于：
 - [AWS-RebootRdsInstance](#)
 - [AWS EC2 重启实例](#)
 - [AWS 启动实例 EC2](#)
 - [AWS-StartRdsInstance](#)
 - [AWS-stop 实例 EC2](#)
 - [AWS-StopRdsInstance](#)
 - [AWS-CreatelImage](#)

- [AWS-CreateRdsSnapshot](#)
- [AWS-CreateSnapshot](#)

 Note

创建服务操作时，您可以将执行角色配置为最终用户的权限、启动角色或您选择的自定义 IAM 角色。所选执行角色必须具有足够的权限才能执行服务操作，并且必须具有允许 Service Catalog 代入 TrustPolicy 该服务操作的权限，否则该服务操作将在执行时失败。我们建议使用具有正确权限和信任策略的，可用作服务操作。AWSManagedServicesServiceCatalogLaunchRole

我还需要使用 AMS RFC 系统做什么？

正式上市 (GA) 后，您仍需要使用 RFCS 来运行以下操作：

- 配置补丁编排器
- 配置备份策略
- 请求实例访问权限
- 创建和分配不符合 AMS 准则的安全组。
- 执行工作负载摄取 (WIGS)
- 创建 IAM 角色

我能否使用 Service Catalog CLI 访问我的 AMS 托管账户中的服务目录？

是的，Service Catalog APIs 可用并通过 CLI 启用。从 Service Catalog 对象的管理到配置和终止这些构件的操作都可用。有关更多信息，请参阅 [AWS Service Catalog 资源](#)，或下载最新的 AWS 开发工具包或 CLI。

谁创建、管理和分发客户的批准产品目录？

客户的目录管理员 and/or IT 管理员或分配的资源负责管理您的 Service Catalog 目录和批准的产品。

我可以使用 AMS AMIs 吗？

2020 年 3 月之后 AMIs 销售的 AMS 可以通过 AWS Service Catalog 进行部署。

如何使用 Service Catalog 迁移到 AMS？

要使用 Service Catalog 将工作负载迁移到 AMS，首先要按照[工作负载摄取](#)WIGs 取 () 流程在 AMS 中创建 AMI。您可以使用 WIGS 生成的 AMI 在 Service Catalog 中创建产品。[AWS Service Catalog-入门](#)中详细介绍了如何执行此操作。

寻找你需要的数据 (SKMS) , AMS

要在使用 AWS Managed Services (AMS) 账户时查找所需的数据，请访问 AMS 服务知识管理 (SKMS) 系统。AMS。

SKMS 代表服务知识管理系统，指的是与为客户提供的 AWS Managed Services (AMS) 服务相关的所有信息。AMS 有一个用于查找数据的 SKMS API。

主题

- [什么是服务知识管理？](#)
- [IDs 在 AMS 中查找 VPC](#)
- [IDs 在 AMS 中查找子网](#)
- [查找 AMI IDs、AMS](#)
- [查找安全组 \(SG\) IDs、AMS](#)
- [在 AMS 中查找 IAM 实体](#)
- [在 AMS IDs 中查找堆栈](#)
- [在 AMS 中查找实例 IDs 或 IP 地址](#)
- [在 AMS 中查找亚马逊资源名称 \(ARNs\)](#)
- [在 AMS 中按照 ARN 查找资源](#)
- [查找 AMS 账户设置](#)

什么是服务知识管理？

服务知识管理是将所有信息存储在您的 AMS 账户上。有关以下内容的信息可通过 AMS 服务知识管理系统 (SKMS)、AMS SKMS API 或 AMS 控制台获得：

- VPCs
- 托管子网
- 堆栈和堆栈组件，包括 Amazon EC2 实例和其他资源
- Amazon 机器映像 (AMIs)

您可以使用来自 SKMS 的信息来了解所管理的基础架构，并作为变更管理和服务请求的输入，以创建、更改或移除基础架构。

Note

所有 AMS SKMS API 调用都记录在中。AWS CloudTrail

通过 AMS SKMS API 访问 SKMS，该API提供用于发现有关环境（VPCs 和子网）以及可以部署在那里的应用程序资源（堆栈、A EC2 mazon 实例和实例映像 AMIs或）的信息的操作。

VPCs 并且实例映像是在入职期间在具有必要访问权限的账户中设置的。在它们建立之后，您可以使用变更管理系统在中填 VPCs 充工作堆栈。

IDs 在 AMS 中查找 VPC

虚拟私有云 (VPC) 有一个或多个子网。在 AMS 中，您的 VPC 位于中，AWS 区域 并且您有私有子网和公有子网。

另请参阅[IDs 在 AMS 中查找子网](#)。

有些人 CTs 需要 VpcId。要查找 VPC ID，您可以使用 AMS 控制台或 API/CLI。

AMS 控制台：

在导航窗格中，选择VPCs和相关的 VPC。所选 VPC 的 VPC 详细信息页面将打开，其中包含包括 VPC ID 在内的信息。

AMS SKMS API ListVpcSummaries 或 CLI：

Note

必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用户指南》中的“AMS 信息资源”部分。您可能需要添加身份验证--profile选项；例如，aws amsskms *ams-cli-command* --profile SAML。您可能还需要添加该--region选项，因为所有 AMS 命令都将使用 us-east-1；例如。aws amscm *ams-cli-command* --region=us-east-1

 Note

AMS API/CLI (amscm 和 amsskms) 终端节点位于 AWS 弗吉尼亚北部区域。us-east-1根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令--region us-east-1时进行添加。如果这是您的身份验证方法--profile saml，则可能还需要添加。

1. 在以下示例中，第一个命令请求账户 VPCs 中所有人的摘要列表。第二个命令请求列表 VPCs，并使用查询过滤器仅列出 2016 年 VPCs 创建的列表，然后输出 CreatedTime VpcId、和 Name。

 Note

您可以通过 AMS 控制台中的开发者资源页面获取 AMS SKMS CLI。

```
aws amsskms list-vpc-summaries --output table
```

	ListVPCSummaries
+-----+	
	VPCSummaries
+-----+	
	CreatedTime
	2016-01-15T18:50:11Z
	VpcId
	vpc-01234567890abcdef
	LastModifiedTime
	2016-01-15T18:50:11Z
	Name
	952444781316-initial-vpc
+-----+	
	Visibility
+-----+	
	Id
	PrivateAndPublic
	Name
	PrivateAndPublic
+-----+	

2. 这次是查询：

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output table
```

```

-----
|                                     ListVPCSummaries                                     |
+-----+-----+-----+-----+
| 2016-01-15T18:50:11Z | vpc-01234567890abcdef | 952444781316-initial-VPC |
+-----+-----+-----+-----+

```

IDs 在 AMS 中查找子网

有几种资源要求您在配置时指定子网或子网列表。要查找子网，您可以使用 AMS 控制台或私有 API/CLI。Note that the AMS SKMS API/CLI 的 AMS SKMS，必须先安装后才能使用。

AMS 控制台：

1. 在导航窗格中，选择VPCs和相关的 VPC。所选 VPC 的 VPC 详细信息页面将打开一个子网表，单击子网 ID 打开详细信息页面并找到 ID。

AMS SKMS API ListSubnetSummaries 或 CLI：

Note

必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用户指南》中的“AMS 信息资源”部分。您可能需要添加身份验证 `--profile` 选项；例如，`aws amsskms ams-cli-command --profile SAML`。您可能还需要添加该 `--region` 选项，因为所有 AMS 命令都将使用 `us-east-1`；例如。`aws amscm ams-cli-command --region=us-east-1`

Note

AMS API/CLI（`amscm` 和 `amsskms`）终端节点位于 AWS 弗吉尼亚北部区域。`us-east-1` 根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令 `--region us-east-1` 时进行添加。如果这是您的身份验证方法 `--profile saml`，则可能还需要添加。

要查找 VPC 的子网，您可以使用如下所示的list-subnet-summaries命令进行搜索。

 **Note**

如果您正在寻找不在 AMS 账户中的子网，可以尝试aws ec2 describe-subnets --region us-west-2。

1. 短信管理系统的 API/CLI ListSubnetSummaries 操作：

一个简单的清单：

```
aws amsskms list-subnet-summaries
```

输出到表格：

```
aws amsskms list-subnet-summaries --output table
```

2. SKMS API ListSubnetSummaries 操作具有根据可见性缩小结果范围的参数。此外，您还可以根据名称[筛选](#)结果。如果您使用的是 CLI，也可以使用该--query选项来缩小输出范围或搜索值的一部分。例如，要查找特定 VPC 的所有子网，您可以使用以下命令：

```
aws amsskms list-subnet-summaries --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

它返回的结果是这样的：

ListSubnetSummaries			
Private	subnet-01234567890abcdef	Demo Deployment Zone #1	
Private	subnet-01234567890abcdef	Demo Deployment Zone #1	
Public	subnet-01234567890abcdef	Demo DMZ #1	
Public	subnet-01234567890abcdef	Demo DMZ #1	

有关使用 CLI 查询的信息，请参阅[如何使用--query 选项过滤输出](#)和查询语言参考[JMESPath 规范](#)。

3. 如果您有多个 VPCs，请在命令中加入一个 VPC 筛选器，然后为每个 VPC 运行该命令。例如：

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxx --query
  "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

4. 在 AWS 中，使用[描述子网](#)。

有关使用 CLI 查询的信息，请参阅[如何使用--query 选项过滤输出](#)和查询语言参考[JMESPath 规范](#)。

子网名称

您的 AMS 子网是在收集您的输入并添加到系统中后自动创建的。AMS 使用公式来创建您的子网名称：A **ACCOUNT_ID-SUBNET-TYPE-AZ-IDENTIFIER**。子网类型将是 dmzshared-services、或 customer-application。如果您有多个客户应用程序子网，则可以在子网名称的账户 ID 后面添加一个可选标识符，以表明该子网是“附加”或“保留”子网。

查找 AMI IDs、AMS

亚马逊系统映像 (AMI) 是基于亚马逊 EC2 实例创建的亚马逊 EC2 实例的模板。AWS 提供每月更新 AMIs (例如补丁)；但是，AWS Managed Services (AMS) AMIs 要求经过修改后才能使用 AMS。AMS 会发布新版本 AMIs，你可以在每个月的补丁周二之后不久使用。

Amazon 系统映像 (AMIs) 是用于在 AWS 中创建 EC2 实例的实例配置模板。AMS 要求对由 AMS 管理 AMIs 的资源使用该特定的资源。创建 EC2 实例和 EC2 Auto Scaling 组的更改类型要求您为 AMS 指定一个 AMI，作为更改类型创建的实例的基础。AMS 建议您始终选择最新可用的 AMI。

要了解更多信息 AWS AMIs，请参阅[AWS AMI 设计](#)。

在为您的 AMS 账户创建 Amazon EC2 堆栈或 Amazon A EC2 uto Scaling 组时，必须通过指定 AMI Amild。您只能以“客户-”开头，我们建议您始终选择最新的 AMI。AMIs

要查找您账户的最新 AMI，您可以使用 AMS SKMS CLI 命令进行搜索或使用 AMS 控制台详细信息页面搜索相关 VPC：

- 使用 AMS 控制台：“可 AMIs 用”列在 AMS 控制台的 AMI 页面上。从 AMIs 以“客户-”开头的名称中进行选择。
- 使用 AMS SKMS API/CLI ListAmis 操作。

Note

必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用户指南》中的“AMS 信息资源”部分。您可能需要添加身份验证 `--profile` 选项；例如，`aws amsskms ams-cli-command --profile SAML`。您可能还需要添加该 `--region` 选项，因为所有 AMS 命令都将使用 `us-east-1`；例如。`aws amscm ams-cli-command --region=us-east-1`

以下是一个 CLI 示例，其中包含一个将结果限制在客户 AMIs 范围内的 `query` 选项：

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --output table
```

此示例使用带有 `filter` 选项的 `query` 选项来查找以“客户”开头 AMIs 的 Windows：

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows --output table
```

- 有关使用 CLI 查询的信息，请参阅[如何使用--query 选项过滤输出](#)和查询语言参考[JMESPath 规范](#)。

查找安全组 (SG) IDs、AMS

Amazon EC2 OpenSearch 创建和创建域名 CTs 需要安全组 ID。这将以表格形式出现 `sg-02ce123456e7893c7`。您的账户至少有两个默认安全组；请参阅[安全组](#)。此外，您可能还有为特定目的创建的安全组。要发现您的安全组，请执行以下操作：

- AWS 控制台：使用 EC2 或 VPC 控制台查看所选 VPC 的所有安全组。
- API/CLI（登录您的 AMS 账户时）：

列出您的安全组：

```
aws ec2 describe-security-groups
```

在 AMS 中查找 IAM 实体

您的账户具有默认 IAM 角色和策略；请参阅[AMS 中的 IAM 用户角色](#)和默认 IAM 实例配置文件；参见[EC2 IAM 实例配置文件](#)默认策略。要了解您的 IAM 角色和策略，请执行以下操作：

- 控制台：使用 IAM 控制台查看您账户的所有 IAM 策略和角色。
- API/CLI（登录您的 AMS 账户时）：

Note

必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用户指南》中的“AMS 信息资源”部分。您可能需要添加身份验证 `--profile` 选项；例如，`aws amsskms ams-cli-command --profile SAML`。您可能还需要添加该 `--region` 选项，因为所有 AMS 命令都将使用 `us-east-1`；例如。`aws amscm ams-cli-command --region=us-east-1`

列出你的角色：

```
aws --profile saml iam list-roles
```

列出您的政策：

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

在 AMS IDs 中查找堆栈

要查找堆栈 ID，您可以使用亚马逊 EC2 控制台、AMS 控制台或 AMS SKMS API/CLI。

AMS 控制台：

- 在导航窗格中，选择 RFCs，然后单击创建堆栈的 RFC。使用顶部的筛选选项来缩小列表范围。RFC 详细信息页面打开，其中包含带有堆栈 ID 的运行输出。
- 或者，您可以在导航窗格中选择堆栈以打开堆栈列表页面，然后在堆栈列表中翻阅您感兴趣的堆栈。如果您知道要查找的堆栈的主题，则此方法会更有用。

亚马逊 EC2 控制台：

在导航窗格中，选择实例、负载均衡器或 Auto Scaling 组。

AMS SKMS API ListStackSummaries 或 CLI：

 **Note**

必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用户指南》中的“AMS 信息资源”部分。您可能需要添加身份验证--profile选项；例如，aws amsskms *ams-cli-command* --profile SAML。您可能还需要添加该--region选项，因为所有 AMS 命令都将使用 us-east-1；例如。aws amscm *ams-cli-command* --region=us-east-1

 **Note**

AMS API/CLI（amscm 和 amsskms）终端节点位于 AWS 弗吉尼亚北部区域。us-east-1根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令--region us-east-1时进行添加。如果这是您的身份验证方法--profile saml，则可能还需要添加。

要查看当前账户中的堆栈列表，请运行 SKMS API (CLI:list-stack-summaries) 的 ListStackSummaries 操作。要获取有关特定堆栈实例的完整信息 StackId，请运行 GetStack。

- 在以下示例中，第一个命令请求账户中所有堆栈实例的摘要列表。第二条命令请求堆栈实例列表，使用查询过滤器仅列出特定堆栈模板的堆栈实例，然后输出 VpcId、Name 和 StackId。

```
aws amsskms list-stack-summaries --output table
```

	ListStackSummaries							
	StackSummaries							
+-----+-----+-----+-----+								
	VpcId		StackId		StackTemplateId		Name	
+-----+-----+-----+-----+								
	vpc-0123abcd		stack-1fb7fe2212345678		stm-sdhopvbb123456789		Test ELB	

```
|vpc-0123abcd|stack-8323cc0e12345678|stm-s2b72beb123456789|S3 store|
|vpc-0123abcd|stack-2309fa0712345678|stm-sdhopvbb123456789|ELB      |
|vpc-0123abcd|stack-5e61a70512345678|stm-sdpabqbb123456789|PatchSim|
|vpc-0123abcd|stack-bd0e080d12345678|stm-s2b72beb123456789|CLI demo|
+-----+-----+-----+-----+-----+
```

有关使用 CLI 查询的信息，请参阅[如何使用--query 选项过滤输出](#)和查询语言参考[JMESPath 规范](#)。

Note

有关使用实例 IDs 进行访问的信息，另请参阅[使用堡垒访问实例](#)。

在 AMS 中查找实例 IDs 或 IP 地址

- 要请求访问实例、登录实例或创建 AMI，您必须拥有实例 ID。对于 EC2 实例（独立实例或堆栈的一部分）或数据库实例，可以通过几种不同的方式查找 ID：
 - ASG 堆栈中实例的 AMS 控制台：在 RFC 详细信息页面上查看创建堆栈的 RFC。在“执行输出”部分，您将找到 ASG 堆栈的堆栈 ID，然后可以转到 EC2 控制台 Auto Scaling Groups 页面搜索该堆栈 ID 并为其查找实例。找到实例后，将其选中，页面底部将打开一个包含详细信息的区域，其中包含包括 IP 地址在内的详细信息。
 - 独立实例 EC2 或数据库 (DB) 实例的 AMS 控制台：在 RFC 详细信息页面上查看创建 EC2 堆栈或数据库实例的 RFC。在“执行输出”部分，您将找到实例 ID 和 IP 地址。
 - AWS EC2 控制台：
 1. 在导航窗格中，选择 Instances (实例)。将打开“实例”页面。
 2. 单击您想要获得 ID 的实例。实例详细信息页面打开并显示 ID 和 IP 地址。
 - AWS 数据库控制台：
 1. 在主页上，选择数据库实例。将打开“实例”页面。
 2. 筛选您想要获取 ID 的数据库实例。实例详细信息页面打开并显示 ID。
 - AMS CLI/API。

Note

必须安装 AMS CLI 才能使这些命令生效。要安装 AMS API 或 CLI，请前往 AMS 控制台开发者资源页面。有关 AMS CM API 或 AMS SKMS API 的参考资料，请参阅《用

户指南》中的“AMS 信息资源”部分。您可能需要添加身份验证`--profile`选项；例如，`aws amsskms ams-cli-command --profile SAML`。您可能还需要添加该`--region`选项，因为所有 AMS 命令都将使用 `us-east-1`；例如。`aws amscm ams-cli-command --region=us-east-1`

 Note

AMS API/CLI (`amscm` 和 `amsskms`) 终端节点位于 AWS 弗吉尼亚北部区域。`us-east-1`根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令`--region us-east-1`时进行添加。如果这是您的身份验证方法`--profile saml`，则可能还需要添加。

运行以下命令以获取堆栈执行输出详细信息：

```
aws amsskms get-stack --stack-id STACK_ID
```

输出如下所示，`InstanceId` 显示在底部附近`Outputs` (显示的值为示例)：

```
{
  "Stack": {
    "StackId": "stack-7fa52bd5eb8240123",
    "Status": {
      "Id": "CreateCompleted",
      "Name": "CreateCompleted"
    },
    "VpcId": "vpc-01234567890abcdef",
    "Description": "Amazon",
    "Parameters": [
      {
        "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
        "Key": "SecurityGroups"
      },
      {
        "Value": "subnet-01234567890abcdef",
        "Key": "InstanceSubnetId"
      },
      {
        "Value": "t2.large",
```

```
        "Key": "InstanceType"
      },
      {
        "Value": "ami-01234567890abcdef",
        "Key": "InstanceAmiId"
      }
    ],
    "Tags": [],
    "Outputs": [
      {
        "Value": "i-0b22a22eec53b9321",
        "Key": "InstanceId"
      },
      {
        "Value": "10.0.5.000",
        "Key": "InstancePrivateIP"
      }
    ],
    "StackTemplateId": "stm-s6xvs0000000000000",
    "CreatedTime": "1486584508416",
    "Name": "Amazon"
  }
}
```

在 AMS 中查找亚马逊资源名称 (ARNs)

Amazon 资源名称 (ARN) 是一个字符串，用于唯一标识 AWS 资源，例如 EC2 实例、S3 存储桶、账户、Lambda 函数等。AWS 当你想在所有（例如 IAM 策略 AWS、亚马逊关系数据库服务 (Amazon RDS) 标签和 API 调用中）中明确指定资源时，需要一个 ARN。ARNs 由指定服务、区域、账户和其他信息的标识符构成。有三种 ARN 格式：

```
arn:aws:service:region:account-id:resource-id
arn:aws:service:region:account-id:resource-type/resource-id
arn:aws:service:region:account-id:resource-type:resource-id
```

Note

ARN 的具体格式取决于服务和资源类型。[要了解更多信息 ARNs，请参阅 Amazon 资源名称 \(ARNs\) 和 AWS 服务命名空间和 ARN 格式。](#)

有关按资源划分的 ARN 格式示例，请参阅 AWS 服务授权参考[资源类型表](#)。

查找 AWS 对象的 ARN 可能很困难。以下是三种尝试方法：

- AWS 服务控制台：前往相关的 AWS 服务控制台，找到资源，然后在该资源的详细信息中找到 ARN。
- AWS API/CLI（必须先安装 AWS CLI）：在 [AWS CLI 命令参考](#) 中查找相关服务，然后，根据 AWS 服务，查找相关操作，例如 `describeget`、或，依此类推。例如，对于所有 IAM 角色、策略和用户，您可以使用以下命令在 CLI 的输出中获取 ARN：

```
aws iam get-role --role-name EMR_DefaultRole
```

- 根据相关格式构建 ARN：通过查看 [AWS 服务的操作、资源和条件键页面](#)，找到相关的服务，然后找到相关的操作，然后深入到资源 ARN 格式，找到资源的 ARN 格式。设置好格式后，用相关设置替换变量。

您可以按照适当的格式（格式因服务和资源类型而异）并填写信息自行构建 ARN。以下是一些 ARN 示例：

- AWS 账户 ARN 的语法如下：

```
arn:aws:iam::ACCOUNT-ID:root
```

- S3 ARN 具有由存储桶和关联对象组成的扁平层次结构：

```
arn:aws:s3:::ams-bucket
```

- EC2 ARN 具有子资源类型，例如图像、安全组、实例等。此示例末尾包含实例 ID：

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Lambda ARN 具有资源 ID 部分的函数名称，您可能需要在末尾添加版本号，如以下示例所示：

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```

该 AWS Key Management Service 服务提供以下信息：[查找密钥 ID 和密钥 ARN](#)。

[要查找 DynamoDB 表的 ARN，请使用 DynamoDB 描述表 CLI。](#)

要了解局外人对发现的看法 AWS ARNs，请参阅 [AR AWS N 解释：Amazon 资源名称指南](#)。

在 AMS 中按照 ARN 查找资源

Amazon 资源名称 (ARNs) 唯一标识 AWS 资源。 [要了解 ARNs 和 ARN 格式，请参阅 Amazon 资源名称 \(ARNs\) 和 AWS 服务命名空间和 ARN 格式。](#)

Note

要从资源的 ARN 中获取有关该资源的详细信息，您必须有权访问创建该资源的账户。

没有从资源 ARN 中 AWS 查找所有资源详细信息的直接路径，因为服务有多种资源类型以及各种相关信息。如果您有资源的 ARN，则可以确定：

- 相关 AWS 服务（第三个 ARN 部分）会告诉您要查看哪个 AWS 控制台才能找到资源
- 资源 ID（第六或第七个 ARN 区段）确认您找到了正确的资源

或者，您可以在《AWS CLI 命令[参考](#)》中[查找该服务可用的 AWS CLI 命令](#)，以获取有关该资源的详细信息的信息。

例如，根据以下 ARN，您可以确定服务是 lambda，账户是 123456789012，资源类型是 function，函数名称是 TestFunction

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

由此，您可以查看 [Lambda 服务的 CL AWS I 文档](#)，了解如何使用各种命令（例如 get-function 和）检索更多详细信息。get-function-configuration

例如，如果您有 Lambda 函数的名称或 ARN，则可以使用以下命令来获取有关 Lambda 函数的更多信息：

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

查找 AMS 账户设置

用于创建 AMS RFCs、设置日程安排和确定谁接收通知的账户设置。

有些设置是在入职期间创建的，需要服务请求才能更改。您应该记下这些账户信息，因为您将在与 AMS 通信时使用这些信息：

- 凭证：如果您需要检索 AMS 用户名或密码，请联系您的本地 IT 管理员——AMS 使用您的公司 Active Directory。
- 云服务交付经理 (CSDM)：此人是您与 AMS 的联络人，可以回答服务问题。您将在入职时获得此人的联系信息，并应将其提供给组织中与 AMS 互动的所有人。您可以期望从此人那里收到有关您的 AMS 服务的月度报告。
- 控制台访问权限：您可以通过专门为您的账户设置的 URL 访问 AMS 控制台。您可以从 CSDM 获取网址。
- AMS CLI：您可以通过 AMS 控制台开发者资源页面获取 AMS CLI，也可以通过 CSDM 获得的可分发软件包获取。获得发行版软件包后，请按照[安装或升级 AMS CLI 中概述的](#)步骤进行操作。
- 维护时段：您的维护时段决定何时对您的 EC2 实例进行修补。AWS Managed Services 维护窗口（或维护窗口）为 AWS Managed Services (AMS) 执行维护活动，并在太平洋时间每个月的第二个星期四下午 3 点至下午 4 点重复。AMS 可能会在 48 小时通知后更改维护时段。您可能在入职时选择了不同的时段，请记录您选择的维护时段。
- 监控：AMS 默认提供一组 CloudWatch 指标，但您也可以请求其他指标。如果你这样做，请记录下来。
- 日志：默认情况下，您的日志存储在 `ams-a-ACCOUNT_ID` log-management 中，**REGION** 这是生成日志的区域。**REGION**
- 缓解：在入职时，AMS 会记录您选择的缓解措施，以防发现针对您的资源的恶意软件攻击。例如，联系某些人。让组织中与 AMS 互动的所有人都能获得这些信息。
- 区域：您可以在 AMS 控制台中查看 VPC 详情页面。您也可以在安装 AMS SKMS CLI 后运行此命令（此命令使用 SAML 配置文件，如果您的身份验证方法不同，请将其删除）：

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

 Important Note

AMS API/CLI (amscm 和 amsskms) 终端节点位于 AWS 弗吉尼亚北部区域。us-east-1 根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令 `--region us-east-1` 时进行添加。如果这是您的身份验证方法 `--profile saml`，则可能还需要添加。

在 AMS FQDNs 中查找

AWS Managed Services (AMSCTs) 访问权限更改类型 () 要求您的 AMS 信任域的完全限定域名或 FQDN，格式为。C844273800838.amazonaws.com 要发现您的 AWS FQDN，请执行以下任一操作：

- AWS 控制台：在 AWS Directory Service 控制台的“目录名称”列中查看。
- CLI：登录域名时使用以下命令：

Windows (返回用户和 FQDN)：

```
whoami /upn
```

或 (DC+DC+DC=FQDN)

```
whoami /fqdn
```

Linux：

```
hostname --fqdn
```

 Note

AMS API/CLI (amscm 和 amsskms) 终端节点位于 AWS 弗吉尼亚北部区域。us-east-1 根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令 `--`

`region us-east-1` 时进行添加。如果这是您的身份验证方法 `--profile saml`，则可能还需要添加。

在 AMS 中查找可用区 (AZs)

可用区：所有账户都至少有两个可用区。要准确找到您的可用区名称，您必须先知道关联的子网 ID。

- AMS 控制台：如有必要 VPCs，在导航窗格中单击，然后单击相关的 VPC。在 VPCs 详细信息页面上，在子网表中选择相关的子网，打开带有关联可用区名称的子网详细信息页面。
- AMS SMS SMS API/CLI：

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

Note

AMS API/CLI (`amscm` 和 `amsskms`) 终端节点位于 AWS 弗吉尼亚北部区域。`us-east-1` 根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令 `--region us-east-1` 时进行添加。如果这是您的身份验证方法 `--profile saml`，则可能还需要添加。

在 AMS 中查找 SNS 话题

您的 SNS 主题决定了在各种情况下谁会收到通知。AMS 提供有关 AMI 通知 (参见 [带有 SNS 的 AMS AMI 通知](#))、CloudWatch 警报和 EC2 资源 (请参阅 [接收 AMS 生成的警报](#)) 等的 SNS 主题。要发现您现有的 SNS 话题，请执行以下操作：

- AWS 控制台：使用 SNS 控制台查看所有主题、应用程序和订阅以及消息图表。还可以创建、删除、订阅和发布主题。
- API/CLI (登录您的 AMS 账户后，需要 AWS CLI)：

列出你的 SNS 话题：

```
aws sns list-topics
```

列出您的 SNS 订阅：

```
aws sns list-subscriptions
```

Note

AMS API/CLI (amscm 和 amsskms) 终端节点位于 AWS 弗吉尼亚北部区域。us-east-1 根据您的身份验证设置方式以及您的账户和资源所在的 AWS 区域，您可能需要在发出命令 `--region us-east-1` 时进行添加。如果这是您的身份验证方法 `--profile saml`，则可能还需要添加。

在 AMS 中查找备份设置

备份和快照由 AMS 通过本机 [AWS Backup](#) 服务进行管理。

配置通过 AWS Backup 计划进行管理。您可以 AWS Backup 制定多个计划，将带标签的资源与备份计划和保留策略相关联。要查找您的 AMS 账户 AWS Backup 设置，请使用 <https://console.aws.amazon.com/backup> 控制台或 AWS CLI 命令参考获取 [备份](#) 命令。

有关 AMS 和的更多信息 AWS Backup，请参阅 [连续性管理](#)。

AMS 中的访问管理

学习如何使用 SSH 或远程桌面协议 (RDP) 访问资源，以及如何使用堡垒。

AWS Managed Services (AMS) 访问管理系统是在入职期间配置的。只有拥有 AMS IAM 用户角色、通过 AMS 联合身份的用户才能访问账户中的 AMS 资源。

除了下文所述的联合信任外，AMS 安全组还是私有和公共应用程序访问的重要组成部分。有关 AMS 安全组以及如何更改安全组的信息，请参阅[安全组](#)。

主题

- [什么是访问管理？](#)
- [如何以及何时在 AMS 中使用 root 用户账户](#)
- [AMS 高级控制台和 Amazon EC2 访问权限](#)
- [访问 AWS 管理控制台和 AMS 控制台](#)
- [使用堡垒访问实例](#)

什么是访问管理？

访问管理是 AMS 通过仅允许授权和经过身份验证的访问来保护您的资源的方式。AMS 使用默认 IAM 用户角色和实例配置文件以及多因素身份验证、安全组、DNS 友好型堡垒名称等来保护您的资源。

AMS 重点介绍需要管理的三种访问类型：

- 控制台访问权限：利用联合，账户 Active Directory 中的用户可以使用单点登录 (SSO) 访问控制台。如果您为这些账户配置了多重身份验证，则可以继续要求 MFA 才能访问控制台。
- 使用 RDP 或 SSH 访问实例：利用 Active Directory 信任，账户现有 Active Directory 中的用户可以请求访问实例，然后使用其现有的公司凭据成功对堡垒和实例进行身份验证。如果您为这些账户配置了多重身份验证，则可以继续要求 MFA 来请求访问实例。AMS 使用自己的 MFA 解决方案来限制 AMS 工程师访问实例。
- 应用程序访问权限：因用例而异。

主题

- [AMS 访问您的账户的原因和时间](#)

AMS 访问您的账户的原因和时间

AWS Managed Services (AMS) 管理您的 AWS 基础设施，有时，出于特定原因，AMS 操作员和管理员会访问您的账户。这些访问事件记录在您的 AWS CloudTrail (CloudTrail) 日志中。

以下主题解释了 AMS 访问您的账户的原因、时间和方式。

AMS 客户账户访问触发器

AMS 客户账户访问活动由触发器驱动。今天的触发器是在我们的问题管理系统中为响应 Amazon CloudWatch (CloudWatch) 警报和事件以及您提交的事件报告或服务请求而创建的 AWS 票证。每次访问可能会执行多个服务呼叫和主机级别的活动。

下表列出了访问理由、触发器和触发器的启动者。

访问触发器

访问	发起者	触发器
修补	AMS	补丁问题
基础设施部署	AMS	部署问题
内部问题调查	AMS	问题问题 (已确定为系统性问题)
警报调查和补救	AMS	AWS Systems Manager 运营工作项目 (SSM OpsItems)
手动执行 RFC	您	变更申请 (RFC) 问题。(非自动化 RFCs 可能需要 AMS 访问您的资源)
事故调查和补救	您	入站支持案例 (您提交的事件或服务请求)
入库服务请求配送	您	

AMS 客户账户访问权限 IAM 角色

触发后，AMS 使用 AWS Identity and Access Management (IAM) 角色访问客户账户。与您账户中的所有活动一样，角色及其使用情况均已登录 CloudTrail。

 Important

请勿修改或删除这些角色。

用于 AMS 访问客户账户的 IAM 角色

角色名称	账户类型 (SALZ 、MALZ 管理、MALZ 应用程序等)	说明
ams-service-admin	SALZ、MALZ	AMS 服务自动化访问和自动基础设施部署，例如 Patch、Backup、自动修复。
ams-application-infra-read-only	SALZ、MALZ 应用程序、MALZ Tools-Application	操作员只读权限
ams-application-infra-operations		操作员访问 incidents/service 请求
ams-application-infra-admin		AD 管理员访问权限
ams-primary-read-only	MALZ 管理层	操作员只读权限
ams-primary-operations		操作员访问 incidents/service 请求
ams-primary-admin		AD 管理员访问权限
ams-logging-read-only	MALZ 日志记录	操作员只读权限
ams-logging-operations		操作员访问 incidents/service 请求
ams-logging-admin		AD 管理员访问权限
ams-networking-read-only	MALZ 网络	操作员只读权限
ams-networking-operations		操作员访问 incidents/service 请求
ams-networking-admin		AD 管理员访问权限

角色名称	账户类型 (SALZ 、MALZ 管理、MALZ 应用程序等)	说明
ams-shared-services-read-only	MALZ 共享服务	操作员只读权限
ams-shared-services-operations		操作员访问 incidents/service 请求
ams-shared-services-admin		AD 管理员访问权限
ams-security-read-only	MALZ 安全	操作员只读权限
ams-security-operations		操作员访问 incidents/service 请求
ams-security-admin		AD 管理员访问权限
ams-access-security-analyst	SALZ、MALZ 应用程序、MALZ Tools-Application、MALZ Core	AMS 安全访问权限
ams-access-security-analyst-只读		AMS 安全，只读权限
Sentinel_ _Role_ 0 m AdminUser BHe PXHaz RQadu PVc CDc	SALZ	[BreakGlassRole] 用于 BreakGlass 进入客户账户
Sentinel_ _Role_ PowerUser S0 0 wZuPu ROOI lazDb RI9	SALZ、MALZ	Poweruser 可以访问客户账户以执行 RFC
Sentinel_ _role_pd4 l6l6rw9rd0lnlkd5 ReadOnlyUser JOo		ReadOnly 访问客户账户以执行 RFC
ams_admin_role		管理员访问客户账户以执行 RFC

角色名称	账户类型 (SALZ 、MALZ 管理、MALZ 应用程序等)	说明
AWSManagedServices_Provisioning_CustomerStacksRole		用于通过 Ingest 代表客户启动和更新 CFN 堆栈 CloudFormation
客户_ssm_自动化_角色		CT 执行将角色传递给 SSM Automation 以执行运行手册
ams_ssm_automation_role	SALZ、MALZ 应用程序、MALZ Core	AMS 服务将角色传递给 SSM Automation 以执行运行手册
ams_ssm_iam_deployment_role	MALZ 应用程序	IAM 目录使用的角色
ams_ssm_shared_services_mediarole	MALZ 共享服务	应用程序 ams_ssm_automation_role 在共享服务账户中执行特定 SSM 文档时使用的角色
AmsOpsCenterRole	SALZ、MALZ	用于在客户账户 OpsItems 中创建和更新
AMSOpsItemAutoExecutionRole		用于获取 SSM 文档、描述资源标签 OpsItems、更新和启动自动化
customer-mc-ec2 实例配置文件		默认客户 EC2 实例配置文件 (角色)

请求实例访问权限

要访问资源，必须先提交变更申请 (RFC) 才能访问该资源。您可以请求两种访问权限：管理员（读/写权限）和只读（标准用户访问权限）。默认情况下，访问持续八小时。此信息为必填项：

- 您要访问的一个或多个实例的堆栈 IDs ID 或堆栈集。
- 您的 AMS 信任域的完全限定域名。
- 想要访问的用户的 Active Directory 用户名。

- 您要访问堆栈所在的 VPC 的 ID。

获得访问权限后，您可以根据需要更新请求。

有关如何请求访问权限的示例，请参阅[堆栈管理员访问权限 | 授予](#)或[堆栈只读访问权限 | 授予](#)。

如何以及何时在 AMS 中使用 root 用户账户

[root 用户](#)是您 AWS 账户中的超级用户。AMS 监控根用户使用情况。我们建议您仅将 root 用于少数需要它的任务，例如：更改账户设置、激活 AWS Identity and Access Management (IAM) 账单和成本管理权限、更改根密码以及启用多因素身份验证 (MFA)。请参阅[《用户指南》中的“需要根用户凭据的 AWS Identity and Access Management 任务”](#)。

Note

在 AMS Advanced 入职期间启用 MFA，明确禁止根用户访问。AMS 管理的账户的根访问权限与其他 AWS 账户不同，对整个 AMS 管理的环境的安全至关重要。配置的 MFA 是虚拟 MFA，使用 AMS 拥有的设备执行。在 AMS 的帮助下配置虚拟 MFA 后，虚拟令牌会立即删除。这样可以确保您和 AMS 都无法以 root 用户身份登录账户。只有在特殊请求时才能重新启用 root 登录（详见下文），AMS 希望仅在绝对必要时才使用此类访问权限。有关 MFA 的信息，请参阅[使用多重身份验证保护新账户](#)。

根访问权限总是会触发 AMS 安全和运营团队的响应。AMS 会监控根访问权限的 API 调用，如果检测到此类访问，则会触发警报。

请求根访问权限在 AMS 账户类型之间略有不同。

使用 AMS 高级单账户登陆区进行根访问权限：

如果您有单账户登录区，请联系您的云服务交付经理 (CSDM) 和云架构师 (CAs)，告知他们您需要的根访问工作。最好在拟议活动开始前二十四小时发出通知。

使用 AMS Advanced 多账号登陆区进行根访问权限：

对于多账户 landing zone 应用程序、共享服务、安全或网络账户，请使用管理 | 其他 | 其他 (ct-1e1xtak34nx76) 更改类型。包括使用根用户凭证的日期、时间和目的，并安排 RFC，确保在建议的活动开始前二十四小时发出通知。使用您的多账户 landing zone 管理账户提交 RFC。

此外，请提前 CAs 24 小时联系您的 CSDM，告知他们您需要的 root 访问工作。

AMS 操作和对 root 用户使用情况的安全响应：

使用 root 用户帐户时，AMS 会收到警报。如果未计划使用根证书，他们会联系 AMS Security 团队和您的账户团队，以验证这是否是预期的活动。如果不是预期的活动，AMS 会与您的安全团队合作调查问题。

AMS 高级控制台和 Amazon EC2 访问权限

访问 AMS 高级控制台。

访问您的亚马逊 EC2 实例。

提交访问请求：

登录您的 AMS Amazon EC2 实例：

访问 AWS 管理控制台和 AMS 控制台

在入职期间，您将获得 AWS 管理控制台的登录信息（权限有限：您可以写入 AMS 控制台，也可以写入客户信息页面中的某些字段）。您可以通过在管理控制台中选择 [Man AWS aged Services](#) 链接来访问 AMS 控制台。联合访问权限或共享凭证（用户名/密码）均按照您的 IT 管理团队的协议进行准备。如需进一步创建账户或群组，请向 AMS 提交服务申请。

有关获取 AWS 管理控制台访问权限的信息，请参阅[使用 AWS 管理控制台](#)。

有关使用 AMS 控制台的一些技巧，请参阅[使用 AMS 控制台](#)。

临时访问 AMS 控制台

如果您尚未设置身份提供商（例如 SAML）来向 AMS 进行身份验证，则可以临时访问 AMS 控制台。请联系您的 CSDM，代表您提交部署 | 高级堆栈组件 | 身份和访问管理 (IAM) | 创建实体或策略变更请求 (ct-3dpd8mdd9jn1r)，其中包含以下值：

- **UserName:** 您正在创建的 IAM 用户实体的名称

- AccessType: “控制台访问权限”
- UserPermissions: “**USERNAME** (您想要获得临时访问权限的人) 的临时 AMS 控制台访问权限”
- 电子邮件通知 : 您的电子邮件地址 , 因此您可以在 AMS 要求您批准请求时批准请求

Note

这份用于临时访问 AMS 控制台的 RFC 需要您的内部安全团队和 AMS Global Security 进行安全审查和接受。

此请求完成并能够登录后, 您需要批准创建的 RFC, 以跟踪批准情况并允许 AMS 团队完成工作。要批准 RFC, 请在 RFC 的列表页面中找到它 (旁边会有一个待批准标志), 选择它以打开该 RFC 的 RFC 详细信息页面, 然后选择批准。请注意, 在 RFC 获得批准之前, 您将无法使用 AMS。

成功完成 RFC 后, AMS 操作会为您提供新的 IAM 用户和密码。然后按照以下步骤操作 :

1. 转到 AWS 管理控制台并使用提供的凭据登录。系统将要求您创建新密码。您还必须在登录时设置多因素身份验证 (MFA); 要了解有关设置的更多信息, [请参阅中的使用多因素身份验证 \(MFA\)](#)。
AWS
2. 在 AWS 管理控制台中, 更改为提供的 IAM 角色
(customer_**CustomerCode**_readonly_user_role)。
3. 打开 AMS Manage d Services 控制台。

Note

临时访问权限默认为六十天; 但是, 您可以联系您的 CSDM 申请延期 30 天。

使用堡垒访问实例

客户和 AMS 运营商对 AMS 管理的账户内资源的所有访问权限均受堡垒主机的使用限制。我们同时维护 Linux 和 Windows RDP 堡垒, 可供多账户着陆区 (MALZ) 和单账户着陆区 (SALZ) AMS Advanced 账户访问。

您的堡垒只能通过您的私人连接 (VPN 或 Direct Connect) DX 访问。除了防火墙以防止入站流量外, 还会定期按固定的时间表重新配置堡垒 (使用现有证书)。

Note

有关将文件移动到 EC2 实例的信息，请参阅[文件传输：将本地 Windows 或 MAC 电脑传输到 Linux 亚马逊 EC2](#)。

MALZ

您可以使用 Active Directory (AD) 凭据登录堡垒实例，从而访问您的账户实例。Amazon 使用位于外围网络 VPC (网络账户) 中的堡垒，而您则使用位于共享服务账户的客户堡垒子网中的客户堡垒。

最初加载 AMS 环境时，您有两个 SSH 堡垒和两个 RDP 堡垒，具体取决于您的选择。

SALZ

您可以使用 Active Directory (AD) 凭据登录堡垒实例，从而访问您的账户实例。AMS 使用位于外围网络子网中的堡垒，而您使用位于私有子网中的堡垒。

默认情况下，当您的账户初始登录时，您有两个 RDP 和两个 SSH 堡垒。

Note

作为单账户着陆区的一部分，AMS 提供 RDP (Windows) 和 SSH (Linux) 堡垒来访问您的堆栈；但是，您可以选择只要 RDP 堡垒还是只要 SSH 堡垒。要请求仅维护 RDP 或仅维护 SSH 堡垒，请提交服务请求。

要访问实例，您需要：

- 授予对堆栈的访问权限。要获得对堆栈的访问权限，请参阅[堆栈管理员访问权限 | 授予](#)或[堆栈只读访问权限 | 授予](#)。
- 您要访问的堆栈 ID，以便授予对实例的访问权限。要查找堆栈 ID，请参阅[在 AMS IDs 中查找堆栈](#)。
- 您要访问的实例 IP。要查找实例 IP，请参阅[在 AMS 中查找实例 IDs 或 IP 地址](#)。
- DNS 友好的堡垒名称或堡垒 IP。接下来将介绍如何使用 DNS 友好的堡垒名称以及如何查找堡垒 IP。

DNS 友好的堡垒名称

AWS Managed Services (AMS) 使用 DNS 友好的堡垒名称。

MALZ

对于多账户着陆区 (MALZ)，将在 AMS 管理的 Active Directory 的 FQDN 中为堡垒创建 DNS 记录。AMS 根据需要取代 Linux 和 Windows 的堡垒。例如，如果必须部署新的堡垒 AMI，堡垒 DNS 记录会动态更新以指向新的有效堡垒。

1. 要访问 SSH (Linux) 堡垒，请使用如下所示的 DNS 记录：`sshbastion(1-4).Your_Domain.com`

例如，域名为Your_Domain：

- `sshbastion1.Your_Domain.com`
- `sshbastion2.Your_Domain.com`
- `sshbastion3.Your_Domain.com`
- `sshbastion4.Your_Domain.com`

2. 要访问 RDP (Windows) 堡垒，请使用像这样的 DNS 记录：。`rdp-Username.Your_Domain.com`

例如，其中用户名是alextest、demobob、或，域是Your_Domain.com：

- `rdp-alex.Your_Domain.com`
- `rdp-test.Your_Domain.com`
- `rdp-demo.Your_Domain.com`
- `rdp-bob.Your_Domain.com`

SALZ

单账户着陆区 (SALZ) 可根据需要取代 Linux 和 Windows 堡垒。例如，如果必须部署新的堡垒 AMI，堡垒 DNS 记录会动态更新以指向新的有效堡垒。

1. 要访问 SSH (Linux) 堡垒，请使用如下所示的 DNS 记录：`sshbastion(1-4).AccountNumber.amazonaws.com.`

例如，账号在123456789012哪里：

- sshbastion1.A123456789012.amazonaws.com
- sshbastion2.A123456789012.amazonaws.com
- sshbastion3.A123456789012.amazonaws.com
- sshbastion4.A123456789012.amazonaws.com

2. 要访问 RDP (Windows) 堡垒，请使用像这样的 DNS 记录：。rdpbastion(1-4).ACCOUNT_NUMBER.amazonaws.com

例如，账号在123456789012哪里：

- rdpbastion1.A123456789012.amazonaws.com
- rdpbastion2.A123456789012.amazonaws.com
- rdpbastion3.A123456789012.amazonaws.com
- rdpbastion4.A123456789012.amazonaws.com

节省购买单账户着陆区 (SALZ) 堡垒的成本

AMS 在默认配置中提供了两个 SSH 堡垒和两个 RDP 堡垒供您连接您的 Amazon EC2 实例，并且还在服务操作的默认配置中部署了两个 DMZ 堡垒。默认情况下，堡垒使用 m4. 大型 Amazon EC2 实例。您可以选择将用于堡垒的 Amazon EC2 实例更改为 t3.small，这样可以节省成本。

如果您使用的是按需实例、竞价型实例或储蓄计划，则应考虑使用此功能并节省成本。如果您使用预留实例，请考虑使用 t3.small 实例是否可以降低成本。要更改实例类型，请使用您的 AMS 账户通过管理 | 高级堆栈组件 | EC2 实例堆栈 | 调整大小 (ct-15mazjj88xc69) CT 提交 RFC。

如有其他问题，或查看是否可以从此功能中受益，请联系您的云服务交付经理 (CSDM)。

使用堡垒 IP 地址

AMS 客户可以使用前面[DNS 友好的堡垒名称](#)描述的 SSH 和 RDP 堡垒，也可以使用堡垒 IP 地址。

要为您的账户查找堡垒 IP 地址（SSH 和 RDP），请执行以下操作：

1. 仅适用于多账户 landing zone：登录共享服务账户。
2. 打开 EC2 控制台并选择运行实例。

将打开“实例”页面。

3. 在顶部的筛选框中，输入 ssh-bastion 或 rdp-bastion。

在顶部的筛选框中，输入 customer-ssh 或 customer-rdp。

将显示您账户的 SSH and/or RDP 堡垒。

请注意，除了 SSH 堡垒外，您可能在列表中看到 AMS 外围网络堡垒，但这些堡垒不可用。

4. 选择 SSH 或 RDP 堡垒。如果你使用的是 Windows 计算机并想登录 Linux 实例，则可以使用 SSH 堡垒。如果你想登录 Windows 实例，你可以使用 RDP 堡垒。如果你使用的是 Linux 操作系统并想登录 Windows 实例，你可以通过 RDP 隧道使用 SSH 堡垒（这样你就可以访问 Windows 桌面）。要从 Linux 操作系统访问 Linux 实例，您需要使用 SSH 堡垒。

AMS 中的实例访问示例

这些示例说明了在通过 RFC 授予访问权限后，如何使用堡垒登录您的 AMS 账户中的实例。有关授予访问权限的信息，请参阅[请求实例访问权限](#)。

Note

有关将文件移动到 EC2 实例的信息，请参阅[文件传输：将本地 Windows 或 MAC 电脑传输到 Linux 亚马逊 EC2](#)。

所需数据：

- 堡垒 DNS 友好名称或 IP 地址：使用中所所述的 DNS 友好名称[DNS 友好的堡垒名称](#)或按中所所述查找堡垒 IP 地址。[使用堡垒 IP 地址](#)

Note

通过 Amazon A EC2 uto Scaling 组创建的亚马逊 EC2 实例将具有循环进出的 IP 地址，您必须使用亚马逊 EC2 控制台来查找该 IP 地址。

- 用户名（例如 `DOMAIN_FQDN\USERNAME`）和密码：帐户的凭据。`USERNAME` 必须是您的活动目录用户名。

请注意，可以使用 `username@customerdomain.com` 格式的用户名，但可能会给你的 PBIS 设置带来麻烦。

- 堆栈 IP 地址：通过查看您为启动堆栈而提交的 RFC 的运行输出来找到此地址，或者在亚马逊 EC2 控制台中查找亚马逊 EC2 实例 IP 地址。对于单个 Amazon EC2 实例，您还可以使用 AMS SKMS

命令 `ListStackSummaries` 查找堆栈 ID，然后 `GetStack` 找到堆栈 IP 地址。有关 AMS SKMS API 参考，请参阅 AWS Artifact 控制台中的“报告”选项卡。

根据需要访问堡垒 IP 地址（SSH 或 RDP），然后使用以下过程之一登录。

Note

RDP 堡垒只允许同时连接两个连接。因此，在最佳情况下，只有 4 个管理员能够同时连接到 Windows 堆栈。如果您需要更多的 RDP 连接，请参阅 [AMS 入门指南中的应用程序迁移/入门期间的 AMS 堡垒选项](#)。

从 Linux 计算机到 Linux

使用 SSH 连接到 SSH 堡垒，然后连接到 Linux 实例。

MALZ

有关友好堡垒名称的更多信息，请参阅 [DNS 堡垒](#)。

要连接到 Linux 实例，您必须先连接到 SSH 堡垒。

1. 打开 shell 窗口并输入：

```
ssh Domain_FQDN\\Username@SSH_bastion_name  
or SSH_bastion_IP
```

如果你的 domain_FQDN 是“corp.domain.com”，你的账号是“123456789123”，你的域名是“amazonaws.com”，你选择堡垒“4”，你的用户名是“”，那会是这样：JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. 使用您的公司活动目录凭据登录。
3. 当出现 Bash 提示时，使用 SSH 登录实例，然后输入：

```
ssh Domain_FQDN\\Username@Instance_IP
```

或者，你可以使用登录标志 (-l)：

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

有关友好堡垒名称的更多信息，请参阅 [DNS 堡垒](#)。

要连接到 Linux 实例，您必须先连接到 SSH 堡垒。

1. 打开 shell 窗口并输入：

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name  
or SSH_BASTION_IP
```

如果你的账号是 123456789123，你选择堡垒 4，你的用户名是：JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. 使用您的公司活动目录凭据登录。
3. 当出现 Bash 提示时，使用 SSH 登录实例，然后输入：

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

或者，你可以使用登录标志 (-l)：

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Linux 计算机到 Windows 实例

使用 SSH 隧道和 RDP 客户端从你的 Linux 计算机连接到 Windows 实例。

MALZ

此过程需要适用于 Linux 的远程桌面连接客户端；该示例使用 Microsoft 远程桌面（用于连接到 Windows 远程桌面服务的开源 UNIX 客户端）。Rdesktop 是另一种选择。

 Note

登录 Windows 实例的方式可能会因所使用的远程桌面客户端而异。

首先建立 SSH 隧道，然后登录。

有关友好堡垒名称的更多信息，请参阅[DNS 友好的堡垒名称](#)。

开始前的准备工作：

- 请求访问您要连接的实例；有关信息，请参阅[访问请求](#)。
- 选择一个友好的 DNS SSH 堡垒名称进行连接；例如：

```
sshbastion(1-4).Your_Domain
```

如果你的 domain_FQDN 是 “corp.domain.com”，你的 AMS 管理的 Your_Domain_Domain 是 “amazonaws.com”，你选择堡垒 “4”，你的用户名是 “”，那会是这样：JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- 查找您要连接的实例的 IP 地址；有关信息，请参阅[查找实例 ID 或 IP 地址](#)。
1. 通过 SSH 隧道设置 RDP，从 Linux 桌面到 Windows 实例。要使用正确的值发出ssh命令，有以下几种方法可以继续：
 - 在 Linux 外壳中，设置变量，然后输入 SSH 连接命令：

```
BASTION="sshbastion(1-4).Your_Domain"  
WINDOWS="Windows_Instance_Private_IP"  
AD="AD_Account_Number"  
USER="AD_Username"  
ssh -L 3389:$WINDOWS:3389 A$AD\\\\"$USER@$BASTION
```

例如，如果使用以下值：

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```



```
AD="ACORP_example"
```

```
USER="john.doe"
```

- 将变量值直接添加到ssh命令中。

无论哪种情况，呈现的请求都是这样（假设变量值相同）：

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. 任一：打开远程桌面客户端，输入环回地址和端口 127.0.0.1:3389，然后打开连接。

或者，从新的 Linux 桌面外壳登录到 Windows 实例。如果使用 RDesktop，则命令如下所示：

```
rdesktop 127.0.0.1:3389
```

Windows 实例的远程桌面窗口将显示在您的 Linux 桌面上。

Tip

如果远程桌面会话无法启动，请在步骤 1 中验证是否允许通过 shell 的端口 3389 通过 SSH 堡垒与 Windows 实例建立网络连接（适当替换 `private_ip_address_of_windows_instance`）：

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

成功：

```
nc 172.16.0.83 3389 -v -z
    Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp      0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

SALZ

单账户登录区域的此过程需要适用于 Linux 的远程桌面连接客户端；该示例使用 Microsoft 远程桌面（用于连接到 Windows 远程桌面服务的开源 UNIX 客户端）。Rdesktop 是另一种选择。

 Note

登录 Windows 实例的方式可能会因所使用的远程桌面客户端而异。

首先建立 SSH 隧道，然后登录。

有关友好堡垒名称的更多信息，请参阅[DNS 友好的堡垒名称](#)。

开始前的准备工作：

- 请求访问您要连接的实例；有关信息，请参阅[访问请求](#)。
- 选择一个友好的 DNS SSH 堡垒名称进行连接；例如：

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

如果你的账号是 123456789123 然后你选择堡垒 4，那会是这样：

```
sshbastion4.A123456789123.amazonaws.com
```

- 查找您要连接的实例的 IP 地址；有关信息，请参阅[查找实例 ID 或 IP 地址](#)。
1. 通过 SSH 隧道设置 RDP，从 Linux 桌面到 Windows 实例。要使用正确的值发出ssh命令，有以下几种方法可以继续：
 - 在 Linux 外壳中，设置变量，然后输入 SSH 连接命令：

```
BASTION="sshbastion(1-4).AMSAccountNumber.amazonaws.com"  
WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"  
AD="AD_ACCOUNT_NUMBER"  
USER="AD_USERNAME"  
ssh -L 3389:$WINDOWS:3389 A$AD\\\\"$USER@$BASTION
```

例如，如果使用以下值：

```
BASTION="sshbastion4.A123456789123.amazonaws.com"
```

```
WINDOWS="172.16.3.254"
```

```
AD="ACORP_example"
```

```
USER="john.doe"
```

- 将变量值直接添加到ssh命令中。

无论哪种情况，呈现的请求都是这样（假设变量值相同）：

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. 任一：打开远程桌面客户端，输入环回地址和端口 127.0.0.1:3389，然后打开连接。

或者，从新的 Linux 桌面外壳登录到 Windows 实例。如果使用 RDesktop，则命令如下所示：

```
rdesktop 127.0.0.1:3389
```

Windows 实例的远程桌面窗口将显示在您的 Linux 桌面上。

Tip

如果远程桌面会话无法启动，请在步骤 1 中验证是否允许通过 shell 的端口 3389 通过 SSH 堡垒与 Windows 实例建立网络连接（适当替换 `private_ip_address_of_windows_instance`）：

```
nc private_ip_address_of_windows_instance 3389 -v -z
```

成功：

```
nc 172.16.0.83 3389 -v -z
Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
netstat -anvp | grep 3389
tcp    0      0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

Windows 计算机到 Windows 实例

使用 Windows 远程桌面连接客户端从你的 Windows 计算机连接到 Windows 实例。

MALZ

有关友好堡垒名称的更多信息，请参阅[DNS 友好的堡垒名称](#)。

1. 打开远程桌面连接程序（标准的 Windows 程序），然后在“主机名”字段中输入 Windows 堡垒的友好 DNS 名称。
2. 选择连接。远程桌面连接尝试与堡垒建立 RDP 连接。

如果成功，则会打开一个凭据对话框。要获得访问权限，请使用您的公司 Active Directory 凭据，就像使用 Windows 实例一样。

3. 在堡垒上打开远程桌面连接程序，输入要连接的 Windows 实例的 IP 地址（例如 10.0.0.100），然后选择 Connect。在连接到 Windows 实例之前，再次需要您的公司 Active Directory 凭据。

SALZ

有关友好堡垒名称的更多信息，请参阅[DNS 友好的堡垒名称](#)。

1. 打开远程桌面连接程序（标准的 Windows 程序），然后在主机名字段中输入 Windows 堡垒的友好 DNS 名称；例如 `rdpbastion(1-4).AAMSAccountNumber.amazonaws.com`，如果你的账号是 123456789123 并且你选择了堡垒 4，则该名称将如下所示。`rdpbastion4.A123456789123.amazonaws.com`
2. 选择连接。远程桌面连接尝试与堡垒建立 RDP 连接。

如果成功，则会打开一个凭据对话框。要获得访问权限，请使用您的公司 Active Directory 凭据，就像使用 Windows 实例一样。

3. 在堡垒上打开远程桌面连接程序，输入要连接的 Windows 实例的 IP 地址（例如 10.0.0.100），然后选择 Connect。在连接到 Windows 实例之前，再次需要您的公司 Active Directory 凭据。

Windows 计算机到 Linux 实例

要从 Windows 环境中对 SSH 堡垒进行 RDP，请按照以下步骤操作。

MALZ

开始前的准备工作：

- 请求访问您要连接的实例；有关信息，请参阅[访问请求](#)。
- 选择一个友好的 DNS SSH 堡垒名称进行连接；例如：

```
sshbastion(1-4).YOUR_DOMAIN
```

如果 YOUR_DOMAIN 是 myamsaddomain.com” 然后你选择堡垒 4，那会是这样：

```
sshbastion4.myamsaddomain.com
```

- 查找您要连接的实例的 IP 地址；有关信息，请参阅[查找实例 ID 或 IP 地址](#)。

要从 Windows 计算机连接到 Linux 实例，必须先连接到 SSH 堡垒。

使用原生 Windows [OpenSSH 客户端](#)或者在本地计算机上安装 P [uTTY](#)。要了解有关 OpenSSH 的更多信息，请参阅 Windows 中的 Op [en](#) SSH。

1. 使用本机 Windows 或打开 PuTTY 并输入 SSH 堡垒的主机名或 SSH 堡垒的 IP 地址。例如，10.65.2.214 (22 是用于 SSH 的端口；默认情况下将设置该端口)。
2. OpenSSH 或 PuTTY 尝试通过 SSH 连接到堡垒并打开外壳窗口。
3. 使用您的公司 Active Directory 凭据来获得访问权限，就像使用 RDP 主机一样。
4. 当出现 Bash 提示时，使用 SSH 进入实例。输入：

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

开始前的准备工作：

- 请求访问您要连接的实例；有关信息，请参阅[访问请求](#)。
- 选择一个友好的 DNS SSH 堡垒名称进行连接；例如：

```
sshbastion(1-4).AMSAccountNumber.amazonaws.com
```

如果你的账号是 123456789123 然后你选择堡垒 4，那会是这样：

```
sshbastion4.A123456789123.amazonaws.com
```

- 查找您要连接的实例的 IP 地址；有关信息，请参阅[查找实例 ID 或 IP 地址](#)。

要从 Windows 计算机连接到 Linux 实例，必须先连接到 SSH 堡垒。

使用原生 Windows [OpenSSH 客户端](#)或者在本地计算机上安装 P [uTTY](#)。要了解有关 OpenSSH 的更多信息，请参阅 Windows 中的 Op [en](#) SSH。

1. 使用本机 Windows 或打开 PuTTY 并输入 SSH 堡垒的主机名或 SSH 堡垒的 IP 地址。例如，10.65.2.214 (22 是用于 SSH 的端口；默认情况下将设置该端口)。
2. OpenSSH 或 PuTTY 尝试通过 SSH 连接到堡垒并打开外壳窗口。
3. 使用您的公司 Active Directory 凭据来获得访问权限，就像使用 RDP 主机一样。
4. 当出现 Bash 提示时，使用 SSH 进入实例。输入：

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

AMS 账户中基于团队或角色的访问控制

场景：两个应用程序组 A 和 B 分别使用一个 AMS 账户来管理他们的应用程序“AA”和“BB”。团队 A 只想访问应用程序“AA”的资源，而团队 B 只想访问应用程序“BB”的资源。我该如何设置？

使用他们的 ITSM 工具实施基于团队的访问控制 (TBAC)。例如，您可以使用 AMS ServiceNow 连接器应用程序与 AMS 集成 APIs。请联系您的 CSDM，获取有关此实施的高级指导。

AMS Advanced 中的自动实例配置

AMS Advanced 自动实例配置服务每天运行，并自动扫描和更新托管 EC2 实例上的 SSM、CloudWatch 代理和配置文件。根据需要，更新适用于：

- SSM 和代理 CloudWatch
- CloudWatch 配置文件

这些更新允许 AMS 访问您的 AMS 托管 EC2 实例，并将您的实例配置为发出相应的[日志](#)和指标。

主题

- [自动配置实例的先决条件](#)
- [SSM 代理自动安装](#)
- [自动更改](#)

自动配置实例的先决条件

对于使用变更管理部署实例的 AMS Advanced 客户，必须满足以下先决条件：

- SSM 代理已安装并处于托管状态。
- 该实例被标记为托管实例。（`aws:cloudformation:stack-name` 标签的值以 `stack-` 或开头 `sc-`。）

如果您的实例上尚未安装 SSM 代理，则可以使用 AMS SSM 代理自动安装功能进行安装。有关更多信息，请参阅 [SSM 代理自动安装](#)。

或者，您可以手动安装 SSM 代理。有关更多信息，请参阅下列内容：

- Linux：在 Linux [EC2 实例上手动安装 SSM 代理——AWS Systems Manager](#)
- Windows：在 Windows [服务器的 EC2 实例上手动安装 SSM 代理——AWS Systems Manager](#)

有关 SSM 代理的更多信息，请参阅 AWS 文档[使用 SSM 代理](#)。

SSM 代理自动安装

要让 AMS 管理您的亚马逊弹性计算云 (Amazon EC2) 实例，您必须在每个实例上安装 AWS Systems Manager SSM 代理。如果您的实例未安装 SSM 代理，则可以使用 AMS SSM 代理自动安装功能。

Note

- 此功能仅适用于不在 Auto Scaling 组中且运行 AMS 支持的 Linux 操作系统的 EC2 实例。
- 默认情况下，AMS SSM 代理自动安装功能处于禁用状态。要启用它，请联系您的 CA 或 CSDM。

使用 SSM 代理的先决条件

- 确保与目标实例关联的实例配置文件具有以下策略之一（或许可名单中的等效权限）：
 - Amazon SSMManaged EC2 InstanceDefaultPolicy
 - Amazon SSMManaged InstanceCore
- 确保没有明确拒绝上述策略中 AWS Organizations 列出的权限的服务控制策略。

有关更多信息，请参阅[配置 Systems Manager 所需的实例权限](#)。

- 要阻止出站流量，请确保在目标实例所在的 VPC 上启用以下接口终端节点（相应地替换 URL 中的“区域”）：
 - ssm.<region>.amazonaws.com
 - ssmmessages.<region>.amazonaws.com
 - ec2messages.<region>.amazonaws.co

有关更多信息，请参阅[使用适用于 Systems Manager 的 VPC 终端节点来提高 EC2 实例的安全性](#)。

有关启用托管节点可用性或对其进行故障排除的一般提示，请参阅[解决方案 2：验证是否已为实例指定了 IAM 实例配置文件（仅限 EC2 实例）](#)。

Note

作为自动安装过程的一部分，AMS 会停止和启动每个实例。当实例停止时，存储在实例存储卷中的数据 and 存储在 RAM 上的数据都将丢失。有关更多信息，请参阅[停止实例时会发生什么](#)。

请求在您的实例上自动安装 SSM 代理

如果您的账户已加入 AMS Accelerate 补丁插件，请为实例配置补丁维护窗口 (MW)。需要一个能正常运行的 SSM 代理才能完成修补过程。如果实例上缺少 SSM 代理，AMS 会尝试在补丁维护时段内自动安装该代理。

Note

作为自动安装过程的一部分，AMS 会停止和启动每个实例。当实例停止时，存储在实例存储卷中的数据和存储在 RAM 上的数据都将丢失。有关更多信息，请参阅[停止实例时会发生什么](#)。

SSM 代理自动安装的工作原理

AMS 使用 EC2 用户数据在您的实例上运行安装脚本。要添加用户数据脚本并在您的实例上运行该脚本，AMS 必须停止并启动每个实例。

如果您的实例已有用户数据脚本，则 AMS 将在自动安装过程中完成以下步骤：

1. 创建现有用户数据脚本的备份。
2. 用 SSM 代理安装脚本替换现有的用户数据脚本。
3. 重启实例以安装 SSM 代理。
4. 停止实例并恢复原始脚本。
5. 使用原始脚本重启实例。

自动更改

AMS Advanced 自动实例配置服务可根据需要对您的 EC2 实例进行更改。

发生了什么变化：

- [在 Linux 实例上自动更新代码](#)
- [在 Linux 实例上自动更新 PBIS](#)
- [自动更新 SSM 和 CloudWatch 代理的最低版本](#)
- [CloudWatch 配置文件，更新详细信息](#)
- [自动配置的日志](#)

在 Linux 实例上自动更新代码

AMS 会自动更新 Linux 实例上的实例代码。这有助于全面提高 AMS 组件和环境的运行稳定性和安全性。

常见问题：

Linux 上的实例化代码 (OIC) 中包含什么？

OIC 包括 `ams-toolkit` 软件包以及一些配置文件和 `cron` 作业。AMS 需要这些文件和软件包进行集成（Active Directory CloudFormation 和其他依赖项）。我们会将这些文件预先烘焙到 AMS 提供的文件中，AMIs 或者在工作负载摄取期间安装到您的实例上。

AMS 何时会更新 OIC？

当我们发布包含错误修复或其他改进的新版本时，AMS 会更新 OIC。检查 OIC 版本和更新的工作流程每天运行。

在 Linux 实例上自动更新 PBIS

AMS 使用 Power Broker 身份服务 (PBIS) 模块将 Linux 实例加入 AMS 管理的 Active Directory。

AMS 会自动更新 Linux 实例上的 PBIS。

常见问题解答：

AMS 何时会更新 PBIS？

AMS 在重启时开启 PBIS 更新。如果有新的 PBIS 版本可用，AMS 将在下次实例重启时尝试安装新版本。

能否关闭 PBIS 更新？

您可以在实例或账户级别关闭 PBIS 更新：

- 账户级别：在 SSM 参数存储中创建参数：名称：`/ams/skip-pbis-update`，值：`true`（任何情况）。

Note

实例配置文件必须具有读取 SSM 参数的权限。如果缺少该标志，则默认行为是运行更新。

- 实例级别：
 - 基于标签：向实例添加以下标签：Key:skip_pbis_update , Value:true (任何情况)。
 - Config 文件：在/opt/aws/ams/etc/ams.conf.d/state.ini文件中添加以下标志：skip_pbis_update = true。

Note

标签的优先级高于 SSM 参数。您可以通过参数在账户级别关闭 PBIS 更新，但可以通过添加标签Key:skip_pbis_update来关闭单个 (或多个) 实例的 PBIS 更新。Value: false

要配置上述任何选项，请按照 AMS 环境中的标准变更管理流程进行操作。

自动更新 SSM 和 CloudWatch 代理的最低版本

AMS Advanced 最低版本 (SSM 或 CloudWatch 代理) 是经过 AMS 服务团队测试并预先批准适用于您的操作系统的版本。我们会尽量保持积极主动并运行最新的稳定兼容版本，因此版本号会随着时间的推移而变化。您可以通过向 AMS 提出服务请求来找到当前的最低版本。

• SSM 代理管理

Amazon SSM 代理负责在实例上运行远程命令。实例配置自动化可确保 SSM 代理运行最低版本。

• 云监视代理管理

Amazon CloudWatch 代理负责发布操作系统日志和指标。自动实例配置执行以下操作：

- 如果需要，禁用旧版 CloudWatch 日志代理并将配置迁移到新的统一代理 CloudWatch
- 如果您的实例运行的是旧版 CloudWatch 日志代理，则自动实例配置会禁用旧版 CloudWatch 日志代理服务并将其配置迁移到统一 CloudWatch 代理。
- 自定义您的 CloudWatch 配置以生成相应的日志和指标。

受影响的文件和目录：

- Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configs\
- Linux
 - /opt/aws/amazon-cloudwatch-agent/etc/

- /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/
- /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

CloudWatch 配置文件，更新详细信息

我们从以下 CloudWatch 目录（参见[推荐目录](#)）中读取您的自定义 CloudWatch 配置（仅限 JSON），并将它们与标准 AMS CloudWatch 配置合并：

- CloudWatch 文件
 - 在实例上：
 - Windows
 - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configs\
 - %ProgramFiles%\ 模块WindowsPowerShell\ AWSManaged 服务.Logging.Utilities\ Files\ Config.json
 - Linux
 - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
 - 在亚马逊 S3 上：
 - Windows:
 - https://ams-configuration-artifacts-*REGION_NAME*.s3. *REGION_NAME*.amazonaws. com/ configurations/cloudwatch/latest/windows-cloudwatch-config.j
 - Linux :
 - https://ams-configuration-artifacts-*REGION_NAME*.s3. *REGION_NAME*.amazonaws. com/ configurations/cloudwatch/latest/linux-cloudwatch-config.j

自动配置的日志

我们将您的实例配置为写入以下日志。

- Windows:
 - Amazon SSMAgent 日志
 - AmazonCloudWatchAgentLog
 - Amazon SSMError 日志
 - AmazonCloudFormationLog

- ApplicationEventLog
- EC2ConfigServiceEventLog
- MicrosoftWindowsAppLockerEXEAndDLLEvent日志
- MicrosoftWindowsAppLockerMSIAndScriptEventLog
- MicrosoftWindowsGroupPolicyOperationalEventLog
- SecurityEventLog
- SystemEventLog
- Linux :
 - /var/log/amazon/ssm/amazon-ssm-agent.log
 - /var/log/amazon/ssm/errors.log
 - /var/log/audit/audit.log
 - /var/log/cloud-init-output.log
 - /var/log/cloud-init.log
 - /var/log/cron
 - /var/log/dpkg.log
 - /var/log/maillog
 - /var/log/messages
 - /var/log/secure
 - /var/log/spooler
 - /var/log/syslog
 - /var/log/yum.log
 - /var/log/zypper.log

AMS 中的监控和事件管理

主题

- [什么是监控？](#)
- [AMS 监控系统监控什么？](#)
- [监控的工作原理](#)
- [查看 AMS 账户的监控配置](#)
- [更改 AMS 账户的监控配置](#)
- [AMS 中的应用程序感知事件通知](#)
- [OpsCenter 在 AMS 中使用](#)
- [来自 AMS 的警报通知](#)
- [在 AMS 中创建其他 CloudWatch 警报](#)
- [在 AMS 中创建自定义 CloudWatch 指标和警报](#)
- [在 AMS 中使用适用于 .Net 和 SQL 服务器的 CloudWatch 应用程序见解](#)
- [在 AMS 中使用亚马逊 EventBridge 托管规则](#)
- [AMS 中值得信赖的修正者](#)

AWS Managed Services (AMS) 监控系统会监控您的 AMS 资源是否存在故障、性能下降和安全问题。AMS 监控系统依赖于 AWS 服务，例如亚马逊 CloudWatch (CloudWatch)、亚马逊 GuardDuty、亚马逊 Macie 和。AWS Health除了监控系统外，AMS 还在亚马逊弹性计算云 (Amazon EC2) 实例上部署 TrendMicro DeepSecurity 以防范恶意软件。有关端点安全 (EPS) 默认值的信息，请参阅[端点安全 \(EPS\)](#)。

AMS 监控具有以下好处：

- 监控基准，即使您没有为托管账户配置任何其他监控，也能获得默认的保护级别。有关信息，请参阅[来自 AMS 基线监测的警报](#)。
- 调查警报，以确定适当的措施。例如，如果 GuardDuty 发现活动表明有人企图对某个 Amazon EC2 实例进行暴力攻击，AMS 就会分析 VPC 流日志以了解该活动的起源和背景。
- 尽可能修复警报，以防止或减少对应用程序的影响。例如，如果您使用的是独立的 Amazon EC2 实例，但该实例未通过系统运行状况检查，AMS 会尝试通过停止并重启该实例来恢复该实例。有关更多信息，请参阅[AMS 自动修复警报](#)。

- 使用可透明显示处于活动状态和之前已解决的警报 OpsCenter。例如，如果您的 Amazon EC2 实例的 CPU 使用率意外偏高，则可以请求访问 AWS Systems Manager 控制台（包括访问 OpsCenter 控制台），然后 OpsItem 直接在 OpsCenter 控制台中查看。

什么是监控？

AMS 监控系统会监控您的 AWS 资源是否存在故障、性能下降和安全问题。作为托管账户，AMS 为适用 AWS 资源配置和部署警报，对其进行监控，并在适用时执行补救。

AMS 监控系统根据您账户中的监控配置生成警报。账户的监控配置是指账户中用于创建警报的所有资源参数；有关资源参数的信息，请参阅[来自 AMS 基线监测的警报](#)。账户的监控配置包括 CloudWatch 警报定义和 CloudWatch 生成警报（警报或事件）的事件规则。

基准监控配置是 AMS 整理的一组警报定义 ([来自 AMS 基线监测的警报](#))，用于监控您的托管账户中的资源。由于您要求进行更改，账户的监控配置可能与基准配置不同。

账户中配置的基准监控生成的即将发生的、正在进行的、即将出现的或潜在的故障、性能下降或安全问题的通知称为警报。警报的示例包括亚马逊 CloudWatch 警报、亚马逊 CloudWatch 事件、事件或来自 Amazon 等 AWS 服务的发现 GuardDuty，以及趋势科技深度安全服务器深度安全防护系统提供的事件或警报。

来自安全相关的 AWS 服务（例如亚马逊 GuardDuty、Amazon Macie 或趋势科技趋势科技深度安全防护系统）的警报被称为安全警报，以区别于其他类型的警报。

AMS 监控具有以下好处：

- 能够自定义基准资源警报以满足您的要求。
- 尽可能自动修复警报，以防止或减少对应用程序的影响。例如，如果您使用的是独立的 Amazon EC2 实例，但该实例未通过系统运行状况检查，AMS 会尝试通过停止并重启该实例来恢复该实例。有关更多信息，请参阅[AMS 自动修复警报](#)。
- 使用可透明显示处于活动状态和之前已解决的警报 OpsCenter。例如，如果您在某个 Amazon EC2 实例上的 CPU 使用率异常高，则可以请求访问 AWS Systems Manager 控制台（包括访问 OpsCenter 控制台），然后 OpsItem 直接在 OpsCenter 控制台中查看。
- 调查警报以确定适当的操作。
- 根据您的账户和支持的 AWS 服务中的配置生成的警报。账户的监控配置是指账户中创建警报的所有资源参数。账户的监控配置包括 CloudWatch 警报定义和生成警报 EventBridge（警报或 CloudWatch 事件）（以前称为事件）。有关资源参数的更多信息，请参阅[来自 AMS 基线监测的警报](#)。

- 关于账户中配置的基准监控所产生的即将发生的、持续的、消退的或潜在的故障、性能下降或安全问题的通知（称为警报）。警报的示例包括 CloudWatch 警报、事件或来自 AWS 服务的发现，例如 GuardDuty 或 AWS Health。

AMS 监控系统监控什么？

为了与 AWS Managed Services (AMS) 共享服务责任模式保持一致，AMS 监控系统会监控您的 AWS 基础设施。有关 AMS 中基线监控的详细信息，包括监控的 AWS 资源和每种资源的警报类型，请参阅[来自 AMS 基线监测的警报](#)。对于 Amazon EC2 实例，AMS 监控操作系统并根据 CPU 利用率和根卷使用率等操作系统指标提供基准监控。

我们建议使用针对您的应用程序量身定制的 AWS 服务来补充 AMS 监控和额外监控。有关可用性监控的指导，请参阅本白皮书《[可靠性支柱](#)》中的“监控和警报”部分。您可以根据自己的运营需求配置自己的监控；在[AMS 中创建其他 CloudWatch 警报](#)和中讨论了如何执行此操作在[AMS 中创建自定义 CloudWatch 指标和警报](#)。

单账户登录区主动监控 AMS 中的 Active Directory 信任

AMS 单账户登录区 (SALZ) 监控您的 AMS 托管账户中的托管活动目录 (AD) 与公司域之间的单向信任状态。与托管 AD 的单向信任对于访问请求和实例登录请求至关重要。通过这种新的监控功能，AMS 现在可以主动响应与信任相关的问题，并缩短了检测访问相关事件的平均时间。

此功能将在您的 AWS Managed Services (AMS) 账户中自动启用。

对成本的影响很小。该功能对一个信任使用四个 AWS CloudWatch 指标和两个 AWS CloudWatch 警报。

监控的工作原理

参见以下有关 AWS Managed Services (AMS) 监控架构的图片。

下图简要概述了 AMS 多账户着陆区和 AMS 单账户着陆区监控工作流程。

- 生成：在账户注册时，AMS 会为您在托管账户中创建的所有资源配置基准监控 CloudWatch（（CW）警报和 CW 事件规则的组合）。当触发 CW 警报或生成 CW 事件时，基准监控配置会生成警报。
- 聚合：

- 多账户登录区：警报由您在应用程序和核心组织部门账户中的资源生成，并通过安全帐户将警报发送到 AMS 监控系统。
- 单账户登录区：您的资源生成的所有警报都将通过将它们定向到账户中的 SNS 主题来发送到 AMS 监控系统。
- 您还可以配置 AMS 如何将 EC2 警报分组在一起。AMS 要么将与同一 EC2 实例相关的所有警报分组为单个事件，要么根据您的偏好为每个警报创建一个事件。您可以随时与云服务交付经理或云架构师合作更改此配置。无论您使用的是多账户着陆区还是单账户着陆区，其运作方式都是一样的。
- 处理：AMS 分析警报并根据其潜在影响进行处理。警报按下文所述进行处理。
- 具有已知客户影响的警报：这些警报会导致创建新的事件报告，AMS 遵循事件管理流程；有关事件管理的信息，请参阅[AMS 事件响应](#)。

警报示例：Amazon EC2 实例未通过系统运行状况检查，AMS 尝试通过停止并重启实例来恢复该实例。

- 对客户影响不确定的警报：对于这些类型的警报，AMS 会发送事件报告，在许多情况下，要求您在 AMS 采取行动之前验证影响。但是，如果与基础设施相关的检查通过，则 AMS 不会向您发送事件报告。

例如：Amazon EC2 实例上 CPU 使用率超过 85% 且持续时间超过 10 分钟的警报不能立即归类为事件，因为根据使用情况，可能会出现这种行为。在此示例中，AMS Automation 对资源执行与基础设施相关的检查。如果这些检查通过，即使 CPU 使用率超过 99%，AMS 也不会发送警报通知。如果 Automation 检测到资源上与基础设施相关的检查失败，则 AMS 会发送警报通知并检查是否需要缓解措施。本节将详细讨论警报通知。AMS 在通知中提供了缓解选项。当您回复确认警报为事件的通知时，AMS 会创建新的事件报告，AMS 事件管理流程随即开始。如果服务通知收到“对客户没有影响”的响应，或者在三天内完全没有回复，则会标记为已解决，相应的警报被标记为已解决。

- 不影响客户的警报：如果 AMS 在评估后确定该警报对客户没有影响，则该警报将关闭。

例如，AWS Health 通知需要替换的 EC2 实例，但该实例此后已终止。

EC2 实例分组通知

您可以将 AMS 监控配置为将来自同一 EC2 实例的警报组合成单个事件。您的云服务交付经理或云架构师可以为您进行配置。您可以为每个 AMS 管理的账户配置四个参数。

1. 范围：选择账户范围或基于标签的范围。

- 要指定适用于该账户中每个 EC2 实例的配置，请选择范围 = 账户范围。
 - 要指定仅适用于该账户中带有特定标签的 EC2 实例的配置，请选择 scope = based tag。
2. 分组规则：选择经典或实例。
- 要为账户中的每个资源配置实例级分组，请选择范围 = 账户范围和分组规则 = 实例。
 - 要将账户中的特定资源配置为使用实例级别分组，请标记这些实例，然后选择范围 = 基于标签和分组规则 = 实例级别。
 - 要不对账户中的警报使用实例分组，请选择分组规则 = classic。
3. 参与选项：选择“无”、“仅限报告”或“默认”。
- 要使 AMS 在配置处于活动状态时不创建事件或自动处理来自这些资源的警报，请选择“无”。
 - 要让 AMS 在配置处于活动状态时不创建事件或自动处理来自这些资源的警报，也不要运行自动修复 Systems Manager 文档，但要在报告中包含这些事件的记录，请选择仅报告。如果您想减少与之互动的事件支持案例数量，并且某些资源中的某些事件（例如非生产账户中的事件）不需要立即关注，这可能会很有用。
 - 要让 AMS 处理您的警报、运行自动化程序并在需要时创建事件案例，请选择默认。
4. 之后解决：选择 24 小时、48 小时或 72 小时。最后，配置何时自动关闭事件案例。如果从上次案例对应的时间达到配置的“解决后解决”值，则事件将关闭。

警报通知

作为警报处理的一部分，AWS Managed Services (AMS) 会根据影响分析创建事件，并在确定影响后启动事件管理流程进行补救。如果无法确定影响，AMS 会通过服务通知向与您的账户关联的电子邮件地址发送提醒通知。在某些情况下，不会发送此警报通知。例如，如果与基础设施相关的检查通过 CPU 使用率高警报，则不会向您发送警报通知。有关更多信息，请参阅中有关警报处理过程的 AMS 监控架构图[监控的工作原理](#)。

基于标签的警报通知

使用标签将资源的警报通知发送到不同的电子邮件地址。最佳做法是使用基于标签的提醒通知，因为当多个开发者团队使用同一个账号时，发送到单个电子邮件地址的通知可能会造成混乱。基于标签的警报通知不受您选择的[EC2 实例分组通知](#)设置的影响。

使用基于标签的警报通知，您可以：

- 向特定的电子邮件地址发送警报：使用标记具有必须发送到特定电子邮件地址的警报的key = OwnerTeamEmail资源value = **EMAIL_ADDRESS**。

- 向多个电子邮件地址发送警报：要使用多个电子邮件地址，请指定以逗号分隔的值列表。
例如 `key = OwnerTeamEmail`、`value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`。值字段的字符总数不能超过 260。
- 使用自定义标签密钥：要使用自定义标签密钥，请在电子邮件中向您的 CSDM 提供自定义标签密钥名称，明确表示同意为基于标签的通信激活自动通知。最佳做法是对所有实例和资源的联系人标签使用相同的标记策略。

Note

键值 `OwnerTeamEmail` 不必是驼峰大小写。但是，标签区分大小写，最佳做法是使用推荐的格式。

必须完整指定电子邮件地址，并用“at 符号” (@) 将本地部分与域名分开。无效电子邮件地址

示例：`Team.AppATabc.xyz` 或 `john.doe`。有关标记策略的一般指导，请参阅 [标记资源](#)。

[AWS](#) 不要在标签中添加个人身份信息 (PII)。尽可能使用通讯组列表或别名。

以下亚马逊服务的资源支持基于标签的警报通知：EC2、弹性块存储 (EBS)、弹性负载平衡 (ELB)、应用程序负载均衡器 (ALB)、网络负载均衡器、关系数据库服务 (RDS) OpenSearch、弹性文件系统 (EFS) 和 VPN。FSx Site-to-Site

查看 AMS 账户的监控配置

您可以查看账户监控配置的两个关键部分：

- CloudWatch 警报：您可以通过进入 CloudWatch 控制台并选择感兴趣的不同服务来查看账户中的所有 CW 警报。
- CloudWatch 活动：
 - 多账户着陆区：CloudWatch 通过使用字符串“ams-”筛选所有 CW 事件规则，可以找到账户中监控的事件。
 - 单账户着陆区：CloudWatch 通过使用字符串“mc-”筛选所有 CW 事件规则，可以找到账户中监控的事件。

更改 AMS 账户的监控配置

您可以更改 Amazon EC2 资源的基准监控配置。有关可以配置的警报，请参阅 [来自 AMS 基线监测的警报](#)。您可以更改基准监控器的警报定义、警报目的地或选择退出警报通知，以使警报满足应用程序的

操作要求。您可以通过提交包含以下详细信息的管理 | 其他 | 其他 | 更新 CT (ct-0xdawir96cy7k) 来申请上述任何或全部更改。

- 实例 IDs [可选，如果未提及，则账户中的所有实例都在范围内]
- CloudWatch 指标名称，例如 CPU 利用率/交换可用率/ IOwait
- 目标-电子邮件 ID /短信的电话号码/SNS 主题

要详细了解您可以在基准监控配置中请求的更改类型，请参阅 [Amazon CloudWatch 文档](#)。

AMS 中的应用程序感知事件通知

使用应用程序感知型自动事件通知，为 AMS 代表您创建的支持案例自定义您的沟通体验。当您使用此功能时，AMS 会从中检索自定义工作负载首选项，使用有关您的应用程序的元数据[AWS Service Catalog AppRegistry](#)来丰富您的 AMS 事件通信，并自定义 AMS 代表您创建的支持案例的严重性。要使用此功能，您必须先在 AMS 账户 AWS Service Catalog AppRegistry 中进行配置。

要了解有关 AMS 监控默认值的更多信息，请参阅[AMS 中的监控和事件管理](#)。

AppRegistry 在您的 AMS 账户中配置并创建应用程序

您的 AMS 账户可在自助配置 (SSP) 模式下使用该 AppRegistry 服务。有关如何请求访问权限的说明，请参阅[使用 AMS SSP AWS Service Catalog AppRegistry 在您的 AMS 账户中进行配置](#)。

置备后 AppRegistry，使用以下方法之一创建应用程序：

1. AWS 控制台：要了解有关 AppRegistry 通过 AWS 控制台创建应用程序的更多信息，请参阅AWS Service Catalog AppRegistry 管理员指南中的[创建应用程序](#)。
2. CloudFormation：您可以像定义任何其他资源一样定义 AppRegistry 应用程序。有关更多信息，请参阅《CloudFormation 用户指南》中的 [AWS Service Catalog AppRegistry 资源类型参考](#)。

创建标签以丰富案例

您必须先为应用程序添加标签，AMS 才能访问应用程序元数据。下表列出了所需的标签。

标签密钥	标签值
ams 托管	true

为您的应用程序自定义 AMS 支持案例的严重性

您可以通过指定您的应用程序对组织的重要程度来自定义 AMS 创建的支持案例的严重程度。此设置由中与您的应用程序关联的属性组控制 AppRegistry。属性组名称的名称必须符合以下模式：

```
AMS.<ApplicationName>.CommunicationOptions
```

在上述模式中，ApplicationName必须与创建应用程序 AppRegistry 时使用的名称相匹配。

示例内容：

```
{
  "SchemaVersion": "1.0",
  "Criticality": "low"
}
```

SchemaVersion

这决定了您正在使用的架构版本以及可供使用的功能子集。

架构版本	功能
1.0	根据重要性值自定义支持案例的严重性

临界性

此应用程序的重要性决定了 AMS 自动化系统创建的支持案例的严重性。

有效值：

```
low|normal|high|urgent|critical
```

有关严重性级别的更多信息，请参阅 AWS 支持 API 参考[SeverityLevel](#)中的。

必需：是

查看所需权限

要使用此功能，AMS 需要访问以下 AWS Identity and Access Management 权限：

- 我是 : ListRoleTags
- 我是 : ListUserTags
- 资源组标记 api: GetResources
- servicecatalog-appregistry: GetApplication
- servicecatalog-appregistry: ListAssociatedAttributeGroups
- servicecatalog-appregistry: GetAttributeGroup

Important

确保没有拒绝上述操作的 IAM 策略或服务控制策略 (SCP)。

API 调用由ams-access-admin角色发出。以下是您可能看到的内容的示例：

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

OpsCenter 在 AMS 中使用

AWS Managed Services (AMS) 运营团队[AWS Systems Manager OpsCenter](#)用于诊断和修复与您的资源相关的许多警报。

使用 OpsCenter 可以缩短解决问题的平均时间 (MTTR)，同时提供对 AMS 运营团队操作队列的透明视图。

借 OpsCenter 助，除了自动化解决方案外，AMS 还为您提供了操作工作项目（也称为 [OpsItems](#)AMS 团队正在积极处理的运营工作项目）的透明视图。

要了解 OpsCenter 和的更多信息 OpsItems，请参阅[AWS Systems Manager OpsCenter](#)。有关访问 AWS 管理控制台的信息，请参阅[使用 AWS 管理控制台](#)。从 AWS 管理控制台中，您可以导航到 AWS Systems Manager 控制台 OpsCenter；要了解更多信息，请参阅[AWS Systems Manager 会话管理器](#)。OpsCenter 还提供了可供您使用的 API；有关信息，请参阅[了解更多信息 OpsCenter](#)。

OpsCenter 是一项定价功能，价格约为1000美元 OpsItems，价格低于10美元。有关更多信息，请参阅 [AWS Systems Manager 定价](#)。

来自 AMS 的警报通知

作为警报处理的一部分，AWS Managed Services (AMS) 会根据影响分析创建事件，并在确定影响后启动事件管理流程进行补救。如果无法确定影响，AMS 会通过服务通知向与您的账户关联的电子邮件地址发送警报通知；有关警报处理流程，请参阅中有关 AMS 监控架构的示意图[监控的工作原理](#)。

接收 AMS 生成的警报

AWS Managed Services (AMS) 使您能够直接接收有关亚马逊 EC2 资源的警报通知，以减少通信延迟。要直接接收亚马逊 EC2 提醒，请使用管理 | 监控和通知 | SNS | 订阅更改类型 (ct-3rcI9u1k017wu) 将您的目标（首选电子邮件）订阅亚马逊 SNS 主题直接客户提醒。

Note

默认情况下，并非所有基准警报都发送到“直接客户警报”主题。要查看 AMS 监控系统生成的所有警报，请订阅 AMS 监控系统的 Amazon SNS 主题。在请求中，询问“AMS 监控主题”，指定接收警报的订阅渠道（Lambda、Amazon SQS、HTTP/S、电子邮件或短信），并指定将接收警报的终端节点（例如，电子邮件地址，如果您选择电子邮件协议）。

AMS 监控主题接收 AMS 共享服务使用的警报，因此可能会很吵。

要了解更多信息，请参阅《亚马逊简单通知服务[订阅 API 参考](#)》中的“订阅”部分。

有关 AMS 提供的基准警报列表，请参阅[来自 AMS 基线监测的警报](#)。

AMS 中基于标签的警报通知

使用标签将您的资源的警报通知发送到不同的电子邮件地址。最佳做法是使用基于标签的提醒通知，因为当多个开发者团队使用同一个账号时，发送到单个电子邮件地址的通知可能会造成混乱。

Important

基于标签的警报通知仅适用于与亚马逊 EC2、亚马逊 EBS、Elastic Load Balancing、网络负载均衡器、应用程序负载均衡器、亚马逊 RDS、Amazon Rds、Amazon Redshift 和相关的通知。OpenSearch

请勿在标签中添加个人身份信息 (PII)。

向特定的电子邮件地址发送警报

使用标记包含必须发送到特定电子邮件地址的警报的key = OwnerTeamEmail资源value = *EMAIL_ADDRESS*。

向多个电子邮件地址发送警报

要使用多个电子邮件地址，请指定以逗号分隔的值列表。例如 key = *OwnerTeamEmail*、value = *EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...*。值字段的字符总数不能超过 260。

使用自定义标签密钥

要使用自定义标签密钥，请在电子邮件中向您的 CSDM 提供自定义标签密钥名称，表示同意为基于标签的通信激活自动通知。最佳做法是对所有实例和资源的联系人标签使用相同的标记策略。

必须完整指定电子邮件地址，并用“at 符号” (@) 将本地部分与域名分开。无效电子邮件地址示例：*Team.AppATabc.xyz*或*john.doe*。有关标记策略的一般指导，请参阅[使用标签](#)。要标记现有资源，请提交 RFC，其中包含部署 | 高级堆栈组件 | 标记 | 创建 (auto) (ct-3cx7we852p3af) 更改类型。



Note

键值*OwnerTeamEmail*不必采用驼峰大小写。但是，标签区分大小写，因此最佳做法是使用推荐的格式。

AMS 自动修复警报

经过验证后，AWS Managed Services (AMS) 会根据本节中描述的特定条件和流程自动修复某些警报。

警报名称	说明	阈值	操作
安全通道中断	当 Windows 实例与 AD 域控制器断开连接时，将在 Windows EC2 实例上触发安全通道中断警报。	在过去 15 分钟内，该阈值高于定义值 10 次。	AMS 自动修复可验证实例是否在 SSM 中处于联机状态、主机名未重复，以及 AD 计算机对象是否与堆栈对齐。CloudFormation 补救措施修复了安全通道连接以恢复对实例的访问权限。

警报名称	说明	阈值	操作
状态检查失败	可能的硬件故障或实例的故障状态。	在过去 15 分钟内，系统至少检测到一次故障状态。	AMS 自动补救首先验证实例是否可访问。如果无法访问该实例，则该实例将停止并重新启动。停止和启动允许实例迁移到新的底层硬件。有关更多信息，请参阅以下“EC2 状态检查失败补救自动化”部分。
AMSLinuxDiskUsage	当您的 EC2 实例上 1 个挂载点（卷上的指定空间）的磁盘使用量已满时触发。	在过去 30 分钟内，该阈值高于定义值的 6 次。	AMS 自动修复首先会删除临时文件。如果这不能释放足够的磁盘空间，则会扩展音量以防止在卷已满时停机。
AMSWindowsDiskUsage	当您的 EC2 实例上 1 个装载点（卷上的指定空间）的磁盘使用量已满时。	在过去 30 分钟内，阈值高于定义值的 6 次。	AMS 自动修复首先会删除临时文件。如果这不能释放足够的磁盘空间，则会扩展音量以防止在卷已满时停机。

警报名称	说明	阈值	操作
RDS- EVENT -0089	数据库实例已使用其分配的存储空间的 90% 以上。	已分配的存储空间超过 90%。	AMS 自动修复首先验证数据库是否处于可修改且可用或存储已满状态。然后，它会尝试通过 CloudFormation 变更集增加分配的存储、IOPS 和存储吞吐量。如果已经检测到堆栈偏移，则会回退到 RDS API 以防止停机。 通过向 RDS 数据库实例添加以下标签，可以选择退出此功能："Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

警报名称	说明	阈值	操作
RDS-EVENT-0007	为数据库实例分配的存储空间已用完。要解决这个问题，请分配额外的存储空间。	存储空间已百分之百配。	AMS 自动修复首先验证数据库是否处于可修改且可用或存储已满状态。然后，它会尝试通过 CloudFormation 变更集增加分配的存储、IOPS 和存储吞吐量。如果已经检测到堆栈偏移，则会回退到 RDS API 以防止停机。 通过向 RDS 数据库实例添加以下标签，可以选择退出此功能："Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".

警报名称	说明	阈值	操作
RDS-EVENT-0224	请求的分配存储空间达到或超过配置的最大存储阈值。	数据库实例的最大存储阈值已用尽或大于或等于请求的分配存储空间。	AMS 自动补救首先会验证请求的 RDS 存储量是否会超过最大存储阈值。如果得到确认，AMS 会尝试使用 CloudFormation 变更集将最大存储阈值提高 30%，或者如果未通过配置资源，则直接使用 RDS API。CloudFormation 通过向 RDS 数据库实例添加以下标签，可以选择退出此功能："Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

警报名称	说明	阈值	操作
RDS 存储容量	为数据库实例分配的存储空间剩余不到 1GB。	存储空间分配了 99%。	AMS 自动修复首先验证数据库是否处于可修改且可用或存储已满状态。然后，它会尝试通过 CloudFormation 变更集增加分配的存储、IOPS 和存储吞吐量。如果已经检测到堆栈偏移，则会回退到 RDS API 以防止停机。 通过向 RDS 数据库实例添加以下标签，可以选择退出此功能："Key: <code>ams:rt:ams-rds-max-allocated-storage-policy</code>, Value: <code>ams-opt-out</code>".

Amazon 安全通道中 EC2 断：补救自动化说明

在 AWS Managed Services (AMS) 自动修复对 Amazon EC2 Windows 安全通道中断问题进行补救之前，自动化会执行以下预检查并创建事件报告以供进一步调查：

- 验证 Amazon EC2 实例 SSM 状态是否为“在线”。
- 验证 Amazon EC2 实例是否属于 Auto Scaling 组，以及 Auto Scaling 组中的所有实例是否具有相同的主机名。
- 检查 Amazon EC2 实例是否属于用于配置它的 CloudFormation 堆栈的一部分。如果实例已从 CloudFormation 堆栈中移除，则自动化将验证关联的 Active Directory 组织单位 (OU) 是否仍在引用该堆栈。

上述验证通过后，将继续进行自动化修复 Broken Secure 频道。

补救步骤：

- 自动修复会尝试修复 EC2 实例和 AD 域之间的安全通道，从而恢复对实例的访问权限。
- 修复后，自动化会检查安全通道是否已建立。如果失败，AMS 就会制造事件并让 AMS 行动部门进行调查。

EC2 状态检查失败：补救自动化注意事项

AMS 自动修复如何处理 EC2 状态检查失败问题：

- 如果您的 Amazon EC2 实例变得无法访问，则必须停止并重新启动该实例，这样才能将其迁移到新硬件并进行恢复。
- 如果问题的根源在于操作系统（fstab 中缺少设备、内核损坏等），则自动化无法恢复您的实例。
- 如果您的实例属于 Auto Scaling 组，则自动化不会执行任何操作——AutoScalingGroup 扩展操作会取代实例。
- 如果您的实例启用了 EC2 自动恢复，则修复不会采取任何措施。

EC2 音量使用补救自动化

AWS Managed Services (AMS) 自动修复如何处理 EC2 卷使用问题：

- 自动化首先会验证是否需要音量扩展，以及是否可以执行音量扩展。如果认为扩展是适当的，则自动化可以增加卷容量。这种自动化流程在增长需求与受控的有限扩张之间取得平衡。
- 在扩展卷之前，自动化会对实例执行清理任务（Windows：磁盘清理器，Linux：Logrotate + Simple Service Manager 代理日志删除），以尝试释放空间。

Note

清理任务不在 EC2 “T” 系列实例上运行，因为它们依赖于 CPU 积分来持续运行。

- 在 Linux 上，自动化仅支持扩展 EXT2 EXT3、EXT4 和 XFS 类型的文件系统。
- 在 Windows 上，自动化仅支持新技术文件系统 (NTFS) 和弹性文件系统 (RefS)。
- 自动化不会扩展属于逻辑卷管理器 (LVM) 或 RAID 阵列的卷。
- 自动化不会扩展实例存储容量。
- 如果受影响的音量已经大于 2 TiB，则自动化不会采取任何行动。
- 通过自动化进行的扩展限制为每周最多三次，在系统的整个生命周期内最多只能进行五次。
- 如果上一次扩展是在过去六小时内进行的，则自动化不会扩大音量。

当这些规则阻止自动化采取行动时，AMS 会通过出站服务请求与您联系，以确定下一步要采取的行动。

Amazon RDS 存储不足事件补救自动化

AWS Managed Services (AMS) 自动修复如何处理 Amazon RDS 存储不足事件问题：

- 在尝试扩展 Amazon RDS 实例存储空间之前，自动化会执行多项检查，以确保 Amazon RDS 实例处于可修改且可用或存储空间已满的状态。
- 如果检测到 CloudFormation 堆栈偏差，则通过 Amazon RDS API 进行补救。
- 在以下情况下，修复操作不会运行：
 - Amazon RDS 实例的状态不是“可用”或“存储空间已满”。
 - Amazon RDS 实例存储目前不可修改（例如，在过去六小时内修改了存储空间时）。
 - Amazon RDS 实例已启用自动缩放存储空间。
 - Amazon RDS 实例不是 CloudFormation 堆栈中的资源。
- 补救仅限于每六小时进行一次扩展，在连续的十四天内不超过三次扩展。
- 当这些情况发生时，AMS 会与您联系，告知出站事件，以确定下一步行动。

在 AMS 中创建其他 CloudWatch 警报

您可以使用 AWS Managed Services (AMS) 部署 | 监控和通知 | CloudWatch | 创建警报更改类型来创建新警报。

Important

AMS 不监控您创建的 CloudWatch 警报。

为 Amazon EC2 实例使用自定义 CloudWatch 指标和警报（仅适用于不依赖部署到 Auto Scaling 组的更新的可变 AMIs 部署）：

1. 生成您的应用程序监控脚本和自定义指标。有关更多信息和访问示例脚本的权限，请参阅[监控 Amazon EC2 Linux 实例的内存和磁盘指标](#)。适用于 Linux 亚马逊 EC2 实例的亚马逊 CloudWatch 监控脚本演示了如何生成和使用亚马逊 CloudWatch 自定义指标。这些示例 Perl 脚本包含一个功能完备的示例，用于报告 Linux 实例的内存、交换文件和磁盘空间使用率指标。

2. 上传您的监控脚本。要将监控脚本上传到您的 Auto Scaling 组或 Amazon EC2 实例配置，您可以在配置 Auto Scaling 组或 Amazon EC2 实例 UserData 时使用，或者，如果您的应用程序是使用部署的 CodeDeploy，则可以使用部署 | CodeDeploy 应用程序 | 部署 CT (ct-2edc3sd1sqmrb) 修改配置。
3. 将您的自定义指标发布到 CloudWatch （首次发布新自定义指标的数据点即已创建），请参阅[发布自定义指标](#)。
4. 创建 CloudWatch 警报，请参阅[为实例创建 CloudWatch 警报](#)。

Important

必须将监控数据发送到此路径 [infra/INSTANCE_ID/YOUR_CUSTOM_METRIC]

要修改或删除 CloudWatch 警报，请使用管理 | 其他 | 其他 | 创建更改类型 (ct-1e1xtak34nx76) 提交 RFC，其中包含完成操作所需的参数，如亚马逊 API 参考中所述。CloudWatch [PutMetricAlarm](#)

您可以使用 CloudWatch 事件流。AMS 已 CloudWatch 与集成，您可以请求任何 AWS API 调用触发 CloudWatch 事件。

为此，请提交包含你感兴趣的 API 调用的管理 | 其他 | 其他 | 更新 CT (ct-0xdawir96cy7k)。AMS 操作员将与您交谈以收集需求。要了解更多信息，请参阅 [Amazon CloudWatch 文档](#)。

要访问 CloudWatch 活动流，请提交“管理 | 其他 | 其他 | 更新 CT” (ct-0xdawir96cy7k)，将派对添加到 SNS 通知主题中。AMS 操作员将与您交谈以收集需求。

在 AMS 中创建自定义 CloudWatch 指标和警报

您可以在 Amazon 中存储您的业务和应用程序指标 CloudWatch。您可以查看图表并根据这些指标设置警报，就像为 CloudWatch 已存储的 AWS Managed Services (AMS) 资源的指标设置警报一样。要了解 CloudWatch 更多信息，请参阅 [Amazon Conce CloudWatch pts](#)。

Amazon SNS 允许应用程序通过“推送”机制向 AMS 托管监控系统或警报发布到的彩信、Amazon SNS (SNS) 主题（在本例中为彩信和您的 SQS 队列）发送时间关键型消息。您可以使用 CloudWatch 创建自定义指标，并通过 SNS 主题让 AMS 适当地向您发出警报。为此，请按照以下步骤操作。

 Note

此过程不适用于依赖于部署到 Auto Scaling 组的更新的 AMIs 不可变部署，它适用于可变应用程序（不是 ASG）部署。

在 AMS Advanced 的限制范围内设置自定义指标是一项复杂的任务。有关来自的示例 CloudWatch，请参阅[示例：计算术语的出现次数](#)。

1. 生成您的应用程序监控脚本和自定义指标（例如发生次数示例）。有关更多信息和访问示例脚本的权限，请参阅[监控 Amazon EC2 Linux 实例的内存和磁盘指标](#)。
2. 上传您的监控脚本。要将监控脚本上传到您的 Auto Scaling 组或 Amazon EC2 实例配置，您可以在配置 Auto Scaling 组或 Amazon EC2 实例 UserData 时使用，或者，如果您的应用程序是使用部署的 CodeDeploy，则可以使用部署 | CodeDeploy 应用程序 | 部署 CT (ct-2edc3sd1sqmrb) 修改配置。
3. 将您的自定义指标发布到 CloudWatch（首次发布新自定义指标的数据点即已创建），请参阅[发布自定义指标](#)。
4. 要将您的客户指标集成到您的应用程序监控系统中，请使用“部署”|“监控和通知”| SNS | 创建更改类型 (ct-3dfnglm4ombbs) 提交 RFC，请求 AMS 为该指标创建 SNS 主题。
5. 创建 CloudWatch 警报，请参阅[创建 Amazon CloudWatch 警报](#)。

 Important

必须将监控数据发送到此路径 [infra/**INSTANCE_ID/YOUR_CUSTOM_METRIC**]。

在 AMS 中使用适用于 .Net 和 SQL 服务器的 CloudWatch 应用程序见解

您可以使用 Amazon App CloudWatch Location Insights 为您的 AWS Managed Services (AMS) 应用程序资源设置监控器，以持续分析数据，寻找应用程序出现问题的迹象，并在解决应用程序问题时缩短平均修复时间 (MTTR)。有关 CloudWatch 应用程序见解的详细信息，请参阅[.NET 和 SQL Server 的 CloudWatch 应用程序见解](#)。

 Important

AMS 不会监控 Applicati CloudWatch on Insights 中的问题，因为这些问题是针对由您控制的应用程序代码。

要使用 App CloudWatch lication Insights，请提交 RFC，其中包含部署 | 高级堆栈组件 | 身份和访问管理 (IAM) Access Management (IAM) | 创建实体或策略 (需要审查) 更改类型 (ct-3dpd8mdd9jn1r)，并请求创建为您提供配置应用程序见解权限的 IAM 角色。CloudWatch 有两种方法可以接收已发现的问题：通过 SNS 主题接收问题或使用 CloudWatch 事件规则中的目标。在 RFC 中，指定您想要的。如果您计划使用 CloudWatch 事件规则，还需要在 RFC 中指定规则定义。设置 App CloudWatch lication Insights 后，您会收到潜在问题的通知，包括指向可能根本原因的见解。

要了解如何担任该角色，请参阅 AMS 入职指南将您的 A [ctive Directory](#) 与 [AMS IAM 角色联合](#) 起来。

在 AMS 中使用亚马逊 EventBridge 托管规则

AMS Advanced 使用 Amazon EventBridge 托管规则。托管规则是一种与 AMS 直接关联的独特规则类型。这些规则匹配传入的事件并将其发送到目标进行处理。托管规则由 AMS 预定义，包括服务管理客户账户所需的事件模式，除非另有定义，否则只有拥有的服务才能使用这些托管规则。

AMS 托管规则与events.managedservices.amazonaws.com服务主体相关联。这些托管规则通过[AWSServiceRoleForManagedServices_Events服务相关角色](#)进行管理。要删除这些规则，需要客户特别确认。有关更多信息，请参阅[删除 AMS 托管规则](#)。

有关规则的更多信息，请参阅 Amazon EventBridge 用户指南中的[规则](#)。

AMS 部署的 Amazon EventBridge 托管规则

亚马逊 EventBridge 托管规则

规则名称	说明	定义
AMSAdvanc edCoreRule	此规则将 Amazon CloudWatc h 警报转发 给 AMS 监	<pre>{ { "source": ["aws.cloudwatch"], "detail-type": ["CloudWatch Alarm State Change"],</pre>

规则名称	说明	定义
	控。Amazon CloudWatch 事件监控 CloudWatch 警报。	<pre>} }</pre>

为 AMS 创建托管规则

您无需手动创建 Amazon EventBridge 托管规则。当您在 AWS 管理控制台、或 AWS API 中加入 AMS 时，AMS 会为您创建它们。AWS CLI

编辑 AMS 的托管规则

AMS 不允许您编辑托管规则。每个托管规则的名称和事件模式均由 AMS 预定义。

删除 AMS 的托管规则

您无需手动删除托管规则。当您在 AWS 管理控制台、或 AWS API 中退出 AMS 时，AMS 会为您清理资源并删除 AMS 拥有的所有托管规则。AWS CLI

如果 AMS 在离职期间未能删除托管规则，您也可以使用 Amazon EventBridge 控制台、AWS CLI 或 AWS API 手动删除托管规则。为此，您必须先退出 AMS，然后强制删除托管规则。

AMS 中值得信赖的修正者

Trusted Remediator 是一种 AWS Managed Services 解决方案，可自动执行补救措施[AWS Trusted Advisor](#)和建议。[AWS Compute Optimizer](#)当 Trusted Advisor Compute Optimizer 向您指出降低成本、提高系统可用性、优化性能或弥合安全漏洞的机会时，Trusted Remediator 会创建建议。AWS 账户借助 Trusted Remediator，您可以使用既定的最佳实践，以安全、标准化的方式解决这些安全、性能、成本优化、容错和服务限制建议的问题。Trusted Remediator 允许您配置修复解决方案，并按照您创建的计划自动运行，从而简化了修复过程。这种简化的方法可以一致、高效地解决问题，且无需人工干预。

可信修正者的主要优点

以下是 Trusted Remediator 的主要优点：

- 提高安全性、性能和成本优化：Trusted Remediator 可帮助您增强账户的整体安全状况，优化资源利用率并降低运营成本。
- 自助服务设置和配置：您可以将 Trusted Remediator 配置为与您的要求和首选项保持一致。
- 自动 Trusted Advisor 检查和 AWS Compute Optimizer 建议修复：配置完成后，Trusted Remediator 会自动为选定的检查运行修复操作。这种自动化消除了手动干预的需求。
- 最佳实践实施：补救措施基于既定的最佳实践，因此以标准化和有效的方式解决问题。
- 计划执行：您可以选择与您的 day-to-day 操作工作流程一致的补救时间表。

Trusted Remediator 使您能够主动解决 AWS 环境中已发现的问题，帮助您遵守最佳实践，维护安全、高性能且经济实惠的云基础架构。

可信修正者的工作原理

以下是“可信修正者”工作流程的示例：

Trusted Remediator 会 AWS 账户 为您评估 Trusted Advisor 和推荐 Compute Optimizer 建议，然后在中创建。AWS Systems Manager [OpsItems](#) OpsCenter 然后，您可以使用 Trusted Remediator 自动化文档 OpsItems 自动或手动修复。以下是每种补救措施的详细信息：

- 自动修复：Trusted Remediator 运行自动化文档并监控运行情况。自动化文档完成后，Trusted Remediator 会解析 Opsitem。
- 手动修复：可信修正者会创建 OpsItem 供您查看。查看后，您可以创建自动 RFC、[可信修正者 | 查找 | 修复](#)，更改类型以修复资源。有关手动修复步骤的信息，请参阅[在“可信修正器”中运行手动修复](#)。

修复日志存储在 Amazon S3 存储桶中。您可以使用 S3 存储桶中的数据来构建用于报告的自定义 QuickSight 仪表板。AMS 还根据要求为可信修正者提供报告。要接收这些报告，请联系您的 CSDM。

可信修正者的关键术语

以下是在 AMS 中使用 Trusted Remediator 时需要了解的术语：

- AWS Trusted Advisor 以及 AWS Compute Optimizer：由提供的云优化服务 AWS。Trusted Advisor Compute Optimizer 会检查您的 AWS 环境并根据以下六个类别的最佳实践提供建议：
 - 成本优化

- 性能
- 安全性
- 容错能力
- 卓越运营
- 服务限制

有关更多信息，请参阅[AWS Trusted Advisor](#)和[AWS Compute Optimizer](#)。

- 可信修正者：用于[Trusted Advisor](#)检查和[AWS Compute Optimizer](#)建议的 AMS 补救解决方案。Trusted Remediator 可帮助您使用已知的最佳实践安全地修复 Trusted Advisor 检查和 Compute Optimizer 建议，以提高安全性、性能并降低成本。可信修正器易于设置和配置。您只需配置一次，Trusted Remediator 就会按照您的首选计划（每天或每周）运行修复。
- AWS Systems Manager SSM 文档：一个 JSON 或 YAML 文件，用于定义对您的 AWS 资源 AWS Systems Manager 执行的操作。SSM 文档可作为声明性规范，用于自动执行跨多个 AWS 资源和实例的操作任务。
- AWS Systems Manager OpsCenter OpsItem：云运营问题管理资源，可帮助您跟踪和解决 AWS 环境中的运营问题。OpsItems 为跨 AWS 服务资源的运营数据和问题提供集中视图和管理系统。每个 OpsItem 代表一个操作问题，例如潜在的安全风险、性能问题或操作事件。
- 配置：配置是存储在中的一组属性 [AWS AppConfig](#)，其功能为 [AWS Systems Manager](#)。中的 Trusted Remediator 应用程序 AWS AppConfig 可帮助在帐户级别配置修复。
- 执行模式：执行模式是一个配置属性，用于确定如何针对每个 Trusted Advisor 检查结果运行修复。支持四种执行模式：自动、手动、有条件和非活动。
- 资源覆盖：此功能使用资源标签来覆盖特定资源的配置。
- 修复项目日志：可信修正者修复 S3 日志存储桶中的日志文件。修复项目日志是在创建修复时创建 OpsItems 的。此日志文件包含手动执行补救 OpsItems 和自动执行补救 OpsItems。使用此日志文件跟踪所有补救项目。
- 自动修复执行日志：可信修正者修复 S3 日志存储桶中的日志文件。自动修复执行日志在 SSM 文档的自动运行完成后创建。此日志包含用于自动执行补救 OpsItems 的 SSM 执行详细信息。使用此日志文件来跟踪自动修复。

开始使用 AMS 中的可信修复器

可信修正器在 AMS 中可用，无需额外付费。Trusted Remediator 支持单账户和多账户配置。

加入可信修复者

要将您的 AMS 账户注册到 Trusted Remediator，请发送电子邮件给您的云架构师或云服务交付经理 (CSDMs)。在电子邮件中，请包含以下信息：

- **AWS 账户：**十二位数的账户识别码。您要注册到 Trusted Remediator 的所有账户都必须属于同一 AMS Advanced 客户。
- **委托管理员帐户：**用于单个或多个帐户 Trusted Advisor 和 Compute Optimizer 检查配置的帐户。
- **成员账户：**这些账号是指关联到委派管理员账号的账号。这些账户继承委派管理员账户的配置。您可以拥有一个成员账户或多个成员账户。

Note

成员账号继承委派管理员账号的配置。如果您需要为特定账户配置不同的配置，请使用您的首选配置注册多个委派管理员帐户。在入职之前，请与您的云架构师一起规划账户结构和配置。

- **AWS 区域：**您的资源所在的位置。AWS 区域 有关列表 AWS 区域，请参阅[AWS 服务 按地区划分](#)。
- **补救时间表和时间：**您的首选补救时间表（每天或每周）。Trusted Remediator 会在计划的时间收集 Trusted Advisor 检查并启动修复。例如，您可以将补救计划设置为每周星期日凌晨 1:00（澳大利亚东部标准时间）。
- **通知电子邮件：**Trusted Remediator 使用通知电子邮件每天通知您是否有补救措施。通知电子邮件的主题是“可信修正者补救摘要”，其内容提供有关过去 24 小时内运行的可信修正者修正的信息。

Note

每次计划修复后，请检查您的应用程序和资源。如需其他支持，请联系 AMS。

在您向 CA 或 CSDM 提交包含所需详细信息的入会申请后，AMS 会将您的账户登录到 Trusted Remediator。Trusted AWS AppConfig Remediator 使用（一种功能）来定义 Trusted Advisor 检查的配置。AWS Systems Manager 这些配置是存储在中的一组属性 AWS AppConfig。为防止对您的资源进行未经授权的费用，当账户加入可信修正者时，所有支持的 Trusted Advisor 检查都将设置为“非活动”。这些配置可帮助您自动修复特定的 Trusted Advisor 检查，或者评估和手动修复剩余的检查。这些配置是高度可定制的，允许您为每项 Trusted Advisor 检查应用配置。有关更多信息，请参阅[在可信修正器中配置 Trusted Advisor 检查修复](#)。

在您的中配置可信修正者 AWS 账户

入职完成后，您的 CA 或 CDSM 会通知您，并在您的授权管理员中创建默认配置。AWS 账户该配置存储在 AWS AppConfig “可信修正者” 应用程序下。您可以使用 RFC [管理 | 可信修正者 | 修正配置 | 更新](#) 来请求配置更新。有关更多信息，请参阅 [在可信修正器中配置 Trusted Advisor 检查修复](#)。

要查看默认的可信修正者配置，请完成以下步骤：

1. 打开 AWS Systems Manager 控制台，网址为 <https://console.aws.amazon.com/systems-manager/>。

Note

请确保您使用的是委派管理员账户。

2. 选择“应用程序管理”，AppConfig。
3. 从应用程序列表中选择“可信修正者”。

以下是显示可信修正者配置的 AWS AppConfig 控制台示例：

选择要修复的检查和建议

默认情况下，您的配置中的所有 Trusted Advisor 检查和 Compute Optimizer 建议的修复执行模式均为“非活动”。这样可以防止未经授权的补救并保护资源。AMS 提供精心策划的 SSM 自动化文档，用于 Trusted Advisor 支票补救。

要选择要使用可信修正者修复的检查，请完成以下步骤：

1. 查看支持的建议 [Trusted Advisor 和 Compute Optimizer 建议列表或关联的 SSM 自动化文档的名称](#)，以决定要使用 Trusted Remediator 修复哪些检查和建议。
2. 提交“[管理](#)”|“[可信修正者](#)”|“[修正配置](#)”|“[更新](#)”请求以更新所选 Trusted Advisor 检查的配置。有关如何选择支票的说明，请参阅 [在可信修正器中配置 Trusted Advisor 检查修复](#)。

在“可信修正者”中跟踪您的补救措施

更新账户级别配置后，Trusted Remediator 会 OpsItems 为每项补救措施创建。Trusted Remediator 会 OpsItems 根据您的补救计划运行 SSM 文档进行自动修复。有关如何 OpsItems 从 Systems Manager OpsCenter 控制台查看所有补救措施的说明，请参阅 [在“可信修正者”中跟踪补救措施](#)。

在“可信修正器”中运行手动修复

您可以使用自动 RFC 手动修复 Trusted Advisor 检查。当您选择手动修复时，可信修正者会创建手动执行 OpsItem。有关更多信息，请参阅 [在“可信修正器”中运行手动修复](#)。

受信任修正者支持的 Compute Optimizer 建议

下表列出了支持的 Compute Optimizer 建议、SSM 自动化文档、预配置的参数以及自动化文档的预期结果。在启用 SSM 自动化文档进行支票补救之前，请查看预期结果，以帮助您根据业务需求了解可能的风险。

确保每个 Compute Optimizer 检查的相应配置规则适用于要为其启用修复的受支持检查。有关更多信息，请参阅[选择使用 AWS Compute Optimizer 支 Trusted Advisor 票](#)。

优化选项	SSM 文档名称和预期结果	支持的预配置参数和约束
规模优化		
亚马逊 EC2 实例建议	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation 根据 Compute Optimizer 的建议更新了亚马逊 EC2 实例类型。如果存在最佳选项，则选择最佳选项，同时保持相同的平台参数（架构、虚拟机管理程序、网络接口、虚拟化类型等）。	• MinimumDaysSinceLastChange：用于指定自上次实例类型更改以来的最小天数的参数。默认值为 7 天。 没有限制 • 创建AMIBefore调整大小：要在调整大小之前创建实例 AMI 作为备份，请设置为“True”。要不创建备份，请将其设置为“False”。默认为“真”。 没有限制
Amazon EBS 卷建议	AWSManagedServices-ModifyEBSVolume Amazon EBS 卷是根据 Compute Optimizer 的建议修改的。修改可能包括卷类型、大小、IOPS、卷生成（gp2、gp3 等）。	• CreateSnapshot：要在修改卷之前创建快照，请设置为“True”。要不创建快照，请将其设置为“False”。默认值为“真”。 没有限制

优化选项	SSM 文档名称和预期结果	支持的预配置参数和约束
		• VolumeType：所需的卷类型。如果未指定类型，则保留现有类型。 没有限制 • VolumeSize：所需的卷大小，以 GiB 为单位。目标卷大小必须大于或等于该卷的现有大小。如果未指定大小，则保留现有大小。 没有限制 • Iops：请求的每秒 I/O 操作数 (IOPS)。此参数仅对 io1、io2 和 gp3 卷有效。 没有限制 • 吞吐量：为卷预配置的吞吐量，最大为 1000 MiB/s。此参数仅对 gp3 卷有效。 没有限制 • RemediateStackDrift：要启动漂移补救，如果任何漂移是由音量修改引起的，请将其设置为 “True”。要不尝试漂移补救，请将其设置为 “False”。默认为 “真”。 没有限制
Lambda 函数推荐	AWSManagedServices-TrusteRemediatorOptimizeLambdaMemory AWS Lambda 根据 Compute Optimizer 的建议对函数内存进行了优化。	RecommendedMemorySize：自定义内存大小（如果与推荐的选项不同）。 没有限制

闲置资源

优化选项	SSM 文档名称和预期结果	支持的预配置参数和约束
闲置亚马逊 EBS 交易量	AWSManagedServices-DeleteUnusedEBSVolume 未连接的 Amazon EBS 卷将被删除。	• CreateSnapshot：要在删除卷之前创建快照，请设置为“True”。要不创建快照，请将其设置为“False”。默认值为“真”。 没有限制 • MinimumUnattachedDays：删除 Amazon EBS 卷的最短未连接天数，最长为 62 天。默认值为 7。 没有限制
空闲的亚马逊 EC2 实例	AWSManagedServices-StopEC2 实例 闲置的 Amazon EC2 实例将被停止。	ForceStopWithInstanceStore：要强制停止使用实例存储的实例，请设置为“True”。要不强制停止，请设置为“False”。默认值为“False”可防止实例停止。 没有限制
空闲的亚马逊 RDS 实例	AWSManagedServices-StopIdleRDSInstance 停止闲置的 Amazon RDS 实例。支持的引擎有：MariaDB、微软 SQL Server、MySQL、Oracle、PostgreSQL。本文档不适用于 Aurora MySQL 和 Aurora PostgreSQL。该实例将在最多 7 天内停止并自动重新启动。	不允许使用预配置参数。 没有限制

Trusted Advisor 受信任修正者支持的检查

下表列出了支持的 Trusted Advisor 检查、SSM 自动化文档、预配置参数以及自动化文档的预期结果。在启用 SSM 自动化文档进行支票补救之前，请查看预期结果以帮助您根据业务需求了解可能的风险。

对于要为其启用补救功能的受支持检查，请确保每 Trusted Advisor 项检查都有相应的配置规则。有关更多信息，请参阅[查看由支持的 AWS Trusted Advisor 支票 AWS Config](#)。如果支票有相应的 AWS Security Hub CSPM 控件，请确保启用了 Security Hub 控件。有关更多信息，请参阅在 [Security Hub 中启用控件](#)。有关管理预配置参数的信息，请参阅 Trusted Remediator 中的[配置 Trusted Advisor 检查修复](#)。

Trusted Advisor 可信修正者支持的成本优化检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Z4 AUBRNSmz 未关联的弹性 IP 地址	AWSManagedServices-TrustedRemediatorReleaseElasticIP 释放未与任何资源关联的弹性 IP 地址。	不允许使用预配置参数。 没有限制
c18d2gz 150-亚马逊实例已停止 EC2	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime-停止天数的 Amazon EC2 实例终止。	- 创建AMIBefore终止：要在终止 Amazon EC2 实例之前创建实例 AMI 作为备份，请选择true。要在终止之前不创建备份，请选择false。默认值为 true。 - AllowedDays：实例在终止之前处于停止状态的天数。默认值为 30。 没有限制
c18d2gz128 未对生命周期策略进行配置的 Amazon ECR 存储库	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy 如果生命周期策略尚不存在，则为指定的存储库创建生命周期策略。	ImageAgeLimit：Amazon ECR 存储库中“任何”图像的最大保存期限（以天为单位）(1-365)。 没有限制
DAvU99Dc4C 未充分利用的 Amazon EBS 卷	AWSManagedServices-DeleteUnusedEBSVolume	CreateSnapshot：如果设置为true，则自动化会在删除 Amazon EBS 卷之前创建该卷的

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
	如果过去 7 天内未连接未充分利用的 Amazon EBS 卷，则删除这些卷。默认情况下会创建 Amazon EBS 快照。	快照。默认设置为 true。有效值为 true 和 false (区分大小写)。 MinimumUnattachedDays：删除 EBS 卷的最少未连接天数，最多 62 天。如果设置为 0，则 SSM 文档不会检查未连接的时段，如果该卷当前处于未连接状态，则会删除该卷。默认值为 7。 没有限制
hj m8 LMh88u 闲置的负载均衡器	AWSManagedServices-DeleteIdleClassicLoadBalancer 如果闲置的 Classic Load Balancer 未使用且未注册任何实例，则将其删除。	IdleLoadBalancerDays：Classic Load Balancer 在考虑处于空闲状态之前有 0 个请求的连接的天数。默认值为七天。 如果启用了自动执行，则如果没有活跃的后端实例，则自动化会删除闲置的 Classic 负载均衡器。对于所有具有活跃后端实例但后端实例运行状况不佳的闲置经典负载均衡器，不会使用自动修复，而是创建 OpsItems 用于手动补救的自动修复。
ti39Halfu8 Amazon RDS 闲置数据库实例	AWSManagedServices-StopIdleRDSInstance 过去七天一直处于空闲状态的 Amazon RDS 数据库实例已停止。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
COr6dfpM05 AWS Lambda 内存大小过度配置的函数	AWSManagedServices-ResizeLambdaMemory AWS Lambda 函数的内存大小已调整为由 Trusted Advisor提供的推荐内存大小。	RecommendedMemorySize : Lambda 函数的推荐内存分配。值范围介于 128 和 10240 之间。 如果在自动化运行之前修改了 Lambda 函数的大小，则该自动化可能会使用推荐的值覆盖这些设置。 Trusted Advisor
qch7dwoux1 低利用率 Amazon EC2 实例	AWSManagedServices-StopEC2Instance (自动和手动执行模式下的默认 SSM 文档。) 使用率低的 Amazon EC2 实例已停止。	ForceStopWithInstanceStore : 设置为 true 以强制停止使用实例存储的实例。否则，设置为 false。默认值为 false 可防止实例停止。有效值为真或假 (区分大小写)。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
qch7dwoux1 低利用率 Amazon EC2 实例	AWSManagedServices-ResizeInstanceByOneLevel 在相同的 EC2 实例系列类型中，Amazon 实例按向下调整一个实例类型的大小。实例在调整大小操作期间停止并启动，并在 SSM 文档运行完成后恢复到初始状态。此自动化不支持调整 Auto Scaling 组中的实例的大小。	- MinimumDaysSinceLastChange：自上次实例类型更改以来的最短天数。如果在指定时间内修改了实例类型，则不会更改实例类型。0 用于跳过此验证。默认值为 7。 - 创建AMIBefore调整大小：要在调整大小之前创建实例 AMI 作为备份，请选择true。要不创建备份，请选择false。默认值为 false。有效值为true和false (区分大小写)。 - ResizelfStopped：要继续更改实例大小，即使实例处于停止状态，也请选择true。要在实例处于停止状态时不自动调整其大小，请选择false。有效值为true和false (区分大小写)。 没有限制
qch7dwoux1 低利用率 Amazon EC2 实例	AWSManagedServices-TerminateInstance 如果未加入 Auto Scaling 组且未启用终止保护，则低利用率的 Amazon EC2 实例将被终止。默认情况下会创建 AMI。	创建AMIBefore终止：将此选项设置false为true或可在终止实例之前创建实例 AMI 作为备份。EC2 默认值为 true。有效值为true和false (区分大小写)。 没有限制
g31sq1e9U Underutilized Amazon Redshift Clusters	AWSManagedServices-PauseRedshiftCluster 亚马逊 Redshift 集群已暂停。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1cj39rr6v Amazon S3 未完成分段上传中止配置	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Amazon S3 存储桶配置了生命周期规则，用于中止某些天后仍未完成的分段上传。	DaysAfterInitiation : Amazon S3 停止未完成的分段上传的天数。默认设置为 7 天。 没有限制
c1z7kmr00n Amazon 针对实例 EC2 的成本优化建议	使用来自的亚马逊 EC2 实例建议和空闲的亚马逊 EC2 实例 受信任修正者支持的 Compute Optimizer 建议 。	不允许使用预配置参数。 没有限制
c1z7kmr02n Amazon EBS 针对卷的成本优化建议	使用来自的 Amazon EBS 交易量建议和空闲亚马逊 EBS 交易量。 受信任修正者支持的 Compute Optimizer 建议	不允许使用预配置参数。 没有限制
c1z7kmr03n Amazon RDS 针对数据库实例的成本优化建议	使用来自的空闲的 Amazon RDS 实例 受信任修正者支持的 Compute Optimizer 建议 。	不允许使用预配置参数。 没有限制
c1z7kmr05n AWS Lambda 函数的成本优化建议	使用来自的 Lambda 函数建议。 受信任修正者支持的 Compute Optimizer 建议	不允许使用预配置参数。 没有限制

Trusted Advisor 受信任修正者支持的安全检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
12Fnkpl8Y5 Exposed Access Keys	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey 公开的 IAM 访问密钥已停用。	不允许使用预配置参数。 使用公开的 IAM 访问密钥配置的应用程序无法进行身份验证。
Hs4ma3G127-应启用 API Gateway REST WebSocket 和 API 执行日志记录 相应的 AWS Security Hub CSPM 支票： APIGateway.1	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging API 阶段已启用执行日志记录。	LogLevel: 用于启用执行日志记录的日志级别，ERROR-仅对错误启用日志记录。 INFO-已为所有事件启用日志功能。 要启用执行日志，您必须授予 API Gateway 读取和写入账户日志的权限，有关详细信息，请参阅 APIs 在 API Gateway 中设置 REST CloudWatch 日志记录 。 CloudWatch
Hs4ma3G129-API Gateway REST API 阶段应该启用追踪 AWS X-Ray 相应的 AWS Security Hub CSPM 支票： APIGateway.3	AWSManagedServices-EnableAPIGatewayXRayTracing 在 API 阶段已启用 X 射线追踪。	不允许使用预配置参数。 没有限制
Hs4Ma3G202-API Gateway	AWSManagedServices-EnableAPIGatewayCacheEncryption	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
REST API 缓存数据应静态加密 相应的 AWS Security Hub CSPM 支票：APIGateway.5	如果 API Gateway REST API 阶段启用了缓存，则为 API Gateway REST API 缓存数据启用静态加密。	
Hs4ma3G177- 相应的 AWS Security Hub CSPM 检查-与负载均衡器关联的 Auto Scaling 组应使用负载均衡器运行状况检查。AutoScaling1	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck 已为 Auto Scaling 组启用了 Elastic Load Balancing 运行状况检查。	HealthCheckGracePeriod：Auto Scaling 在检查已投入使用的亚马逊弹性计算云实例的运行状况之前等待的时间，以秒为单位。 如果连接到 Auto Scaling 组的任何 Elastic Load Balancing 负载均衡器报告运行状况不佳，则启用 Elastic Load Balancing 运行状况检查可能会导致替换正在运行的实例。有关更多信息，请参阅将 Elastic Load Balancing 负载均衡器附加到您的 Auto Scaling 组
Hs4ma3G245-CloudFormation 堆栈应与亚马逊简单通知服务集成 相应的 AWS Security Hub CSPM 支票：CloudFormation.1	AWSManagedServices-EnableCFNStackNotification 将 CloudFormation 堆栈与 Amazon SNS 主题关联以获得通知。	通知ARNs：要与 ARNs 选定 CloudFormation 堆栈关联的 Amazon SNS 主题。 要启用 auto 修复，必须提供NotificationARNs 预配置参数。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G210-CloudFront 发行版应该启用日志记录 相应的 AWS Security Hub CSPM 支票：CloudFront.2	AWSManagedServices-EnableCloudFrontDistributionLogging 已为 Amazon CloudFront 分配启用日志记录。	• BucketName：您要在其中存储访问日志的 Amazon S3 存储桶的名称。 • S3KeyPrefix：亚马逊 CloudFront 分配日志在 S3 存储桶中的位置的前缀。 • IncludeCookies：表示是否在访问日志中包含 Cookie。 要启用 auto 修复，必须提供以下预配置参数： • BucketName • S3KeyPrefix • IncludeCookies 有关修正限制，请参阅如何为我的 CloudFront 分配开启日志记录？
Hs4ma3G109-应启用 CloudTrail 日志文件验证 相应的 AWS Security Hub CSPM 支票：CloudTrail.4	AWSManagedServices-TrustedRemediatorEnableCloudTrailLoggingValidation 启用 CloudTrail 跟踪日志验证。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G108 —— CloudTrail 轨迹应与亚马逊日志集成 CloudWatch 相应的 AWS Security Hub CSPM 支票：CloudTrail.5	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail 已与 CloudWatch 日志集成。	- CloudWatchLogsLogGroupName：将 CloudWatch 日志传递到的日志 CloudTrail 日志组的名称。您必须使用账户中存在的日志组。 - CloudWatchLogsRoleName：CloudWatch 日志终端节点要代入的写入用户日志组的 IAM 角色的名称。您必须使用账户中存在的角色。 要启用 auto 修复，必须提供以下预配置参数： - CloudWatchLogsLogGroupName - CloudWatchLogsRoleName
Hs4ma3G217-CodeBuild 项目环境应该有日志配置 AWS 相应的 AWS Security Hub CSPM 支票：CodeBuild.4	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig 启用 CodeBuild 项目日志记录。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G306-Neptune 数据库集群应启用删除保护 相应的 AWS Security Hub CSPM 支票：documentDB.3	AWSManagedServices-TrustedRolemediatorDisablePublicAccessOnDocumentDBSnapshot 从 Amazon DocumentDB 手动集群快照中移除公共访问权限。	不允许使用预配置参数。 没有限制
Hs4ma3G308-亚马逊 DocumentDB 集群应启用删除保护 相应的 AWS Security Hub CSPM 支票：documentDB.5	AWSManagedServices-TrustedRolemediatorEnableDocumentDBClusterDeletionProtection 为亚马逊文档数据库集群启用删除保护。	不允许使用预配置参数。 没有限制
Hs4ma3G323-DynamoDB 表应该启用删除保护 相应的 AWS Security Hub CSPM 检查：dynamodb.6	AWSManagedServices-TrustedRolemediatorEnableDynamoDBTableDeletionProtection 为非 AMS DynamoDB 表启用删除保护。	不允许使用预配置参数。 没有限制
eps02jt06w-亚马逊 EBS 公开快照	AWSManagedServices-TrustedRolemediatorDisablePublicAccessOnEBSSnapshot 已禁用 Amazon EBS 快照的公共访问权限。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G118-VPC 默认安全组不应允许入站或出站流量 相应的 AWS Security Hub CSPM 支票：EC2.2	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG 默认安全组中的所有入口和出口规则都将被删除。	不允许使用预配置参数。 没有限制
Hs4Ma3G117-附加的 EBS 卷应在静态状态下进行加密 相应的 AWS Security Hub CSPM 支票：EC2.3	AWSManagedServices-EncryptInstanceVolume 实例上附加的 Amazon EBS 卷已加密。	- KMSKeyID：用于加密卷的 AWS KMS 密钥 ID 或 ARN。 - DeleteStaleNonEncryptedSnapshotBackups：一个标志，用于决定是否应删除未加密的旧卷的快照备份。 作为修复的一部分，实例将重新启动，如果DeleteStaleNonEncryptedSnapshotBackups 将其设置为有助于恢复，则可以进行false回滚。
Hs4ma3G120-应在指定的时间段后移除已停止的 EC2 实例 相应的 AWS Security Hub CSPM 支票：EC2.4	AWSManagedServices-TerminateInstance (auto 和手动执行模式的默认 SSM 文档) 停止 30 天的 Amazon EC2 实例将被终止。	创建AMIBefore终止：. 要在终止实例之前创建实例 AMI 作为备份，请选择true。EC2 要在终止之前不创建备份，请选择false。默认值为true。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G120-应在指定的时间段后移除已停止的 EC2 实例 相应的 AWS Security Hub CSPM 支票：EC2.4	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime-在 Security Hub 中定义的停止天数 (默认值为 30) 的亚马逊 EC2 实例将被终止。	创建AMIBefore终止：要在终止实例之前创建实例 AMI 作为备份，请选择true。EC2 要在终止之前不创建备份，请选择false。默认值为true。 没有限制
Hs4ma3G121-应启用 EBS 默认加密 相应的 AWS Security Hub CSPM 支票：EC2.7	AWSManagedServices-EncryptEBSByDefault 默认情况下，Amazon EBS 加密是针对特定的 AWS 区域	不允许使用预配置参数。 默认加密是区域特定的设置。如果您为某个区域启用该功能，则无法为该区域的单个卷或快照禁用该功能。
Hs4Ma3G124-EC2 亚马逊实例应使用实例元数据服务版本 2 () IMDSv2 相应的 AWS Security Hub CSPM 支票：EC2.8	AWSManagedServices-TrustedRemote mediator启用EC2实例 IMDSv2 Amazon EC2 实例使用实例元数据服务版本 2 (IMDSv2)。	- IMDSv1MetricCheckPeriod：分析 IMDSv1 使用情况指标的天数 (42-455) CloudWatch。如果 Amazon EC2 实例是在指定时间段内创建的，则分析将从实例的创建日期开始。 - HttpPutResponseHopLimit：实例元数据令牌允许的最大网络跳数。可以在1和2跳数之间配置此值。跳跃限制为将令牌访问1限制为直接在实例上运行的进程，而跳跃限制为则2允许从实例上运行的容器进行访问。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G207-EC2 子网不应自动分配公有 IP 地址 相应的 AWS Security Hub CSPM 支票：EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4个地址 VPC 子网配置为不自动分配公有 IP 地址。	不允许使用预配置参数。 没有限制
Hs4ma3G209-未使用的网络访问控制列表已删除 相应的 AWS Security Hub CSPM 支票：EC2.16	AWSManagedServices-DeleteUnusedNACL 删除未使用的网络 ACL	不允许使用预配置参数。 没有限制
Hs4ma3G215-应移除未使用的 EC2 亚马逊安全组 相应的 AWS Security Hub CSPM 支票：EC2.22	AWSManagedServices-DeleteSecurityGroups 删除未使用的安全组。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G247-Amazon Transit Gateway EC2 不应自动接受 VPC 连接请求 相应的 AWS Security Hub CSPM 支票：EC2.23	AWSManagedServices-TrustedResourceMediatorDisableTGWAUTOVPCAttach-禁用自动接受指定非 Amazon Transit Gateway 的 VPC 连接请求。	不允许使用预配置参数。 没有限制
Hs4Ma3G235-ECR 私有存储库应配置标签不可变性 相应的 AWS Security Hub CSPM 支票：ECR.2	AWSManagedServices-TrustedResourceMediatorSetImageTagImmutability 将指定存储库的图像标签可变性设置为 IMMUTABLE。	不允许使用预配置参数。 没有限制
Hs4Ma3G216-ECR 存储库应至少配置一个生命周期策略 相应的 AWS Security Hub CSPM 支票：ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy ECR 存储库已配置生命周期策略。	LifecyclePolicyText：要应用于存储库的 JSON 存储库策略文本。 要启用 auto 修复，必须提供以下预配置参数： LifecyclePolicyText

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G325-EKS 集群应启用审核日志记录 相应的 AWS Security Hub CSPM 支票：EK S.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog 已为 EKS 集群启用审核日志。	不允许使用预配置参数。 没有限制
Hs4Ma3G183-应用程序负载均衡器应配置为丢弃 HTTP 标头 相应的 AWS Security Hub CSPM 支票：EL B.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer 配置为无效的标头字段。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G184-应启用应用程序负载均衡器和经典负载均衡器日志记录 相应的 AWS Security Hub CSPM 支票：EL B.5	AWSManagedServices-EnableELBLogging（auto 和手动执行模式的默认 SSM 文档） 应用程序负载均衡器和经典负载均衡器日志记录已启用。	• BucketName：存储桶名称（不是 ARN）。确保已正确配置存储桶策略以进行日志记录。 • S3KeyPrefix：Elastic Load Balancing 日志在 Amazon S3 存储桶中的位置的前缀。 要启用 auto 修复，必须提供以下预配置参数： • BucketName • S3KeyPrefix Amazon S3 存储桶必须具有存储桶策略，该策略授予 Elastic Load Balancing 将访问日志写入存储桶的权限。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G184-应启用应用程序负载均衡器和经典负载均衡器日志记录 相应的 AWS Security Hub CSPM 支票：EL B.5	AWSManagedServices-EnableELBLoggingV2 应用程序负载均衡器和经典负载均衡器日志记录已启用。	• TargetBucketTagKey：用于标识目标 Amazon S3 存储桶的标签名称（区分大小写）。使用它TargetBucketTagValue 来标记将用作访问日志的目标存储桶的存储桶。 • TargetBucketTagValue：用于标识目标 Amazon S3 存储桶的标签值（区分大小写）。使用它TargetBucketTagKey 来标记将用作访问日志的目标存储桶的存储桶。 • S3BucketPrefix：Amazon S3 存储桶的前缀（逻辑层次结构）。您指定的前缀不得包含字符串 AWSLogs。要获取更多信息，请参阅使用前缀整理对象。 要启用 auto 修复，必须提供以下预配置参数： • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix Amazon S3 存储桶必须具有存储桶策略，该策略授予 Elastic Load Balancing 将访问日志写入存储桶的权限。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G326-应启用亚马逊 EMR 屏蔽公开访问设置 相应的 AWS Security Hub CSPM 支票：EMR.2	AWSManagedServices-TrustedR emediatorEnableEMRBlockPublicAccess 该账户的 Amazon EMR 屏蔽公开访问设置已开启。	不允许使用预配置参数。 没有限制
Hs4ma3G135-AWS KMS 密钥不应无意中删除 相应的 AWS Security Hub CSPM 支票：KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS 密钥删除已取消。	不允许使用预配置参数。 没有限制
Hs4ma3G299-A Amazon DocumentDB 手动集群快照不应公开 相应的 AWS Security Hub CSPM 支票：Neptune.4	AWSManagedServices-TrustedR emediatorEnableNeptuneDBClusterDeletionProtection 为 Amazon Neptune 集群启用删除保护。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G319-Network Firewall 防火墙应该启用删除保护 相应的 AWS Security Hub CSPM 支票：Network Firewall.9	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection-为 AWS Network Firewall 启用删除保护。	不允许使用预配置参数。 没有限制
Hs4ma3G223-OpenSearch 域名应加密节点之间发送的数据 相应的 AWS Security Hub CSPM 支票：OpenSearch.3	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption 已为域启用节点到节点加密。	不允许使用预配置参数。 启用 node-to-node 加密后，您无法禁用该设置。取而代之的是，手动拍摄加密域的快照，创建另一个域，迁移您的数据，然后删除旧域名。
Hs4ma3G222-应该启用记录到日志的 OpenSearch 域名错误 CloudWatch 相应的 AWS Security Hub CSPM 支票：OpenSearch.4	AWSManagedServices-EnableOpenSearchLogging 已为该 OpenSearch 域启用错误日志记录。	CloudWatchLogGroupArn：亚马逊 CloudWatch 日志组的 ARN。 要启用 auto 修复，必须提供以下预配置参数：CloudWatchLogGroupArn。 Amazon CloudWatch 资源策略必须配置权限。有关更多信息，请参阅 Amazon OpenSearch 服务用户指南中的启用审计日志

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G221-OpenSearch 域名应启用审核日志 相应的 AWS Security Hub CSPM 支票：Open search.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch 域配置为启用审核日志。	CloudWatchLogGroupArn：要向其发布 CloudWatch 日志的日志组的 ARN。 要启用 auto 修复，必须提供以下预配置参数：CloudWatchLogGroupArn Amazon CloudWatch 资源策略必须配置权限。有关更多信息，请参阅 Amazon OpenSearch 服务用户指南中的启用审计日志
Hs4Ma3G220-与 OpenSearch 域名的连接应使用 TLS 1.2 进行加密 相应的 AWS Security Hub CSPM 支票：Open search.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 TLS 策略设置为“policy-min-tls-1-2-2019-07”，并且只允许通过 HTTPS (TLS) 进行加密连接。	不允许使用预配置参数。 使用 TLS 1.2 需要与 OpenSearch 域建立连接。加密传输中数据可能会影响性能。使用此功能测试您的应用程序，以了解 TLS 的性能状况和影响。
Hs4ma3G194-亚马逊 RDS 快照应该是私有的 相应的 AWS Security Hub CSPM 支票：RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 Amazon RDS 快照的公共访问已禁用。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G192-RDS 数据库实例应禁止公共访问，具体取决于配置 PubliclyAccessible AWS 相应的 AWS Security Hub CSPM 支票：RDS.2	AWSManagedServices-TrustedR emediatorDisablePublicAccessOnRDSInstance 在 RDS 数据库实例上禁用公共访问权限。	不允许使用预配置参数。 没有限制
Hs4Ma3G189-为亚马逊 RDS 数据库实例配置了增强监控 相应的 AWS Security Hub CSPM 支票：RDS.6	AWSManagedServices-TrustedR emediatorEnableRDSEnhancedMonitoring 为 Amazon RDS 数据库实例启用增强监控	- MonitoringInterval：为数据库实例收集增强监控指标的时间间隔，以秒为单位。有效间隔为 0、1、5、10、15、30 和 60。要禁用收集增强监控指标，请指定 0。 - MonitoringRoleName：允许 Amazon RDS 向 Amazon CloudWatch Logs 发送增强型监控指标的 IAM 角色的名称。如果未指定角色，rds-monitoring-role 则使用或创建默认角色（如果该角色不存在）。 如果在自动化执行之前启用了增强监控，则此自动化可能会使用在预配置参数中配置的 MonitoringInterval 和 MonitoringRoleName 值来覆盖这些设置。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G190-Amazon RDS 集群应启用删除保护 相应的 AWS Security Hub CSPM 支票：RDS.7	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection 已为 Amazon RDS 集群启用删除保护。	不允许使用预配置参数。 没有限制
Hs4Ma3G198-Amazon RDS 数据库实例应启用删除保护 相应的 AWS Security Hub CSPM 支票：RDS.8	AWSManagedServices-TrustedR emediatorEnableRDSDeletionP rotection 已为 Amazon RDS 实例启用删除保护。	不允许使用预配置参数。 没有限制
Hs4Ma3G199-RDS 数据库实例应将日志发布到日志 CloudWatch 相应的 AWS Security Hub CSPM 支票：RDS.9	AWSManagedServices-TrustedR emediatorEnableRDSLogExports 已为 RDS 数据库实例或 RDS 数据库集群启用 RDS 日志导出。	不允许使用预配置参数。 需要服务相关角色 AWSServiceRoleForRDS。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G160-应为 RDS 实例配置 IAM 身份验证 相应的 AWS Security Hub CSPM 支票：RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management 已为 RDS 实例启用身份验证。	ApplyImmediately: 表示是否尽快异步应用此请求中的修改和任何待处理的修改。要立即应用更改，请选择true。要在下一个维护时段安排更改，请选择false。 没有限制
Hs4Ma3G161-应为 RDS 集群配置 IAM 身份验证 相应的 AWS Security Hub CSPM 支票：RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication 已为 RDS 集群启用了 IAM 身份验证。	ApplyImmediately: 表示是否尽快异步应用此请求中的修改和任何待处理的修改。要立即应用更改，请选择true。要在下一个维护时段安排更改，请选择false。 没有限制
Hs4Ma3G162-应启用 RDS 自动次要版本升级 相应的 AWS Security Hub CSPM 支票：RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade Amazon RDS 的自动次要版本升级配置已启用。	不允许使用预配置参数。 Amazon RDS 实例必须处于available 状态才能进行此修复。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G163-RDS 数据库集群应配置为将标签复制到快照 相应的 AWS Security Hub CSPM 支票：RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagstosnapshot Amazon RDS 集群的设置已启用。	不允许使用预配置参数。 Amazon RDS 实例必须处于可用状态才能进行此修复。
Hs4Ma3G164-RDS 数据库实例应配置为将标签复制到快照 相应的 AWS Security Hub CSPM 支票：RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots CopyTagsToSnapshot Amazon RDS 的设置已启用。	不允许使用预配置参数。 Amazon RDS 实例必须处于可用状态才能进行此修复。
rss93 HQwa1 Amazon RDS 公有快照	AWSManagedServices-DisablePublicAccessOnRDSnapshotV2 Amazon RDS 快照的公共访问已禁用。	不允许使用预配置参数。 没有限制
Hs4ma3G103-亚马逊 Redshift 集群应禁止公众访问 相应的 AWS Security Hub CSPM 支票：Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster 亚马逊 Redshift 集群上的公共访问已禁用。	不允许使用预配置参数。 禁用公共访问会阻止所有来自互联网的客户端。而且，Amazon Redshift 集群在几分钟内处于修改状态，同时修复会禁用集群上的公共访问权限。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G106-亚马逊 Redshift 集群应启用审核日志 相应的 AWS Security Hub CSPM 支票：Redshift ft.4	AWSManagedServices-TrustedRedshiftClusterAuditLogging 在维护时段内，您的 Amazon Redshift 集群启用了审核日志。	不允许使用预配置参数。 要启用 auto 修复，必须提供以下预配置参数。 BucketName: 存储桶必须位于同一个桶中 AWS 区域。集群必须具有读取存储桶和放置对象权限。 如果在自动化执行之前启用了 Redshift 集群日志记录，则该自动化可能会使用在预配置参数中配置的 BucketName 和 S3KeyPrefix 值覆盖日志设置。
Hs4ma3G105-Amazon Redshift 应该启用自动升级到主要版本的功能 相应的 AWS Security Hub CSPM 支票：Redshift ft.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade-在维护时段内，主要版本升级会自动应用于集群。Amazon Redshift 集群不会立即停机，但是如果升级到主要版本，您的 Amazon Redshift 集群可能会在其维护时段内停机。	不允许使用预配置参数。 没有限制
Hs4ma3G104-亚马逊 Redshift 集群应使用增强型 VPC 路由 相应的 AWS Security Hub CSPM 支票：Redshift ft.7	AWSManagedServices-TrustedRedshiftClusterEnhancedVPCRouting 亚马逊 Redshift 集群已启用增强型 VPC 路由。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G173-S3 阻止公共访问设置应在存储桶级别启用 相应的 AWS Security Hub CSPM 支票：S3.8	AWSManagedServices-TrustedRolemediatorBlockS3BucketPublicAccess Amazon S3 存储桶采用存储桶级别的公共访问封禁。	不允许使用预配置参数。 此补救措施可能会影响 S3 对象的可用性。有关 Amazon S3 如何评估访问权限的信息，请参阅阻止公众访问您的 Amazon S3 存储。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G230-S3 存储桶服务器访问日志应启用 相应的 AWS Security Hub CSPM 支票：S3.9	AWSManagedServices-EnableBucketAccessLogging (auto 和手动执行模式的默认 SSM 文档) Amazon S3 服务器访问日志已启用。	• TargetBucket：用于存储服务器访问日志的 S3 存储桶的名称。 • TargetObjectKeyFormat: 日志对象的 Amazon S3 密钥格式 (值区分大小写)。要对日志对象使用 S3 密钥的简单格式，请选择SimplePrefix。要对日志对象使用分区 S3 密钥并使用 EventTime 分区前缀，请选择。PartitionedPrefixEventTime 要对日志对象使用分区 S3 密钥并使用 DeliveryTime 分区前缀，请选择。PartitionedPrefixDeliveryTime 有效值为 SimplePrefix、PartitionedPrefixEventTime 和 PartitionedPrefixDeliveryTime。 要启用 auto 修复，必须提供以下预配置参数：TargetBucket。 目标存储桶必须与源存储桶位于 AWS 账户 相同 AWS 区域 且具有正确的日志传输权限。有关更多信息，请参阅启用 Amazon S3 服务器访问日志记录。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G230 — 应启用 S3 存储桶服务器访问日志记录 相应的 AWS Security Hub CSPM 支票：S3.9	AWSManagedServices-TrustedResourceMediatorEnableBucketAccessLoggingV2-已启用 Amazon S3 存储桶日志记录。	• TargetBucketTagKey：用于标识目标存储桶的标签名称（区分大小写）。使用此和标记TargetBucketTagValue要用作访问日志记录的目标存储桶的存储桶。 • TargetBucketTagValue：标签值（区分大小写），用于标识目标存储桶、使用该值以及标记TargetBucketTagKey要用作访问日志记录的目标存储桶的存储桶。 • TargetObjectKeyFormat: 日志对象的 Amazon S3 密钥格式（值区分大小写）：要使用日志对象的 S3 密钥的简单格式，请选择SimplePrefix。要对日志对象使用分区 S3 密钥并使用 EventTime 分区前缀，请选择。PartitionedPrefixEventTime要对日志对象使用分区 S3 密钥并使用 DeliveryTime 分区前缀，请选择。PartitionedPrefixDeliveryTime默认值为 PartitionedPrefixEventTime。 要启用 auto 修复，必须提供以下参数：TargetBucketTagKey 和TargetBucketTagValue。 目标存储桶必须与源存储桶位于 AWS 账户 相同 AWS 区域 且具有正确的日志传输权限。有关更多信息，请参阅启用 Amazon S3 服务器访问日志记录。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Pfx0 RwgBli Amazon S3 存储桶权限	AWSManagedServices-TrustedR emediatorBlockS3BucketPubli cAccess 阻止公有访问	不允许使用预配置参数。 此检查由多个警报标准组成。这种自动化修复了公共访问问题。Trusted Advisor 不支持修复标记为的其他配置问题。此修复确实支持修复 AWS 服务已创建的 S3 存储桶 (例如 cf-templates-000000000000) 。
Hs4Ma3G272-用户不应拥有笔记本实例的根访问权限 SageMaker 相应的 AWS Security Hub CSPM 支票 : SageMaker .3	AWSManagedServices-TrustedR emediatorDisableSageMakerNo tebookInstanceRootAccess 对于 SageMaker 笔记本实例，用户的 root 访问权限已禁用。	不允许使用预配置参数。 如果 SageMaker 笔记本实例 InService 处于状态，则此补救措施会导致中断。
Hs4Ma3G179-SNS 主题应使用静态加密 AWS KMS 相应的 AWS Security Hub CSPM 支票 : SNS.1	AWSManagedServices-EnableSN SEncryptionAtRest SNS 主题配置了服务器端加密。	KmsKeyId : 适用于 Amazon SNS 的 AWS 托管客户主密钥 (CMK) 或用于服务器端加密 (SSE) 的自定义 CMK 的 ID。默认值设置为 alias/aws/sns。 如果使用自定义 AWS KMS 密钥，则必须为其配置正确的权限。有关更多信息，请参阅 Amazon SNS 主题的启用服务器端加密 (SSE)

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4ma3G158-SSM 文档不应公开 相应的 AWS Security Hub CSPM 支票：SSM.4	AWSManagedServices-TrustedR emediatorDisableSSMDocPubli cSharing-禁用 SSM 文档的公开共 享。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Hs4Ma3G136-亚马逊 SQS 队列应在静态时加密 相应的 AWS Security Hub CSPM 支票：SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest 亚马逊 SQS 中的消息经过加密。	• SqsManagedSseEnabled：设置true为使用Amazon SQS拥有的加密密钥启用服务器端队列加密，设置false为使用密钥启用服务器端队列加密。AWS KMS • KMSKeyID：Amazon SQS 的 AWS 托管客户主密钥 (CMK) 或用于队列服务器端加密的自定义 CMK 的 ID 或别名。如果未提供，alias/aws/sqs则使用。 • KmsDataKeyReusePeriodSeconds：在再次调用之前，Amazon SQS 可以重复使用数据密钥来加密或解密消息的时间长度，以秒为单位。AWS KMS 一个表示秒数的证书，介于 60 秒（1 分钟）和 86400 秒（24 小时）之间。如果设置为，SqsManagedSseEnabled 则忽略此设置true。 匿名 SendMessage 和对加密队列的 ReceiveMessage 请求将被拒绝。针对启用了 SSE 的队列的所有请求都必须使用 HTTPS 和 Signature Version 4。

Trusted Advisor 可信修正者支持的容错检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c18d2gz138 亚马逊 DynamoDB 恢复 Point-in-time	AWSManagedServices-TrustedR emediatorEnableDDBPITR 启用 DynamoDB 表的 point-in-time 恢复。	不允许使用预配置参数。 没有限制
r365s2qddf Amazon S3 Bucket Versionin g	AWSManagedServices-TrustedR emediatorEnableBucketVersioning Amazon S3 存储桶版本控制已启用。	不允许使用预配置参数。 此修复不支持修复 AWS 服务 已创建的 S3 存储桶 (例如 cf-templa tes-0000000000000) 。
BueAdj7nrp Amazon S3 存储 桶日志记录	AWSManagedServices-EnableBu cketAccessLogging 已启用 Amazon S3 存储桶日志记 录。	• TargetBucket : 用于存储服务器访问日志的 S3 存储桶的名称。 • TargetObjectKeyFormat: 日志对象的 Amazon S3 密钥格式, 要使用日志对象的 S3 密钥的简单格式, 请选择SimplePrefix 。要对日志对象使用分区 S3 密钥并使用 EventTime 分区前缀, 请选择。PartitionedPrefixEventTime 要对日志对象使用分区 S3 密钥并使用 DeliveryTime 分区前缀, 请选择。PartitionedPrefixDeliveryTime 默认值为 PartitionedPrefixEventTime 。有效值为SimplePrefix 、 PartitionedPrefixEventTime 和PartitionedPrefixDeliveryTime (区分大小写) 。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
		要启用 auto 修复，必须提供以下预配置参数： TargetBucket 目标存储桶必须与源存储桶位于 AWS 账户相同 AWS 区域 且具有正确的日志传输权限。有关更多信息，请参阅启用 Amazon S3 服务器访问日志记录。
f2ik5r6dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ 已启用多可用区部署。	不允许使用预配置参数。 在此更改期间，性能可能会降低。
H7 lgTzj TYb Amazon EBS Snapshots	AWSManagedServices-TrustedRemediatorCreateEBSSnapshot 亚马逊 EBSsnapshots 已创建。	不允许使用预配置参数。 没有限制
op QPADk zvH RDS 备份	AWSManagedServices-EnableRDSBackupRetention 已为数据库启用 Amazon RDS 备份保留功能。	- BackupRetentionPeriod：保留自动备份的天数 (1-35)。 - ApplyImmediately：表示是否尽快异步应用 RDS 备份保留期更改和任何待处理的修改。true 选择立即应用更改，或者 false 将更改安排到下一个维护时段。 如果将 ApplyImmediately 参数设置为 true，则数据库上待处理的更改将与 RDSBackup 保留设置一起应用。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1qf5bt013 Amazon RDS 数据库实例已关闭存储自动扩缩功能	AWSManagedServices-TrustedR emediatorEnableRDSInstanceS torageAutoScaling-已为 Amazon RDS 数据库实例启用存储自动扩展。	MaxAllocatedStorageIncrease Percentage: 电流的增加百分比 AllocatedStorage，用于设置 MaxAllocatedStorage。默认值设置为 26。 您必须将最大存储阈值设置为比当前分配的存储空间至少多 10%。最佳做法是将最大存储阈值设置为至少 26%。有关详细信息，请查看使用 Amazon Relational Database Service 存储自动扩展功能自动管理容量。 没有限制
7q GXs KIUw Classic Load Balancer Connection 耗尽	AWSManagedServices-TrustedR emediatorEnableCLBConnectio nDraining Classic Load Balancer 已启用连接耗尽功能。	ConnectionDrainingTimeout：取消注册实例之前保持现有连接打开状态的最长时间（以秒为单位）。默认设置为 300 秒。
c18d2gz106 计划中 AWS Backup 未包含亚马逊 EBS	AWSManagedServices-TrustedR emediatorAddVolumeToBackupPlan Amazon EBS 已包含在 AWS Backup 计划中。	补救措施使用以下标签对标记 Amazon EBS 卷。标签对必须符合的基于标签的资源选择标准。AWS Backup - TagKey - TagValue 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c18d2gz107 计划中未包含亚马逊 DynamoDB 表 AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan 计划中包含亚马逊 DynamoDB 表。AWS Backup	补救措施使用以下标签对标记 Amazon DynamoDB。标签对必须符合的基于标签的资源选择标准。AWS Backup • TagKey • TagValue 没有限制
c18d2gz117 AWS Backup 计划中未包含亚马逊 EFS	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS 包含在 AWS Backup 计划中。	补救措施使用以下标签对 Amazon EFS 进行标记。标签对必须符合的基于标签的资源选择标准。AWS Backup • TagKey • TagValue 没有限制
c18d2gz105 网络负载均衡器 跨区域负载均衡	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing 在 Network Load Balancer 上启用了跨区域负载平衡。	不允许使用预配置参数。 没有限制
c1qf5bt026 亚马逊 RDS synchronous_commit 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Amazon RDS 的参数 synchronous_commit 已开启。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1qf5bt030 亚马逊 RDS innodb_flush_log_at_trx_commit 参数不是 1	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter 对innodb_flush_log_at_trx_commit 于 Amazon RDS1，参数设置为。	不允许使用预配置参数。 没有限制
c1qf5bt031 亚马逊 RDS sync_binlog 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的参数sync_binlog 已开启。	不允许使用预配置参数。 没有限制
c1qf5bt036 Amazon RDS innodb_default_row_format 参数设置不安全	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter 对innodb_default_row_format 于 Amazon RDS DYNAMIC，参数设置为。	不允许使用预配置参数。 没有限制
c18d2gz144 未启用 Amazon EC2 详细监控	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring 已为 Amazon 启用详细监控 EC2。	不允许使用预配置参数。 没有限制

Trusted Advisor 可信修正者支持的性能检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
COr6dfpM06 AWS Lambda 内存大小的函数配置不足	AWSManagedServices-ResizeLambdaMemory Lambda 函数的内存大小已调整为提供的建议内存大小。Trusted Advisor	RecommendedMemorySize : Lambda 函数的推荐内存分配。值范围介于 128 和 10240 之间。 如果在自动执行之前修改了 Lambda 函数的大小，则此自动化可能会使用推荐的值覆盖设置。Trusted Advisor
ZRxQIPsb6c 高利用率 Amazon EC2 实例	AWSManagedServices-ResizeInstanceByOneLevel 在相同的 EC2 实例系列中，Amazon 实例按一种实例类型向上调整大小。在调整大小操作期间，实例将停止并启动，并在执行完成后返回到初始状态。此自动化不支持调整 Auto Scaling 组中的实例的大小。	• MinimumDaysSinceLastChange : 自上次实例类型更改以来的最短天数。如果在指定时间内修改了实例类型，则不会更改实例类型。0 用于跳过此验证。默认值为 7。 • 创建AMIBefore调整大小：要在调整大小之前创建实例 AMI 作为备份，请选择true。要不创建备份，请选择false。默认值为 false。有效值为true和false (区分大小写)。 • ResizelfStopped : 要继续更改实例大小，即使实例处于停止状态，也请选择true。要在实例处于停止状态时不自动调整其大小，请选择false。有效值为true和false (区分大小写)。 没有限制
c1qf5bt021 使用小于最佳值的 Amazon RDS	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
innodb_change_buffering 参数	对于 Amazon RDS , innodb_change_buffering 参数NONE的值设置为。	
c1qf5bt025 亚马逊 RDS autovacuum 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的参数autovacuum 已开启。	不允许使用预配置参数。 没有限制
c1qf5bt028 亚马逊 RDS enable_indexonlyscan 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的参数enable_indexonlyscan 已开启。	不允许使用预配置参数。 没有限制
c1qf5bt029 亚马逊 RDS enable_indexscan 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的参数enable_indexscan 已开启。	不允许使用预配置参数。 没有限制
c1qf5bt032 亚马逊 RDS innodb_stats_persistent 参数已关闭	AWSManagedServices-TrustedRemediatorRemediateRDSParaterGroupParameter Amazon RDS 的参数innodb_stats_persistent 已开启。	不允许使用预配置参数。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1qf5bt037 亚马逊 RDS general_logging 参数已开启	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter 亚马逊 RDS 的参数 general_logging 已关闭。	不允许使用预配置参数。 没有限制

Trusted Advisor 受信任修正者支持的服务限制检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
ln7rr0l7j9 EC2-VPC 弹性 IP 地址	AWSManagedServices-UpdateVpcElasticIPQuota 请求对 EC2-VPC 弹性 IP 地址设置新的限制。默认情况下，该限制会增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用 OK 状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
km7qq0l7j9 VPC 互联网网关	AWSManagedServices-IncreaseServiceQuota-请求对 VPC 互联网网关设置新的限制。默认情况下，该限制增加三个。	增量：要增加当前配额的数字。默认值为 3。 如果在使用 OK 状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
jl7pp0l7j9 VPC	AWSManagedServices-IncreaseServiceQuota 请求对 VPC 设置新的限制。默认情况下，该限制增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用 OK 状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
fw7hh0l7j9	AWSManagedServices-IncreaseServiceQuota	增量：要增加当前配额的数字。默认值为 3。

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
Auto Scaling 组	请求对 Auto Scaling 组设置新的限制。默认情况下，该限制增加 3。	如果在使用 OK 状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
3njm0 DJQO9 RDS 选项组	AWSManagedServices-Increase ServiceQuota 请求对 Amazon RDS 选项组设置新的限制。默认情况下，该限制增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用 OK 状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
EM8b3yLRTr ELB Application Load Balancer	AWSManagedServices-Increase ServiceQuota 请求对 ELB 应用程序负载均衡器设置新的限制。默认情况下，该限制增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用 OK 状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。
8wiQ K YSt25 ELB Network Load Balancer	AWSManagedServices-Increase ServiceQuota 请求对 ELB 网络负载均衡器设置新的限制。默认情况下，该限制增加 3。	增量：要增加当前配额的数字。默认值为 3。 如果在使用 OK 状态更新 Trusted Advisor 支票之前多次运行此自动化，则可能会增加更高的限额。

Trusted Advisor 可信修正者支持的卓越运营检查

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c18d2gz125 Amazon API Gateway 未记录执行日志	AWSManagedServices-TrustedRemediatorEnableAPIGatewayExecutionLogging API 阶段已启用执行日志记录。	不允许使用预配置参数。 要启用执行日志，您必须授予 API Gateway 读取和写入账户日志的权限，有关详细信息，请参阅 APIs

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
		在 API Gateway 中设置 REST CloudWatch 日志记录 。CloudWatch
c18d2gz168 没有为负载均衡器启用 Elastic Load Balancing 删除保护	AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection-Elastic Load Balancer 的删除保护已开启。	不允许使用预配置参数。 没有限制
c1qf5bt012 Amazon RDS Performance Insights	AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights 亚马逊 RDS 的 Performance Insights 已开启。	- PerformanceInsightsRetentionPeriod : 保留 Performance Insights 数据的天数。有效值 : 7或月 * 31 , 其中月是 1-23 之间的月数。示例 : 93 (3 个月 * 31) 、 341 (11 个月 * 31) 、 589 (19 个月 * 31) 或731。 - PerformanceInsightsKMSKeyID : Performance Insights 数据加密的密 AWS KMS 钥 ID。如果您没有为 PerformanceInsights KMSKey ID 指定值 , 则 Amazon RDS 将使用您的默认 AWS KMS 密钥。 没有限制

检查身份证和姓名	SSM 文档名称和预期结果	支持的预配置参数和约束
c1fd6b96l4 已启用 Amazon S3 访问日志	AWSManagedServices-TrustedR emediatorEnableBucketAccess LoggingV2 Amazon S3 存储桶访问日志已启用。	• TargetBucketTagValue : 标签值 (区分大小写) , 用于标识目标存储桶、使用该值以及标记 TargetBucketTagKey 要用作访问日志记录的目标存储桶的存储桶。 • TargetObjectKeyFormat: 日志对象的 Amazon S3 密钥格式 (值区分大小写) 。要对日志对象使用 S3 密钥的简单格式, 请选择SimplePrefix 。要对日志对象使用分区 S3 密钥并使用 EventTime 分区前缀, 请选择。PartitionedPrefixEventTime 要对日志对象使用分区 S3 密钥并使用 DeliveryTime 分区前缀, 请选择。PartitionedPrefixDeliveryTime 有效值为 SimplePrefix 、 PartitionedPrefixEventTime 和 PartitionedPrefixDeliveryTime 。 要启用 auto 修复, 必须提供以下预配置参数: TargetBucketTagKey 和 TargetBucketTagValue 目标存储桶必须与源存储桶位于 AWS 账户 相同 AWS 区域 且具有正确的日志传输权限。有关更多信息, 请参阅启用 Amazon S3 服务器访问日志记录。

在可信修正器中配置 Trusted Advisor 检查修复

配置 AWS AppConfig 作为可信修正者应用程序的一部分存储在中。每个 Trusted Advisor 检查类别都有单独的配置文件。有关 Trusted Advisor 类别的更多信息，请参阅[查看支票类别](#)。

您可以请求按资源或按 Trusted Advisor 检查配置补救措施。您可以使用资源标签来应用例外。

Note

目前使用配置了对 Trusted Advisor 发现结果的补救 AWS AppConfig，目前已完全支持此功能。AMS 预计，这种情况将来会改变。最佳做法是避免构建依赖的自动化 AWS AppConfig，因为这种方法可能会发生变化。请注意，为了兼容性，将来可能需要更新或修改围绕当前 AWS AppConfig 实现构建的自动化。

Compute Optimizer-> EC2 实例功能标志有额外的参数：

- allow-upscale 允许配置不足但未经过优化的高档实例。EC2 默认值为“false”。
- min-savings-opportunity-percentage 自动修复的最低节省百分比机会。默认值为 10%

默认补救配置

单个 Trusted Advisor 检查的配置存储为 AWS AppConfig 标志。旗帜名称与支票名称相匹配。每个检查配置都包含以下属性：

- 执行模式：确定可信修正者如何执行默认修复：
 - 自动：Trusted Remediator 通过创建资源来自动修复资源 OpsItem，运行 SSM 文档，然后在成功执行 OpsItem 后解决问题。
 - 手动：OpsItem 已创建，但是 SSM 文档不会自动执行。您可以查看 OpsItem 并使用自动 RFC 进行修复。有关更多信息，请参阅[在“可信修正者”中使用补救措施](#)。
 - 有条件的：默认情况下，修正处于禁用状态。您可以使用标签为特定资源启用它。有关更多信息，请参阅以下各节[使用资源标签自定义补救措施](#)和[使用资源覆盖标签自定义补救措施](#)。
 - 非活动：不会进行修复，OpsItem 也不会创建任何修复。对于设置为非活动状态的 Trusted Advisor 支票，您无法覆盖其执行模式。
- 预配置参数：输入自动修复所需的 SSM 文档参数的值，格式为，用逗号 (Parameter=Value,) 分隔。有关每[Trusted Advisor 受信任修正者支持的检查](#)项检查的关联 SSM 文档支持的预配置参数，请参阅。

- `alternative-automation-document`：此属性有助于用另一个支持的文档覆盖现有的自动化文档（如果可用于特定检查）。默认情况下，此属性处于未选中状态。

Note

该 `alternative-automation-document` 属性不支持自定义自动化文档。您可以使用中列出的现有受支持的可信修正者自动化文档。[Trusted Advisor 受信任修正者支持的检查](#) 例如，为了便于检查 Qch7DwouX1，有三个关联的 SSM 文档：AWSManagedServices-StopEC2Instance、AWSManagedServices-ResizeInstanceByOneLevel、和 AWSManagedServices-TerminateInstance 的值 `alternative-automation-document` 可以是 AWSManagedServices-ResizeInstanceByOneLevel 或 AWSManagedServices-TerminateInstance（AWSManagedServices-StopEC2Instance 是要修复 Qch7DwouX1 的默认 SSM 文档）。

每个属性的值必须与该属性的约束条件相匹配。

Tip

在为 Trusted Advisor 检查应用默认配置之前，最好考虑使用以下各节中描述的资源标记和资源覆盖功能。默认配置适用于账户内的所有资源，这可能并非在所有情况下都是理想的。

以下是控制台屏幕截图示例，其中执行模式设置为“手动”，且属性与其约束条件相匹配。

使用资源标签自定义补救措施

校验配置中的 `automated-for-tagged-only` 和 `manual-for-tagged-only` 属性允许您指定资源标签，说明如何修复单个检查。当您需要对共享相同标签的一组资源应用一致的修复行为时，最好使用此方法。以下是这些标签的描述：

- `automated-for-tagged-only`：指定资源标签（一个或多个标签对，以逗号分隔），以便检查自动修复，无论默认执行模式如何。
- `manual-for-tagged-only`：为无论默认执行模式如何，都应手动执行的修复指定资源标签（一个或多个标签对，以逗号分隔）。

例如，如果您要为所有非生产资源启用自动修复并对生产资源强制执行手动修复，则可以按以下方式设置配置：

```
"execution-mode": "Conditional",  
"automated-for-tagged-only": "Environment=Non-Production",  
"manual-for-tagged-only": "Environment=Production",
```

在您的资源上设置了上述配置后，检查修复行为如下所示：

- 标有“环境=非生产”的资源会自动修复。
- 标有“环境=生产”的资源需要手动干预才能进行修复。
- 没有“环境”标签的资源遵循默认的执行模式（在本例中为“条件”）。因此，不会对剩余资源采取任何行动）。

要获得有关配置的更多支持，请联系您的云架构师。

使用资源覆盖标签自定义补救措施

资源覆盖标签允许您自定义单个资源的修复行为，无论其标签如何。通过向资源添加特定标签，可以覆盖该资源和 Trusted Advisor 检查的默认执行模式。资源覆盖标签优先于默认配置和资源标记设置。因此，如果您使用资源覆盖标签将资源的默认执行模式设置为“自动”、“手动”或“有条件”，则它将覆盖默认执行模式和任何资源标记配置。

要覆盖资源的执行模式，请完成以下步骤：

1. 确定要覆盖其修复配置的资源。
2. 确定要 Trusted Advisor 改写的支票的支票编号。您可以在中找到支持的签 IDs 入的 Trusted Advisor 支票[Trusted Advisor 受信任修正者支持的检查](#)。
3. 使用 Tag | Update 或 [Tag | Bulk Update](#) 更改类型向具有以下键和值的资源添加标签：

- 标签密钥:TR-*Trusted Advisor check ID*-Execution-Mode (区分大小写)

在前面的标签密钥示例中，Trusted Advisor check ID 替换为要覆盖的 Trusted Advisor 支票的唯一标识。

- 标签值：使用以下值之一作为标签值：
 - 自动：受信任的修正者会自动修复此 Trusted Advisor 检查的资源。
 - 手动：已 OpsItem 为资源创建，但不会自动执行修复。您可以使用自动检查并运行补救措施。有关更多信息，请参阅 [在“可信修正者”中使用补救措施](#)。

- 非活动：未对此资源和指定的 Trusted Advisor 检查执行修复和 OpsItem 创建。

例如，要使用 Trusted Advisor 支票编号自动修复 Amazon EBS 卷，请向 EBS 卷 DAvU99Dc4C 添加标签。标签键为 TR-DAvU99Dc4C-Execution-Mode，标签值为 Automated。

以下是显示标签部分的控制台示例：

执行模式决策工作流程

有多个级别可以为您的资源和每项 Trusted Advisor 检查配置执行模式。下图显示了 Trusted Remediator 如何根据您的配置决定使用哪种执行模式：

配置补救教程

以下教程提供了在 Trusted Remediator 中创建常见补救措施的示例

手动修复所有资源

此示例为 Trusted Advisor 支票编号为 DAv U99Dc4C（未充分利用的亚马逊 EBS 卷）的所有亚马逊 EBS 卷配置手动修复。

为支票编号 DAv 为 U99dc4C 的亚马逊 EBS 卷配置手动修复

1. 使用“修正配置|更新”，更改类型来请求配置更新。
2. 输入以下参数：
 - CheckIds: DAv U99Dc 4C
 - ExecutionMode: 手册

Note

可以在单个请求中配置多项检查。对于需要相同配置的校验，请在 CheckIds 参数 IDs 中包括多重校验。对于需要不同配置的检查，请创建一个新 RemediationConfiguration 对象。

3. 提交 RFC。

自动修复所有资源，所选资源除外

此示例为 Trusted Advisor 支票 ID DAv U99Dc4C (未充分利用的 Amazon EBS 卷) 的所有 Amazon EBS 卷配置自动修复，但无法修复的指定卷 (指定为“非活动”) 除外。

为支票编号为 DAv U99dc4C 的 Amazon EBS 卷配置自动修复，选定的非活动资源除外

1. 覆盖对选定的 Amazon EBS 卷的自动修复：

使用 [Tag | Update](#) 或 [Tag | Bulk Update](#) 更改类型为要从自动修复中排除的卷应用以下标记：

- 密钥：TR-DAv U99Dc4C-Execution-Mode
- 值：非活动

2. 使用“修正配置”|“更新”更改类型来请求配置更新。

3. 输入以下参数：

- CheckIds: DAv U99Dc 4C
- ExecutionMode: 自动化

4. 提交 RFC。

自动修复已标记的资源

此示例为带有 Trusted Advisor 支票 ID DAv U99Dc4C (未充分利用的 Amazon EBS 卷) 标签 Stage=NonProd 的所有亚马逊 EBS 卷配置自动修复。没有此标签的所有其他资源都不会被修复。

使用支票 ID DAv U99dc4C 的标签 **Stage=NonProd** 为亚马逊 EBS 卷配置自动修复

1. 使用“[修正配置](#)”|“[更新](#)”，更改类型”来请求配置更新。

2. 输入以下参数：

- CheckIds: DAv U99Dc 4C
- ExecutionMode: 有条件的
- AutomatedForTaggedOnly: {“舞台”:“ NonProd “}

Note

为AutomatedForTaggedOnly参数指定的值将覆盖先前配置的值。要保留现有标签，请将其包含在新值中。

3. 提交 RFC。

将配置重置为默认值

此示例删除了检查 Hs4 ma3G104 的现有automated-for-tagged-only配置。要移除先前应用的标签配置，请将AutomatedForTaggedOnly参数值设置为 {}。

将配置重置为默认值以进行检查 Hs4ma3G104

1. 使用 [“修正配置”](#) | [“更新”](#) 更改类型来请求配置更新。
2. 输入以下参数：
 - CheckIds: Hs4ma3 G104
 - ExecutionMode: 输入当前使用的值
 - AutomatedForTaggedOnly: {}
3. 提交 RFC。

在“可信修正者”中使用补救措施

在“可信修正者”中跟踪补救措施

要跟踪 OpsItems 修正情况，请完成以下步骤：

1. 打开 AWS Systems Manager 控制台，网址为<https://console.aws.amazon.com/systems-manager/>。
2. 选择“运营管理”，OpsCenter。
3. （可选）按“来源 = 可信修正者”筛选列表，以便在列表中仅包括受信任的修正者 OpsItems 。

以下是按来源=可信修正者筛选的 OpsCenter 屏幕示例：

Note

除了 OpsItems 从中查看之外 OpsCenter，您还可以查看 AMS S3 存储桶中的修复日志。有关更多信息，请参阅 [可信修正者中的修复日志](#)。

在“可信修正器”中运行手动修复

可信修正者为配置 OpsItems 为手动修复的检查进行创建。您必须查看这些检查并手动开始修复过程。

要手动修复 OpsItem，请完成以下步骤：

1. 打开 AWS Systems Manager 控制台，网址为 <https://console.aws.amazon.com/systems-manager/>。
2. 选择“运营管理”，OpsCenter。
3. （可选）按“来源 = 可信修正者”筛选列表，以便在列表中仅包括受信任的修正者 OpsItems。
4. 选择您 OpsItem 要查看的。
5. 查看的操作数据 OpsItem。操作数据包括以下项目：
 - trustedAdvisorCheck类别：支 Trusted Advisor 票编号的类别。例如，容错
 - trustedAdvisorCheckID：唯一的 Trusted Advisor 支票编号。
 - trustedAdvisorCheck元数据：资源元数据，包括资源 ID。
 - trustedAdvisorCheck名称：支 Trusted Advisor 票的名称。
 - trustedAdvisorCheck状态：检测到的资源 Trusted Advisor 检查的状态。
 - trustedAdvisorCheckManualRemediation：为手动修复提供参考详细信息的自定义数据。
 - ManualExecutionInput：一个对象，它定义了在执行手动修复时可以修改其值的参数。
 - DocumentName: 运行手册的名称（SSM 文档）。
 - CustomizableParameters：您可以修改的参数名称。
 - DefaultInput：定义用于手动修复的参数名称和值的对象。这些值是根据预配置的参数填充的。
6. 要手动修复 OpsItem，请完成以下步骤：
 - a. 使用[可信修正者 | 发现 | 修复 ct-1c7ch8z5phrj p](#)更改类型
 - b. 输入以下参数的值：

- `DocumentName`: 一定是 `AWSManagedServices-RemediateTrustedRemediatorFinding`。
- 区域: 的 AWS 区域, 格式为 `us-east-1`。
- 参数: 输入手动修复参数:
 - `OpsItemId`: 行动物品的 ID。
 - `RemediationDocumentName`: 要使用的 SSM 自动化文档的名称。该文档必须与 Ops 项目关联。如果有多个文档与 Ops Item 关联, 则 `DocumentName` 必须指定。
 - `RemediationParameters`: 自动化执行的参数 key/value 映射, 格式为: `{\"ParameterName1\": [\"ParameterValue1\"], \"ParameterName2\": [\"ParameterValue2\"]}`。你只能使用行动物品中存在的参数 `trustedAdvisorCheckManualRemediation CustomizableParameters`。如果未指定, 则从 Ops Item 中检索参数和值。
- c. 选择运行。如果没有错误, 则会显示成功创建的 RFC 页面, 其中包含已提交的 RFC 详细信息和初始运行输出。
- d. 监控 RFC 的执行进度。
- e. 执行完成后, 将 OpsItem 得到解决。如果 RFC 失败, 请按照中的[对可信修正者中的修正进行故障排除](#)步骤操作。如需其他故障排除支持, 请联系 AMS。

对可信修正者中的修正进行故障排除

如需有关手动补救和补救失败的帮助, 请联系 AMS。

要查看修复状态和结果, 请完成以下步骤:

1. 打开 AWS Systems Manager 控制台, 网址为 <https://console.aws.amazon.com/systems-manager/>。
2. 选择“运营管理”, OpsCenter。
3. (可选) 按“来源 = 可信修正者”筛选列表, 以便在列表中仅包括受信任的修正者 OpsItems。
4. 选择您 OpsItem 要查看的。
5. 在“自动化执行”部分中, 查看文档名称和状态以及结果。
6. 查看以下常见的自动化故障。如果您的问题未在此处列出, 请联系您的 CSDM 寻求帮助。

常见的补救错误

自动化执行中未列出任何执行任务

任何与关联的执行都 OpsItem 可能表示由于参数值不正确而导致执行未能启动。

故障排除步骤

1. 在运营数据中，查看trustedAdvisorCheckAutoRemediation属性值。
2. 验证DocumentName和参数值是否正确。要获得正确的值，请查看[在可信修正器中配置 Trusted Advisor 检查修复](#)有关如何配置 SSM 参数的详细信息。要查看支持的校验参数，请参阅 [Trusted Advisor 受信任修正者支持的检查](#)
3. 验证 SSM 文档中的值是否与允许的模式相匹配。要查看文档内容中的参数详细信息，请在“运行手册”部分中选择文档名称。
4. 检查并更正参数后，手动修复。OpsItem有关补救步骤，请参阅[在“可信修正器”中运行手动修复](#)。
5. 为防止此错误再次发生，请确保在配置中使用正确的参数值配置补救措施。有关更多信息，请参阅[在可信修正器中配置 Trusted Advisor 检查修复](#)。

自动化执行中的执行失败

补救文档包含多个步骤，这些步骤与通过 AWS 服务 执行各种操作进行交互 APIs。要确定故障的具体原因，请完成以下步骤：

故障排除步骤

1. 要查看各个执行步骤，请在“自动化执行”部分中选择“执行 ID”链接。以下是 Systems Manager 控制台的示例，显示了所选自动化的执行步骤：
2. 选择状态为“失败”的步骤。以下是错误消息示例：

- NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist

此错误表示在修正配置的预配置参数中指定的存储桶名称不正确。

要解决此错误，[请使用正确的存储桶名称手动运行自动化](#)。为防止此问题再次发生，[请使用正确的存储桶名称更新修复配置](#)。

- DB instance my-db-instance-1 is not in available status for modification.

此错误表示由于数据库实例处于无效状态，自动化无法进行预期的更改。

要解决此错误，[请手动运行自动化](#)。

可信修正者中的修复日志

Trusted Remediator 创建 JSON 格式的日志并将其上传到亚马逊简单存储服务。日志文件将上传到 AMS 创建并命名的 S3 存储桶。ams-trusted-remediator-{your-account-id}-logsAMS 在委派管理员账户中创建 S3 存储桶。您可以将日志文件导入到中 QuickSight 以生成自定义的修复报告。

修复项目日志

可信修正者会在创建修正 Remediation item log OpsItem 时创建。此日志包含手动修复 OpsItem 和自动修复 OpsItem。您可以使用 Remediation item log 来跟踪所有修正的概述。

Compute Optimizer 建议的修复项目日志位置

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
compute_optimizer_remediation_items/remediation creation time in yyyy-mm-  
dd format/10 digits epoch time or unix timestamp-Trusted Advisor check ID-  
Resource ID.json
```

用于 Trusted Advisor 检查的修正项目日志位置

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs/  
remediation_items/remediation creation time in yyyy-mm-dd format/10 digits  
epoch time or unix timestamp-Trusted Advisor check ID- Resource ID.json
```

修复项目日志示例文件 URL

```
s3:///ams-trusted-remediator-111122223333-logs/  
remediation_items/2023-02-06/1675660464-DAvU99Dc4C-  
vol-00bd8965660b4c16d.json
```

Compute Optimizer 修复项目日志格式

```
{
```

```
"AccountID": "Account_ID",
"ComputeOptimizerCheckID": "Compute Optimizer check ID",
"ComputeOptimizerCheckName": "Compute Optimizer check name",
"ResourceID": "Resource ID",
"RemediationTime": Remediation creation time,
"ExecutionMode": "Automated or Manual",
"OpsItemID": "OpsItem ID"
}
```

Trusted Advisor 修正项目日志格式

```
{
  "TrustedAdvisorCheckID": Trusted Advisor check ID,
  "TrustedAdvisorCheckName": Trusted Advisor check name,
  "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
  "ResourceID": Resource ID,
  "RemediationTime": Remediation creation time,
  "ExecutionMode": Automated or Manual,
  "OpsItemID": OpsItem ID
}
```

Compute Optimizer 修复项目日志格式示例内容

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor 修复项目日志格式示例内容

```
{
  "TrustedAdvisorCheckID": "DAvU99Dc4C",
  "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
  "TrustedAdvisorCheckResultTime": 1675614749,
  "ResourceID": "vol-00bd8965660b4c16d",
  "RemediationTime": 1675660464,
  "OpsItemID": "oi-cca5df7af718"
}
```

```
}
```

自动修复执行日志、Compute Optimizer 和 Trusted Advisor

Trusted Remediator 会在自动运行 SSM 文档完成 Automated remediation execution log 时创建。此日志包含 OpsItem 仅用于自动修复的 SSM 运行详细信息。您可以使用此日志文件来跟踪自动修复。

Compute Optimizer 自动修复日志位置

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs//  
remediation_executions/remediation creation time in yyyy-mm-dd format/10  
digits epoch time or unix timestamp-Compute Optimizer recommendation  
ID.json
```

Trusted Advisor 自动修复日志位置

```
s3://ams-trusted-remediator-delegated-administrator-account-id-logs//  
remediation_executions/remediation creation time in yyyy-mm-dd format/10  
digits epoch time or unix timestamp-Trusted Advisor check ID-Resource  
ID.json
```

Compute Optimizer 自动修复日志位置示例

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2025-06-26/1750908858-123456789012-compute-  
optimizer-ec2-i-1235173471d2cd789.json
```

Trusted Advisor 自动修复日志位置示例

```
s3://ams-trusted-remediator-111122223333-logs/  
remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-  
vol-00bd8965660b4c16d.json
```

自动修复日志格式示例内容

```
{  
  "OpsItemID": "oi-767c77e05301",  
  "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",  
  "SSMExecutionStatus": "Success"}
```

《可信修正者》中的最佳实践

以下是帮助您使用可信修正器的最佳实践：

- 如果您不确定补救结果，请从手动执行模式开始。有时，从一开始就对补救应用自动执行可能会导致意想不到的结果。
- 每周对补救措施进行一次回顾 OpsItems，深入了解可信修复者的结果。
- 成员账户继承委派管理员账户的配置。因此，重要的是要以一种有助于您管理具有相同配置的多个帐户的方式来构建帐户。您可以使用标签将资源排除在默认配置之外。

受信任的修正者 FAQs

以下是有关可信修正者的常见问题：

什么是 Trusted Remediator？它对我有什么好处？

当 Compute Optimizer 发现违规行为 Trusted Advisor 或发布建议时，Trusted Remediator 会根据您指定的偏好进行响应，方法是应用补救措施、通过手动修正寻求批准，或者在即将到来的月度业务回顾 (MBR) 中报告补救措施。补救将在您的首选补救时间或计划进行。Trusted Remediator 使您能够自助服务并对 Trusted Advisor 支票采取行动，并且可以灵活地单独或批量配置和修复支票。AMS 拥有经过测试的补救文件库，通过应用安全检查和遵循 AWS 最佳实践，不断禁止提高您的账户。只有当您在配置中指定这样做时，您才会收到通知。AMS 用户可以选择加入 Trusted Remediator，无需额外付费。

Trusted Remediator 与其他 AWS 服务人有何关系和协作？

作为现有企业支持计划的一部分，您可以访问 Trusted Advisor 支票和 Compute Optimizer 建议。Trusted Remediator 与 Trusted Advisor Compute Optimizer 集成，可利用现有的 AMS 自动化功能。具体而言，AMS 使用 AWS Systems Manager 自动化文档（运行手册）进行自动修复。AWS AppConfig 用于配置修复工作流程。您可以通过 Systems Manager OpsCenter 查看所有当前和过去的补救措施。修复日志存储在 Amazon S3 存储桶中。您可以使用日志在中导入和构建自定义报告仪表盘 QuickSight。

谁来配置补救措施？

您的账户中的配置归您所有。管理您的配置是您的责任。您也可以联系 AMS 以获取配置更改、支持和手动补救以及修复失败的疑难解答。

如何安装 SSM 自动化文档？

SSM 自动化文档会自动共享给已注册的 AMS 账户。

AMS 拥有的资源也会得到补救吗？

可信修正者不会标记 AMS 拥有的资源。Trusted Remediator 只关注您的资源。

AWS 区域 Trusted Remediator 中有哪些可用以及谁可以使用它？

可信修正器适用于 AMS 高级版客户。有关支持区域的最新列表，请参阅[AWS 服务 按地区划分](#)。

可信修正者会导致资源漂移吗？

由于 SSM 自动化文档直接通过 AWS API 更新资源，因此可能会出现资源偏差。您可以使用标签来隔离通过现有 CI/CD 包创建的资源。您可以将 Trusted Remediator 配置为在修复其他资源的同时忽略已标记的资源。

如何暂停或停止可信修正者？

使用“[管理](#)”|“[可信修正者](#)”|“[状态](#)”|“[启用或禁用](#)”更改类型来停止可信修正者服务。使用相同的更改类型来重新启用可信修正者。

如何修复可信修正者不支持的检查？

您可以继续通过按需运营 (OOD) 与 AMS 联系，获取不支持的支票。AMS 可帮助您补救这些检查。有关更多信息，请参阅[按需操作](#)。

Trusted Remediator 会将哪些资源部署到您的账户？

可信修正者在可信修正者委派的管理员帐户中部署以下资源：

- 一个名为 `ams-trusted-remediator-{your-account-id}-logs` 的 Amazon S3 存储桶。Trusted OpsItem Remediator Remediation item log 在创建补救措施时以 JSON 格式创建，并将日志文件上传到此存储桶。
- 用于保存支持的 Trusted Advisor 检查和 Compute Optimizer 建议的补救配置的 AWS AppConfig 应用程序。

可信修正者不会在可信修正者成员帐户中部署资源。

日志管理

主题

- [什么是日志管理？](#)
- [AMS 日志的工作原理](#)
- [访问 日志](#)
- [自定义您的日志配置](#)

AMS 日志管理收集、汇总和控制托管账户日志的保留期。AWS 日志管理将来自 Amazon EC2 实例和您账户中部署的 AWS 资源的日志汇总到 CloudWatch 日志中。当前从中汇总日志的服务的完整列表可在[中找到AMS 聚合服务日志](#)。

什么是日志管理？

日志管理是处理实例、应用程序和 AWS 服务生成的日志事件的过程。此功能定义了 AMS 如何处理、存储和轮换在您的托管 AWS 账户中生成的日志事件。基础设施日志用于事件解决期间和支持系统审计。

AMS 日志的工作原理

AMS 单账户 landing zone (SALZ) 日志管理使用各种预安装的代理和工具，这些代理和工具是在加载或配置实例和应用程序时实施的。

日志记录是在账户注册过程中和堆栈启动时配置的。

由实例和 AWS 服务生成的 AMS 多账户着陆区 (MALZ) 日志在 AMS 管理的每个账户中的 CloudWatch 日志或亚马逊简单存储服务 (Amazon S3) Simple Storage Service 中可用。AMS 多账户 landing zone 提供了一个中央日志账户，该账户充当单个应用程序账户生成的某些日志的中央聚合位置。

[访问 日志](#)各小节中的表格描述了哪些日志在个人账户中可用，哪些日志在中央日志账户中可用。

访问 日志

要访问您的日志，请确保您拥有所需的 IAM 角色之一，并且位于您的 AMS 账户中。然后导航到显示的目录。

Multi-Account Landing Zone (MALZ)

提供五个默认 IAM 角色，每个角色都允许访问您账户中的所有日志（所有角色均以开头为 `AWSManagedServices`）：

- `AdminRole`
- `CaseRole`
- `ChangeManagementRole`
- `ReadOnlyRole`
- `SecurityOpsRole`

对这些角色的访问权限是通过联合配置的，每个角色都映射到您的 Active Directory 域中的一个组。

要了解有关这些角色的更多信息，请参阅[AMS 中的 IAM 用户角色](#)。

Single-Account Landing Zone (SALZ)

AMS 单账户 landing zone 的默认设置 `Customer_ReadOnly_Role` 允许您访问账户中的所有日志。使用映射到 Active Directory 组的 AWS Identity and Access Management (IAM) 角色控制对日志的访问。

AMS 聚合服务日志

每项 AWS 服务都会记录到“CloudWatch 日志”或 Amazon S3 存储桶中的特定位置。

Note

除非特别说明，否则所有日志位置都是生成日志的账户的本地位置，不会汇总到中央日志账户中。

要在 SALZ 和 MALZ 账户中查找默认 AMS CloudTrail 跟踪名称，请前往 AWS 控制台，CloudTrail 然后前往 Trails 页面搜索 AMS。由于 AMS 资源有标签，因此您可以通过这种方式找到路径。AMS CloudTrail 标签示例：

```
Environment    AMSInfrastructure
```

要访问您的日志，请确保您拥有所需的 IAM 角色之一，并且位于您的 AMS 账户中。然后导航到显示的目录。

Multi-Account Landing Zone

AMS 多账户 landing zone 聚合服务日志

	服务名称	日志详细信息	日志位置
1	Amazon Aurora	一般日志、慢速查询日志和错误日志。	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/ { <i>log_name</i> }
2	AWS CloudFormation (CFN)	仅限 API 调用记录。	AWS CloudFormation API 调用是通过记录的 CloudTrail，它会将日志发送到， CloudWatch LogGroup 然后将日志同步到 S3 存储桶中。默认情况下，日志在中保留 14 天 CloudWatch LogGroup，并在 S3 存储桶中无限期保留。 CloudWatch LogGroup:/CloudTrail/着陆区日志 S3 存储桶 [在中央日志账户中] : aws-landing-zone-logs-ams-a {<i>account_ID</i> }-log-management- { <i>region</i> 路径：AWSLogs/{<i>account_ID</i> }CloudTrail/
3	亚马逊 CloudFront (CloudFront)	用户请求记录。 CloudFront 必须明确启用日志记录。有关信息，请参阅 为支持的服务启用日志记录 。	S3 存储桶：ams-a {<i>account_ID</i> }-日志管理-{ <i>region</i> 路径：AWS/RedShift/{ <i>CloudFront distribution ID</i>

	服务名称	日志详细信息	日志位置
4	亚马逊 CloudWatch (CloudWatch)	仅限 API 调用记录。	CloudWatch LogGroup:/CloudTrail/着陆区日志 S3 存储桶 [在中央日志账户中] : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> } 路径 : AWSLogs//{ <i>account_ID</i> }CloudTrail/
5	Amazon Elastic Block Store (Amazon EBS)	EBS 服务不生成任何日志。	不适用
6	亚马逊弹性计算云 (亚马逊 EC2)	系统和应用程序日志。 有关更多信息，请参阅 亚马逊弹性计算云 (Amazon EC2)-系统级日志 。	CloudWatch 日志 : /{ <i>instance ID</i> }
7	Amazon Elastic File System (Amazon EFS)	仅限 API 调用记录。	CloudWatch LogGroup:/CloudTrail/着陆区日志 S3 存储桶 [在中央日志账户中] : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> } 路径 : AWSLogs//{ <i>account_ID</i> }CloudTrail/

	服务名称	日志详细信息	日志位置
8	弹性负载均衡 (ELB)	访问和错误日志条目。 弹性负载均衡器会记录发送给它们的所有请求，包括未路由到后端实例的请求。例如，如果客户端发送了格式错误的请求，或者没有运行正常的实例可以响应，则仍会记录该请求。 有关 Elastic Load Balancing 日志条目的更多信息，请参阅 - 经典负载均衡器：访问日志条目。 - 应用程序负载均衡器：访问日志条目。 - 网络负载均衡器：访问日志条目。	API 调用日志： CloudWatch LogGroup:/CloudTrail/着陆区日志 S3 存储桶 [在中央日志账户中]：aws-landing-zone-logs-<i>{account_ID}</i> -<i>{region}</i> 路径：AWSLogs//<i>{account_ID}</i> }CloudTrail/ 访问日志： S3 存储桶：mc-a<i>{account_ID}</i> }-logs <i>{region}</i> 路径：aws/elbaccess
9	亚马逊 OpenSearch 服务 (OpenSearch 服务)	服务错误日志。 您必须明确启用 OpenSearch 日志记录。有关信息，请参阅。为支持的服务启用日志记录	CloudWatch LogGroup:/CloudTrail/着陆区日志 S3 存储桶 [在中央日志账户中]：aws-landing-zone-logs-<i>{account_ID}</i> -<i>{region}</i> 路径：AWSLogs//<i>{account_ID}</i> }CloudTrail/

	服务名称	日志详细信息	日志位置
10	亚马逊 ElastiCache	仅限 API 调用记录。	CloudWatch LogGroup://CloudTrail/着陆区日志
11	亚马逊 GuardDuty		S3 存储桶 [在中央日志账户中] : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> }
12	Amazon Inspector		路径 : AWSLogs/{ <i>account_ID</i> }CloudTrail/
13	Amazon Macie		
14	Amazon Redshift	连接、用户和活动日志。 当你通过调用 Create Redshift 集群 CT (ct-1malj7snzxrkr) 创建 Redshift 集群时，日志记录默认处于启用状态。 有关信息，请参阅数据库审计日志。	S3 存储桶 : ams-a {<i>account_ID</i>}-日志管理-{<i>region</i>} 路径 : /AWS/RedShift/{ <i>CloudFront Distribution ID</i>}
15	Amazon Relational Database Service (RDS)	特定于数据库类型的日志。 您必须明确启用 RDS 日志记录。有关信息，请参阅为支持的服务启用日志记录 您只能通过存储过程访问 MSSQL 日志；有关信息，请参阅存档日志文件。	CloudWatch LogGroup: /aws/rds/ (<i>instance</i>或<i>cluster</i>)/ {}/{<i>database_name log_name</i>}

	服务名称	日志详细信息	日志位置
16	亚马逊 S3 (S3)	存储桶访问日志。每条访问日志记录都提供有关单个访问请求的详细信息，例如请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果有）。访问日志信息可能在安全和访问审核方面十分有用。它还可以帮助您了解您的客户群并了解您的 Amazon S3 账单。 有关 S3 访问日志条目的更多信息，请参阅 S3 服务器访问日志格式。	S3 存储桶：mc-a {<i>account_ID</i> }-日志管理-{} <i>region</i> 路径：/aws/s3access/ {} <i>bucket_name</i> S3 存储桶 [在中央日志账户中]：aws-landing-zone-s3-access-logs- {<i>account_ID</i> }-{} <i>region</i> 路径：/
17	Amazon Simple Email Service (SES)	SES API 服务调用。	CloudWatch LogGroup:/CloudTrail/着陆区日志 S3 存储桶 [在中央日志账户中]：aws-landing-zone-logs- {<i>account_ID</i> }-{} <i>region</i> 路径：AWSLogs//{<i>account_ID</i> }CloudTrail/
18	Amazon Virtual Private Cloud (VPC)	VPC 流量数据（有关进出您的 VPC 网络接口的 IP 流量的信息）。	CloudWatch LogGroup: /aws/vpcflow/ {} <i>VPC_ID</i>
19	Auto Scaling	仅限 API 调用记录。	CloudWatch LogGroup:/CloudTrail/着陆区日志
20	AWS Certificate Manager		S3 存储桶 [在中央日志账户中]：aws-landing-zone-logs- {<i>account_ID</i> }-{} <i>region</i> 路径：AWSLogs//{<i>account_ID</i> }CloudTrail/

	服务名称	日志详细信息	日志位置
21	AWS CodeDeploy	特定于实例的部署日志。	在实例上
22	AWS Config	AWS Config API 服务调用。	CloudWatch LogGroup:/CloudTrail/着陆区日志 S3 存储桶 [在中央日志账户中] : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> } 路径 : AWSLogs//{ <i>account_ID</i> }CloudTrail/
		资源配置的变化，由 AWS Config 跟踪。	S3 存储桶 [在中央日志账户中] : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> } 路径 : /AWSLogs/{ <i>account_ID</i> }/Config/
23	AWS Database Migration Service	数据库迁移日志。 有关信息，请参阅 AWS Database Migration Service 中的日志管理简介 。	数据库迁移控制台
24	AWS Direct Connect (DX)	仅限 API 调用记录。	CloudWatch LogGroup:/CloudTrail/着陆区日志
25	AWS 冰川		S3 存储桶 [在中央日志账户中] : aws-landing-zone-logs- { <i>account_ID</i> }-{ <i>region</i> }
26	AWS IAM (IAM)		
27	AWS Key Management Service		路径 : AWSLogs//{ <i>account_ID</i> }CloudTrail/

	服务名称	日志详细信息	日志位置
28	AWS 管理控制台 (控制台或 AWS 控制台)		
29	AWS 简单通知服务 (SNS) Simple Notification Service		
30	AWS 简单队列服务 (SQS)		

Single-Account Landing Zone

AMS 单账户 landing zone 聚合服务日志

	服务名称	日志详细信息	日志位置
1	Amazon Aurora	一般日志、慢速查询日志和错误日志。	CloudWatch LogGroup: /aws/rds/cluster/{ <i>database_name</i> }/ { <i>log_name</i> }
2	亚马逊 CloudFormation (CloudFormation 或 CFN)	仅限 API 调用记录。	CloudFormation API 调用是通过记录的 CloudTrail，它会将其日志发送到， CloudWatch LogGroup 然后将日志同步到 S3 存储桶中。 CloudWatch LogGroup: /aws/ams/cloudtrail S3 存储桶：ams-a { <i>account_ID</i> }-日志管理-{} <i>region</i>
3	亚马逊 CloudFront (CloudFront)	用户请求记录。	S3 存储桶：ams-a { <i>account_ID</i> }-日志管理-{} <i>region</i>

	服务名称	日志详细信息	日志位置
		您必须明确启用 CloudFront 日志记录。有关信息，请参阅 为支持的服务启用日志记录	路径：AWS/RedShift/{ <i>CloudFront_distribution_ID</i>
4	亚马逊 CloudWatch (CloudWatch)	仅限 API 调用记录。	CloudWatch LogGroup: /aws/ams/cloudtrail
5	Amazon Elastic Block Store (EBS)	EBS 服务不生成任何日志。	不适用
6	亚马逊弹性计算云 (EC2)	系统和应用程序日志。 有关更多信息，请参阅 亚马逊弹性计算云 (Amazon EC2)-系统级日志 。	CloudWatch 日志：/{ <i>instance_ID</i> }
7	Amazon Elastic File System (Amazon EFS)	仅限 API 调用记录。	CloudWatch LogGroup: /aws/ams/cloudtrail

	服务名称	日志详细信息	日志位置
8	弹性负载均衡 (ELB)	访问和错误日志条目。 弹性负载均衡器会记录发送给它们的所有请求，包括未路由到后端实例的请求。例如，如果客户端发送了格式错误的请求，或者没有运行正常的实例可以响应，则仍会记录该请求。 有关弹性负载均衡器日志条目的更多信息，请参阅 - 经典负载均衡器：访问日志条目。 - 应用程序负载均衡器：访问日志条目。 - 网络负载均衡器：访问日志条目。	CloudWatch LogGroup: /aws/ams/cloudtrail S3 存储桶：<code>mc-a {<i>account_ID</i> }-logs-{<i>region</i>}</code> 路径：<code>aws/elbaccess</code>
9	亚马逊 OpenSearch 服务 (OpenSearch 服务)	服务错误日志。 您必须明确启用 OpenSearch 日志记录。有关信息，请参阅。为支持的服务启用日志记录	CloudWatch LogGroup: /aws/ams/cloudtrail
10	亚马逊 ElastiCache	仅限 API 调用记录。	CloudWatch LogGroup: /aws/ams/cloudtrail
11	亚马逊 GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		

	服务名称	日志详细信息	日志位置
14	Amazon Redshift	连接、用户和活动日志。 当你通过调用 Create Redshift 集群 CT (ct-1malj7snzxrkr) 创建 Redshift 集群时，日志记录默认处于启用状态。 有关信息，请参阅数据库审计日志。	S3 存储桶：ams-a {<i>account_ID</i> }-日志管理-{} <i>region</i> 路径：/AWS/RedShift/{} <i>CloudFront_Distribution_ID</i>
15	Amazon Relational Database Service (RDS)	特定于数据库类型的日志。 必须明确启用 RDS 日志记录。有关信息，请参阅为支持的服务启用日志记录 您只能通过存储过程访问 MSSQL 日志；有关信息，请参阅存档日志文件。	CloudWatch LogGroup: /aws/rds/(instance cluster)/{数据库名称}/{日志名称}
16	亚马逊 S3 (S3)	存储桶访问日志。每条访问日志记录都提供有关单个访问请求的详细信息，例如：请求者、存储桶名称、请求时间、请求操作、响应状态和错误代码（如果有）。访问日志信息可用于安全和访问审计；它还可以帮助您了解您的客户群并了解您的 Amazon S3 账单。 有关 S3 访问日志条目的更多信息，请参阅S3 服务器访问日志格式。	S3 存储桶：mc-a {<i>account_ID</i> }-日志管理-{} <i>region</i> 路径：/aws/s3access/ {} <i>bucket_name</i>

	服务名称	日志详细信息	日志位置
17	Amazon Simple Email Service (SES)	SES API 服务调用。	CloudWatch LogGroup: /aws/ams/cloudtrail S3 存储桶 : <code>ams-a {<i>account_ID</i> }-日志管理-{} <i>region</i></code> 路径 : <code>AWS/CloudTrail/AWSLogs/{<i>account_ID</i> }/{CloudTrail/{<i>region</i>}</code>
18	Amazon Virtual Private Cloud (VPC)	VPC 流量数据 (有关进出您的 VPC 网络接口的 IP 流量的信息) 。	CloudWatch LogGroup: /aws/vpcflow/ {vpc_id}
19	Auto Scaling	仅限 API 调用记录。	CloudWatch LogGroup: /aws/ams/cloudtrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	特定于实例的部署日志。	举个例子
22	AWS Config	AWS Config API 服务调用。	CloudWatch LogGroup: /aws/ams/cloudtrail S3 存储桶 : <code>ams-a {<i>account_ID</i> }-日志管理-{} <i>region</i></code> 路径 : <code>AWS/CloudTrail/AWSLogs/{<i>account_ID</i> }/{CloudTrail/{<i>region</i>}</code>
23	AWS Database Migration Service	数据库迁移日志。 有关信息，请参阅 AWS Database Migration Service 中的日志管理简介 。	数据库迁移控制台

	服务名称	日志详细信息	日志位置
24	AWS Direct Connect (DX)	仅限 API 调用记录。	CloudWatch LogGroup: /aws/ams/cloudtrail
25	AWS 冰川		
26	AWS IAM (IAM)		
27	AWS Key Management Service		
28	AWS 管理控制台 (控制台或 AWS 控制台)		
29	AWS 简单通知服务 (SNS) Simple Notification Service		
30	AWS 简单队列服务 (SQS)		

AMS 共享服务日志

下表描述了您账户中 AMS 共享服务的日志和日志位置。

要访问您的日志，请确保您拥有所需的 IAM 角色之一，并且位于您的 AMS 账户中。然后导航到显示的目录。

AMS 单账号 landing zone 共享服务日志

	共享服务名称	日志详细信息	日志位置
1	堡垒主机	有关访问堡垒主机的用户的信息。	Linux 堡垒： CloudWatch 日志：/{实例 ID}/var/log/secure

	共享服务名称	日志详细信息	日志位置
			CloudWatch 日志：/{实例 ID}/var/log/audit/audit.log Windows 堡垒： CloudWatch 日志：/{实例 ID}/SecurityEventLog
2	管理主机	脚本输出，这些脚本有助于在账户内自动执行访问管理操作。	CloudWatch 日志：/{实例 ID}/ApplicationEventLog
4	EPS 主机 (DSM)	有关将实例注册到趋势科技服务器深度安全防护系统管理平台的信息。	CloudWatch 日志：/{实例 ID}/var/log/DSM.log
5	目录服务	账户目录中有关账户登录、账户管理、详细跟踪、对象访问、政策变更和权限使用的信息。 必须明确启用目录服务日志记录。有关信息，请参阅 为支持的服务启用日志记录 。	CloudWatch 日志：/aws/directoryservice/{目录 ID}-{目录 dns 名称}
6	Lambda	各种 lambda 的输出，这些输出有助于在账户内自动执行操作操作。	CloudWatch 日志：/aws/lambda/{lambda name}

AMS 多账户 landing zone 共享服务日志

	共享服务名称	日志详细信息	日志位置
1	堡垒	实例登录和身份验证失败的输出。	Linux 堡垒 CloudWatch 日志：/{ <i>instance_ID</i> }/log var/log/secure

	共享服务名称	日志详细信息	日志位置
			Windows 堡垒 CloudWatch 日志 : / { <i>instance_ID</i> }/SecurityEventLog
2	管理主机	scriptsy 的输出，它有助于在 账户内自动执行访问管理操 作。	CloudWatch 日志 : /{ <i>instance_ ID</i> }/ApplicationEventLog
3	EPS 主机 (DSM)	有关将实例注册到趋势科技 服务器深度安全防护系统管 理平台的信息。	CloudWatch 日志 : /{ <i>instance_ ID</i> }/var/log/DSM.log
4	目录服务	账户目录中有关账户登录、 账户管理、详细跟踪、对象 访问、政策变更和权限使用 的信息。 必须明确启用目录服务日志 记录。有关信息，请参阅 为 支持的服务启用日志记录 。	CloudWatch 日志 : /aws/directorys ervice/ {}-{} <i>directory_ID</i> <i>directory_DNS_name</i>
5	Lambda	各种 lambda 的输出，这些输 出有助于在账户内自动执行 操作操作。	CloudWatch 日志 : /aws/lambda/ {} <i>Lambda_name</i>

亚马逊弹性计算云 (Amazon EC2)-系统级日志

实例日志由在实例上运行的 CloudWatch 日志代理收集，并且可以通过与实例同名的 CloudWatch 日志组进行访问。例如，如果实例 ID 为 i-0123456789abcdef0，日志文件名为 /var/log/messages, the Log Group would be i-0123456789abcdef0 and the Log Stream /var/log/messages

另请参阅[AMS 聚合服务日志](#)。

要访问您的日志，请确保您拥有所需的 IAM 角色之一，并且位于您的 AMS 账户中。然后导航到显示的目录。

 Note

默认情况下会收集以下日志。

亚马逊 Linux/红帽 Linux/Centos Linux/Ubuntu/SUSE Linux

日志文件/日志流

```
/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
/var/log/secure
/var/log/spooler
/var/log/yum.log
/var/log/aws/ams/bootstrap.log
/var/log/aws/ams/build.log
/var/log/syslog
/var/log/dpkg.log
/var/log/auth.log
/var/log/zypper.log
```

 Note

有关访问亚马逊 Linux 2023 日志的信息，请参阅为[什么 /var/log 目录缺少我的 EC2 亚马逊 Linux 2023 实例中的日志？](#)

Windows

日志文件/日志流

SecurityEventLog

```
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
AmazonSSMErrorLog
```

与 Splunk 集成

AMS 支持基于 AWS Lambda 的推送到客户日志分析服务，例如 Splunk。

AMS 利用适用于亚马逊网络服务的 Splunk 附加组件，该插件允许将 AWS 数据流式传输到 Splunk。请参阅[硬件和软件要求](#)。

请参阅这篇 Splunk 博客文章[如何将 AWS CloudWatch 日志流式传输到 Splunk \(提示：这比你想象的更容易\)](#)。由于 AMS 客户默认启用 CloudWatch 日志流，并且 AMS 会为您配置 AWS Lambda 函数，但您需要配置 Splunk HTTP 事件收集器 (HEC) 输入并向 AMS 提交请求以获取新增功能。

以下是数据输入设置的样子：

自定义您的日志配置

您可以更改日志的日志数据保留期，也可以为 CloudWatch 其他 AWS 服务启用日志记录。

更改 CloudWatch 日志保留期

您可以更改日志的日志数据保留设置。CloudWatch 默认情况下，日志将无限期保留且永不过期。您可以调整每个日志组的保留策略，保持无限期保留或选择介于 10 年和一天之间的保留期。要查看 AMS 中允许的最短保留期，请参阅 AWS Artifact 上提供的 AMS 技术标准文档。要访问 AWS Artifact，请联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。

CloudWatch 日志日志保留功能根据保留策略删除流中的日志事件。它不会删除日志流或日志组。有关一般信息，请参阅亚马逊 CloudWatch 日志用户指南[什么是亚马逊 CloudWatch 日志？](#)。

有关自定义日志保留期的信息以及要了解更多信息，请参阅[更改日志中的 CloudWatch 日志数据保留期](#)。

为支持的服务启用日志记录

某些服务默认情况下未启用日志记录，因此需要明确启用。

要启用 CloudFront、OpenSearch、Amazon RDS 和 Route53 的日志记录，请使用[管理 | 其他 | 其他 | 创建更改类型 \(ct-1e1xtak34nx76\)](#) 提交 RFC，其中包含以下值，并酌情替换：*variables*

Subject: Enable logging for *SERVICE_NAME*
Description: Service ARN: *SERVICE_ARN*

安全管理

AWS Managed Services (AMS) 安全管理是 AMS 识别组织资产并实施保护这些资产的策略和程序的流程。

Note

AMS 现在有了变更类型 (CT)，即部署 | 高级堆栈组件 | ACM 证书以及其他 SANs | Create (ct-3l14e139i5p50)，你可以用它来提交证书申请。AWS Certificate Manager 有关信息，请参阅 [AWS::CertificateManager::Certificate](#)。本 CT 规定创建其他主题备用名称 (SAN)。

要更好地了解一般 AWS 安全性，[请参阅安全、身份和合规性最佳实践](#)。

AMS 将安全风险分类如下：

- 反恶意软件检测到的已知风险，恶意软件缓解过程会处理这些风险。
- 安全事件，包括访问漏洞，由安全事件管理流程处理。

主题

- [AMS 中的数据保护](#)
- [身份和访问管理](#)
- [AMS 中的安全事件响应](#)
- [在 AMS Advanced 中更改请求安全审查](#)

AMS 中的数据保护

AMS 利用亚马逊 GuardDuty、Amazon Macie（可选）等原生 AWS 服务以及其他内部专有工具和流程，持续监控您的托管账户。警报触发后，AMS 将负责对警报的初始分类和响应。我们的响应流程基于 NIST 标准。AMS 定期与您一起使用安全事件响应模拟来测试其响应流程，使您的工作流程与现有客户安全响应计划保持一致。

当 AMS 检测到您的安全策略有任何违规行为或迫在眉睫的 AWS 违规威胁时，我们会收集信息，包括受影响的资源和任何与配置相关的更改。AMS 提供 24/7/365 follow-the-sun 支持，由专门的操作员积极审查和调查所有托管账户的监控仪表板、事件队列和服务请求。AMS 会与我们的安全专家一起调查调查结果，分析活动并通过您账户中列出的安全升级联系人通知您。

根据我们的调查结果，AMS 会主动与您互动。如果您认为该活动未经授权或可疑，AMS 会与您合作，调查和补救或遏制问题。由 GuardDuty 生成的某些调查结果类型要求您先确认影响，然后 AMS 才能采取任何行动。例如，GuardDuty 查找结果类型 UnauthorizedAccess : IAMUser/ConsoleLogin 表示您的一个用户从不寻常的位置登录；AMS 会通知您并要求您查看调查结果以确认这种行为是否合法。

Amazon Macie

AWS Managed Services 建议您使用 Macie 来检测大量而全面的敏感数据，例如个人健康信息 (PHI)、个人身份信息 (PII) 和财务数据。

可以将 Macie 配置为在任何 Amazon S3 存储桶上定期运行，从而随着时间的推移自动评估存储桶内任何新的或修改过的对象。生成安全调查结果后，AMS 将通知您并根据需要与您合作进行补救。

有关更多信息，请参阅[分析 Amazon Macie 调查结果](#)。

亚马逊 Macie 安全

Macie 是一项人工 intelligence/AI 驱动的安全服务，可通过自动发现、分类和保护存储在 AWS 中的敏感数据来帮助您防止数据丢失。Macie 使用机器学习来识别敏感数据，例如个人身份信息 (PII) 或知识产权，分配业务价值，并提供对这些数据的存储位置以及组织中如何使用这些数据的可见性。Macie 会持续监控数据访问活动中是否存在异常情况，并在检测到未经授权的访问或无意中数据泄露的风险时发出警报。Macie 服务支持 Amazon S3 和 AWS CloudTrail 数据源。

AMS 会持续监控来自 Macie 的警报，如果收到警报，则会迅速采取措施保护您的资源和帐户。将 Macie 添加到 AMS 支持的服务列表后，我们现在还负责根据您的指示在您的所有帐户中启用和配置 Macie。您可以在 AWS 控制台或支持的集成中查看 Macie 警报和我们的操作。在帐户注册期间，您可以指定用于存储 PII 的帐户。对于所有具有 PII 的新帐户，我们建议使用 Macie。对于已有 PII 的帐户，请联系我们，我们将在您的帐户中将其启用。因此，您可以获得额外的保护层，并在由 AMS 管理的 AWS 环境中享受 Macie 的所有好处。

AMS Macie FAQs

- 当所有 AMS 帐户都已启用趋势科技并 GuardDuty 启用后，为什么还需要 Macie？

Macie 可帮助您对拥有的数据、数据对业务的价值以及与访问这些数据相关的行为进行分类，从而保护您在 Amazon S3 中的数据。Amazon GuardDuty 通过帮助识别威胁行为者侦察、实例问题和有问题的帐户活动等威胁，为您的 AWS 帐户、工作负载和数据提供广泛的保护。这两项服务都包含用户行为分析、机器学习和异常检测，以检测各自类别的威胁。趋势科技并不专注于识别 PII 及其威胁。

- 如何在我的 AMS 账户中开启 Macie ？

如果您已在自己的账户中 PII/PHI 存储或计划将其存储，请联系您的 CSDM 或提出服务请求，为您由 AMS 管理的新账户或现有账户启用 Macie。

- 在我的 AMS 账户中启用 Macie 会产生哪些成本影响？

AMS 的 Macie 定价与亚马逊弹性计算云 (Amazon EC2) 等其他服务类似。您需要根据使用量为 Amazon Macie 付费，并根据您的使用情况支付 AMS 升级。SLAsMacie 费用基于使用情况，参见 [Amazon Macie](#) 定价，该定价 AWS CloudTrail 基于事件和亚马逊 S3 存储空间进行衡量。请注意，Macie 的费用往往会从启用后的第二个月起趋于平缓，因为它根据添加到 Amazon S3 存储桶的增量数据收费。

要了解有关 Macie 的更多信息，请参阅[亚马逊 Macie](#)。

GuardDuty

GuardDuty 是一项持续的安全监控服务，它使用威胁情报源（例如恶意 IP 地址和域名列表）以及机器学习来识别您的 AWS 环境中意外且可能未经授权的恶意活动。这可能包括权限升级、使用暴露的凭据或与恶意 IP 地址或域的通信等问题。GuardDuty 还可以监控 Amazon Web Services 账户访问行为是否存在泄露迹象，例如未经授权的基础设施部署（例如部署在从未使用过的区域中的实例）或异常的 API 调用（例如更改密码策略以降低密码强度）。有关更多信息，请参阅《[GuardDuty 用户指南](#)》。

要查看和分析您的 GuardDuty 发现，请按以下步骤操作。

1. 打开 [GuardDuty 管理控制台](#)。
2. 选择“调查结果”，然后选择特定的调查结果以查看详细信息。每个发现的详细信息因发现类型、所涉及的资源和活动性质而异。

有关可用查找字段的更多信息，请参阅[GuardDuty 查找结果详细信息](#)。

GuardDuty 安全

Amazon GuardDuty 提供威胁检测功能，使您能够持续监控和保护您的 AWS 账户和工作负载。Amazon GuardDuty 会分析从您的账户生成的连续元数据流以及 AWS CloudTrail 事件、Amazon VPC 流日志和域名系统 (DNS) 日志中发现的网络活动。它还使用集成的威胁情报（例如已知的恶意 IP 地址、异常检测和机器学习）来更准确地识别威胁。GuardDuty 是一项受监控的 AMS 服务。要了解有关 Amazon GuardDuty 监控的更多信息，请参阅[GuardDuty 监控](#)。要了解更多信息 GuardDuty，请参阅 [Amazon GuardDuty](#)。

默认情况下，所有新的 AMS 账户均已 GuardDuty 启用。AMS GuardDuty 在账户注册期间进行配置。您可以随时提交更改请求以修改设置。GuardDuty AMS 的定价方式与亚马逊弹性计算云 (Amazon EC2) 等其他服务类似。您 GuardDuty 根据使用量付费，并根据您的使用情况进行 AMS 提升。SLAs GuardDuty 费用基于使用量 ([亚马逊 GuardDuty 定价](#))，根据您的 Amazon VPC 流日志 AWS CloudTrail 的事件和流量进行衡量。

GuardDuty 在 AMS 中，启用了以下主要检测类别：

- 侦测--暗示威胁行为者侦测的活动，例如异常 API 活动、VPC 内部端口扫描、登录请求失败的异常模式或来自已知不良 IP 的未屏蔽端口探测。
- 实例问题--有问题的实例活动，例如加密货币挖矿、使用域生成算法 (DGA) 的恶意软件、出站拒绝服务活动、网络流量异常大、网络协议异常、与已知恶意 IP 的出站实例通信、外部 IP 地址使用的临时亚马逊 EC2 凭证以及使用 DNS 进行数据泄露。
- 账户活动--表明账户活动的常见模式包括来自异常地理位置或匿名代理的 API 调用、尝试禁用 AWS CloudTrail 日志记录、异常启动实例或基础设施、在异常的 AWS 区域部署基础设施，以及来自已知恶意 IP 地址的 API 调用。

AMS GuardDuty 在您的托管账户中使用来持续监控调查结果和提醒，如果收到警报，AMS 运营部门会采取积极措施保护您的资源和账户。GuardDuty 您可以在 AWS 控制台或支持的集成中查看 GuardDuty 发现结果和我们的操作。

GuardDuty 在您的帐户中与趋势科技趋势科技服务器深度安全防护系统管理中心配合使用。趋势科技趋势科技服务器深度安全防护系统管理中心提供基于主机的入侵检测/入侵防护服务。趋势科技 Web 信誉服务 GuardDuty 在检测主机何时尝试与已知构成威胁的主机或 Web 服务通信的能力方面存在一些重叠之处。但是，GuardDuty 提供了其他威胁检测类别，并通过监视网络流量来实现这一点，这种方法是对趋势科技基于主机的检测的补充。基于网络的威胁检测允许在主机出现问题行为时控制失败，从而提高安全性。AMS 建议 GuardDuty 在您的所有 AMS 账户中使用。

要了解有关趋势科技的更多信息，请参阅[趋势科技趋势科技服务器深度安全防护系统帮助中心](#)；请注意，非亚马逊链接可能会更改，恕不另行通知。

GuardDuty 监控

GuardDuty 通过生成[安全调查结果](#)，AMS 可以捕获并发出警报，从而告知您 AWS 环境的状态。

Amazon 通过分析和处理 VPC 流日志、AWS CloudTrail 事件日志和域名系统日志来 GuardDuty 监控您的 AWS 环境的安全。您可以通过配置 GuardDuty 为同时使用自己的自定义、可信 IP 列表和威胁列表来扩展此监控范围。

- 可信 IP 列表由您允许与 AWS 基础设施和应用程序进行安全通信的 IP 地址组成。GuardDuty 不会生成可信 IP 列表上的 IP 地址的查找结果。在任何给定时间，每个区域的每个 AWS 账户只能上传一个可信 IP 列表。
- 威胁列表由已知的恶意 IP 地址组成。GuardDuty 根据威胁列表生成调查结果。在任何给定时间，每个区域的每个 AWS 账户最多可以上传六份威胁清单。

要实施 GuardDuty，请使用 AMS CT 部署 | 监控和通知 | GuardDuty IP 集 | 创建 (ct-08avsj2e9mc7g) 创建一组经批准的 IP 地址。你也可以使用 AMS CT 部署 | 监控和通知 | GuardDuty 威胁情报集 | 创建 (ct-25v6r7t8gvkq5) 来创建一组被拒绝的 IP 地址。

有关 AMS 监控的服务的列表，请参阅[AMS 监控系统监控什么？](#)。

亚马逊 Route 53 解析器 DNS 防火墙

Amazon Route 53 Resolver 以递归方式响应来自公共记录 AWS 资源、亚马逊 VPC 特定的 DNS 名称和 Amazon Route 53 私有托管区域的 DNS 查询，默认情况下全部可用。VPCs 使用 Route 53 Resolver DNS Firewall，您可以筛选和管理 Virtual Private Cloud (VPC) 的出站 DNS 流量。为此，您需要在 DNS Firewall 规则组中创建可重复使用的筛选规则集合，将规则组关联到您的 VPC，然后监控 DNS Firewall 日志和指标中的活动。根据活动，您可以相应地调整 DNS Firewall 的行为。有关更多信息，请参阅[使用 DNS 防火墙过滤出站 DNS 流量](#)。

要查看和管理 Route 53 解析器 DNS 防火墙配置，请按以下步骤操作：

1. 登录 AWS 管理控制台 并打开 Amazon VPC 控制台，网址为<https://console.aws.amazon.com/vpc/>。
2. 在 DNS 防火墙下，选择规则组。
3. 查看、编辑或删除现有配置，或创建新的规则组。有关更多信息，[请参阅 Route 53 解析器 DNS 防火墙的工作原理](#)。

Amazon Route 53 解析器 DNS 防火墙监控和安全

Amazon Route 53 DNS 防火墙使用规则关联、规则操作和规则评估优先级的概念。域列表是您在规则组内的 DNS Firewall 规则中使用的一组可重复使用的域规范。当您关联规则组与 VPC 时，DNS Firewall 会将您的 DNS 查询与规则中使用的域列表进行比较。如果 DNS Firewall 找到匹配项，则它会根据匹配规则的操作处理 DNS 查询。有关规则组和规则的更多信息，请参阅[DNS 防火墙规则组和规则](#)。

域列表分为两大类：

- 托管域名列表，AWS 可为您创建和维护。
- 您自己的域名列表，由您创建和维护。

根据规则组的关联优先级指数对其进行评估。

默认情况下，AMS 部署的基准配置由以下规则和规则组组成：

- 一个名为的规则组DefaultSecurityMonitoringRule。对于每个已启用的现有 VPC，规则组在创建时具有最高的关联优先级 AWS 区域。
- 规则组中一个优先级为 DefaultSecurityMonitoringRule 1 的DefaultSecurityMonitoringRule规则，使用带有操作 ALE RT 的AWSManagedDomainsAggregateThreatList托管域列表。

如果您已有配置，则部署基准配置的优先级将低于现有配置。您的现有配置是默认配置。如果您的现有配置没有提供有关如何处理查询解析的更高优先级的指令，则可以使用 AMS 基准配置作为包罗万象的配置。要更改或删除基准配置，请执行以下操作之一：

- 请联系您的云服务交付经理 (CSDM) 或云架构师 (CA)。
- 使用[管理 | 其他 | 其他 | 创建 CT \(ct-1e1xtak34nx76\) 创建变更请求 \(RFC\)](#)。
- 创建服务请求。

如果您的账户在开发者模式或直接更改模式下运行，则可以自己进行更改。

AWS Certificate Manager (ACM) 证书

AMS 有一个 CT、部署 | 高级堆栈组件 | ACM 证书以及其他 SANs | Create (ct-3l14e139i5p50)，你可以用它来提交 AWS Certificate Manager 证书申请，还有最多五个额外的主题备用名称 (SAN) (例如 example.com、example.net 和 example.org)。有关详细信息，请参阅[什么是 AWS Certificate Manager ?](#) 和 [ACM 证书特征](#)。

Note

此超时设置不仅与运行有关，还涉及您通过电子邮件验证对 ACM 证书的验证。未经您的验证，RFC 就会失败。

AMS 中的数据加密

AMS 使用多种 AWS 服务进行数据加密，尤其是亚马逊简单存储服务、AWS Key Management Service (AWS KMS)、亚马逊 Elastic Block Store、Amazon Relational Database Service Amazon Redshift Amazon ElastiCache AWS Lambda、、、、和亚马逊 OpenSearch 服务。

Amazon S3

Amazon S3 提供了多种对象加密选项，用于保护传输中的数据 and 静态数据。服务器端加密在将对象保存到数据中心的磁盘上之前加密对象，然后在下载对象时对数据进行解密。只要您验证了您的请求并且拥有访问权限，您访问加密和未加密对象的方式就没有区别。有关更多信息，请参阅 [Amazon S3 中的数据保护](#)。

Amazon EBS

使用 Amazon EBS 加密，您无需构建、维护和保护自己的密钥管理基础设施。Amazon EBS 加密在创建加密卷和快照时使用 AWS KMS 密钥。加密操作发生在托管 Amazon EC2 实例的服务器上。这样做是为了确保实例 data-at-rest 与其连接的 Amazon EBS 存储 data-in-transit 之间的安全性。您可以同时将加密卷和未加密卷附加到实例。有关更多信息，请参阅 [Amazon EBS 加密](#)。

Amazon RDS

Amazon RDS 可以加密您的 Amazon RDS 数据库实例。静态加密的数据包括数据库实例的底层存储、其自动备份、只读副本和快照。Amazon RDS 加密的数据库实例使用行业标准的 AES-256 加密算法对托管 Amazon RDS 数据库实例的服务器上的数据进行加密。在加密数据后，Amazon RDS 将以透明方式处理访问的身份验证和数据的解密，并且对性能产生的影响最小。您无需修改数据库客户端应用程序来使用加密。有关更多信息，请参阅 [加密 Amazon RDS 资源](#)。

Amazon Simple Queue Service

除了默认的 Amazon SQS 托管服务器端加密 (SSE) 选项外，Amazon SQS 托管 SSE (SSE-SQS) 还允许您创建自定义托管服务器端加密，该加密使用亚马逊 SQS 托管的加密密钥来保护通过消息队列发送的敏感数据。服务器端加密 (SSE) 允许您采用加密队列的方式传输敏感数据。SSE 使用 Amazon SQS 托管的加密密钥 (SSE-SQS) 或在 (SSE-KMS) 中管理的密钥来保护队列中的消息内容。AWS KMS 有关使用管理 SSE 的信息 AWS 管理控制台，请参阅 [静态加密](#)。

静态数据加密

OpenSearch 服务域提供静态数据加密，这是一项有助于防止未经授权访问您的数据的安全功能。该功能使用 AWS Key Management Service (AWS KMS) 来存储和管理您的加密密钥，并使用 256 位密钥

的高级加密标准算法 (AES-256) 来执行加密。有关更多信息，请参阅 [Amazon OpenSearch 服务的静态数据加密](#)。

密钥管理

AWS KMS 是一项托管服务，可让您轻松创建和控制客户主密钥 (CMKs)，即用于加密数据的加密密钥。AWS KMS CMKs 受经过 FIPS 140-2 加密模块验证计划验证的硬件安全模块 (HSMs) 保护，中国（北京）和中国（宁夏）地区除外。有关更多信息，请参阅[什么是 AWS Key Management Service？](#)

身份和访问管理

AWS Identity and Access Management (IAM) 是一项 Web 服务，可帮助您安全地控制对 AWS 资源的访问。可以使用 IAM 来控制谁通过了身份验证（准许登录）并获得授权（具有相应权限）来使用资源。在 AMS 入职期间，您负责在每个托管账户中创建跨账户 IAM 管理员角色。

多账户登录区 (MALZ) IAM 保护措施

AMS 多账户登陆区 (MALZ) 要求将 Active Directory (AD) 信任作为 AMS 访问管理的主要设计目标，以允许每个组织（包括 AMS 和客户）管理自己的身份的生命周期。这样就无需在彼此的目录中拥有凭证。配置了单向信任，以便其中的托管 Active Directory AWS 账户信任客户拥有或托管 AD 来对用户进行身份验证。由于信任只是一种方式，因此并不意味着客户活动目录信任托管 AD。

在此配置中，管理用户身份的客户目录称为用户林，Amazon EC2 实例所连接的托管 AD 称为资源林。这是 Microsoft 常用的用于 Windows 身份验证的设计模式；有关更多信息，[请参阅森林设计模型](#)。

这种模式允许两个组织自动执行各自的生命周期，并允许 AMS 和您在员工离开组织时快速撤消访问权限。如果没有这种模式，如果两个组织都使用公共目录（或 users/groups 在彼此的目录中创建），那么两个组织都必须投入额外的工作流程和用户同步，以考虑员工的起步和离职情况。这会带来风险，因为该过程存在延迟并且容易出错。

MALZ 访问权限的先决条件

MALZ 身份提供商集成，用于访问 AWS/AMS 控制台、CLI、SDK。

对您的 AMS 账户中的 Amazon EC2 实例进行单向信任。

使用身份进行身份验证

AMS 使用 IAM 角色，这是一种 IAM 身份。IAM 角色与用户非常相似，因为它是一个具有权限策略的身份，该策略决定了该身份可以做什么和不能做什么 AWS。但是，一个角色没有与之关联的凭证，而且，一个角色不是与一个人有唯一的关联，而是让任何需要它的人都可以担任。IAM 用户可担任角色来暂时获得针对特定任务的不同权限。

访问角色由内部组成员资格控制，内部组成员资格由运营管理部门管理和定期审查。

AMS 中的 IAM 用户角色

IAM 角色与 IAM 用户类似，因为它是一个具有权限策略的 AWS 身份，该策略决定了该身份可以做什么和不能做什么 AWS。但是，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。

目前，对于标准 AMS 账户，有一个 AMS 默认用户角色 `Customer_ReadOnly_Role`，还有一个角色适用于使用托管 Active Directory 的 AMS 账户。 `customer_managed_ad_user_role`

角色策略设置了 Amazon S3 日志操作的权限、AMS 控制台访问权限、对大多数控制台的只读限制 AWS 服务、对账户 S3 控制台的限制访问以及 AMS 更改类型访问权限。 CloudWatch

此外，还 `Customer_ReadOnly_Role` 具有可变的预留实例权限，允许您预留实例。它具有一些节省成本的价值，因此，如果您知道在很长一段时间内将需要一定数量的 Amazon EC2 实例，则可以调用这些 APIs 实例。要了解更多信息，请参阅 [Amazon EC2 预留实例](#)。

Note

除非要重复使用现有策略，否则为 IAM 用户创建自定义 IAM 策略的 AMS 服务级别目标 (SLO) 为四个工作日。如果您想修改现有的 IAM 用户角色或添加新角色，请分别提交 [IAM：更新实体](#) 或 [IAM：创建实体](#) RFC。

如果您不熟悉 Amazon IAM 角色，请参阅 [IAM 角色](#) 了解重要信息。

多账户着陆区 (MALZ)：要查看 AMS 多账户着陆区默认、未自定义的用户角色政策，请参阅下文。 [MALZ：默认 IAM 用户角色](#)

MALZ：默认 IAM 用户角色

默认多账户 AMS 多账户 landing zone 用户角色的 JSON 政策声明。

 Note

用户角色是可自定义的，并且可能因每个账户而异。提供了有关如何找到您的角色的说明。

以下是默认 MALZ 用户角色的示例。要确保设置了所需的策略，请运行 AWS 命令[get-role](#)或登录 AWS 管理-> [IAM 控制台](#)，然后在导航窗格中选择角色。

OU 账户的核心

核心账户是 MALZ 管理的基础设施账户。AMS 多账户 landing zone Core 账户包括一个管理账户和一个网络账户。

OU 核心 OU 账户：常见角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (公共 AWS 托管策略) 。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupport访问权限 (公有 AWS 托管策略) 。
AWSManagedServicesChangeManagementRole (核心账户版本)	ReadOnlyAccess
	AWSSupport访问
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

核心 OU 账户：管理账户角色和政策

角色	政策或政策
AWSManagedServicesBillingRole	AMSBilling政策 (AMSBilling政策) 。
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (公共 AWS 托管策略) 。
AWSManagedServicesCaseRole	ReadOnlyAccess

角色	政策或政策
AWSManagedServicesChangeManagementRole (管理账户版本)	AWSSupport访问权限 (公有 AWS 托管策略) 。
	ReadOnlyAccess
	AWSSupport访问
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

核心 OU 账户：网络账户角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (公共 AWS 托管策略) 。
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupport访问权限 (公有 AWS 托管策略) 。
AWSManagedServicesChangeManagementRole (网络账户版本)	ReadOnlyAccess
	AWSSupport访问
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

应用程序账户角色

应用程序账户角色适用于您的应用程序专用账户。

应用程序账户：角色和政策

角色	政策或政策
AWSManagedServicesReadOnlyRole	ReadOnlyAccess (公共 AWS 托管策略)。
AWSManagedServicesCaseRole	ReadOnlyAccess AWSSupport访问权限 (公有 AWS 托管策略)。 该政策提供对所有支持操作和资源的访问权限。 有关信息，请参阅 AWS Support 入门 。
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess AWSSupport访问 示例 该政策提供对所有支持操作和资源的访问权限。 AWSCertificateManagerFullAccess 信息，(公共 AWS 托管政策) AWSWAFFullAccess 信息，(公共 AWS 托管政策)。此政策授予对 AWS WAF 资源的完全访问权限。 AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (应用程序账号版本)	ReadOnlyAccess AWSSupport访问权限 (公有 AWS 托管策略)。 该政策提供对所有支持操作和资源的访问权限。 有关信息，请参阅 AWS Support 入门 。 AMSSecretsManagerSharedPolicy

角色	政策或政策
AWSManagedServicesAdminRole	AMSCheckManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Policy
	ReadOnlyAccess
	AWSSupport访问
	AMSCheckManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSCheckManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFull访问
	AMSS3Policy
	AMSReservedInstancesPolicy

策略示例

提供了大多数使用的策略的示例。要查看该 ReadOnlyAccess 政策（只要它提供对所有 AWS 服务的只读访问权限，则为页面），如果您有活跃的 AWS 账户，则可以使用此链接：[ReadOnlyAccess](#)。此外，此处还包括精简版。

AMSBilling政策

AMSBillingPolicy

您的会计部门可以使用新的账单角色来查看和更改管理账户中的账单信息或账户设置。要访问诸如备用联系人之类的信息、查看账户资源使用情况、查看账单甚至修改付款方式，您可以使用此角色。这个新角色包含 [AWS 账单 IAM 操作网页](#) 中列出的所有权限。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aws-portal:ViewBilling",
        "aws-portal:ModifyBilling"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToBilling"
    },
    {
      "Action": [
        "aws-portal:ViewAccount",
        "aws-portal:ModifyAccount"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToAccountSettings"
    },
    {
      "Action": [
        "budgets:ViewBudget",
        "budgets:ModifyBudget"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToAccountBudget"
    },
    {
      "Action": [
        "aws-portal:ViewPaymentMethods",
        "aws-portal:ModifyPaymentMethods"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToPaymentMethods"
    },
    {
      "Action": [
```

```

        "aws-portal:ViewUsage"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToUsage"
},
{
    "Action": [
        "cur:DescribeReportDefinitions",
        "cur:PutReportDefinition",
        "cur>DeleteReportDefinition",
        "cur:ModifyReportDefinition"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToCostAndUsageReport"
},
{
    "Action": [
        "pricing:DescribeServices",
        "pricing:GetAttributeValues",
        "pricing:GetProducts"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPricing"
},
{
    "Action": [
        "ce:*",
        "compute-optimizer:*"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToCostExplorerComputeOptimizer"
},
{
    "Action": [
        "purchase-orders:ViewPurchaseOrders",
        "purchase-orders:ModifyPurchaseOrders"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowAccessToPurchaseOrders"
}

```

```

    },
    {
      "Action": [
        "redshift:AcceptReservedNodeExchange",
        "redshift:PurchaseReservedNodeOffering"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AllowAccessToRedshiftAction"
    },
    {
      "Action": "savingsplans:*",
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "AWSSavingsPlansFullAccess"
    }
  ]
}

```

AMSChangeManagementReadOnlyPolicy

AMSChangeManagementReadOnlyPolicy

查看所有 AMS 变更类型以及请求更改类型的历史记录的权利。

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

请求 Deployment | Managed landing zone | 管理账户 | 创建应用程序账户 (使用 VPC) 更改类型的权限。

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

请求 Deployment | Managed landing zone | 网络账户 | 创建应用程序路由表更改类型的权限。

AMSChangeManagementInfrastructurePolicy

AMSChangeManagementInfrastructurePolicy (管理层 | 其他 | 其他 CTs)

请求 “管理” | “其他” | “其他” | “创建” 和 “管理” | “其他” | “其他” | “更新” 更改类型的权限。

AMSSecretsManagerSharedPolicy

AMSSecretsManagerSharedPolicy

查看 AMS 通过 passwords/hashtes 共享的机密的权限 AWS Secrets Manager（例如，用于审计的基础设施密码）。

创建与 AMS 共享 password/hashtes 的密钥的权限。（例如，需要部署的产品的许可证密钥）。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowAccessToSharedNameSpaces",
    "Effect": "Allow",
    "Action": "secretsmanager:*",
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
      "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    ]
  },
  {
    "Sid": "DenyGetSecretOnCustomerNamespace",
    "Effect": "Deny",
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
  },
  {
    "Sid": "AllowReadAccessToAMSNameSpace",
    "Effect": "Deny",
    "NotAction": [
      "secretsmanager:Describe*",
      "secretsmanager:Get*",
      "secretsmanager:List*"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
  ]
}
```

AMSCheckManagementPolicy

AMSCheckManagementPolicy

请求和查看所有 AMS 变更类型的权限，以及请求的更改类型的历史记录。

AMSReservedInstancesPolicy

AMSReservedInstancesPolicy

管理亚马逊 EC2 预留实例的权限；有关定价信息，请参阅[亚马逊 EC2 预留实例](#)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "AllowReservedInstancesManagement",
    "Effect": "Allow",
    "Action": [
      "ec2:ModifyReservedInstances",
      "ec2:PurchaseReservedInstancesOffering"
    ],
    "Resource": [
      "*"
    ]
  }]
}
```

AMSS3Policy

AMSS3Policy

在现有 Amazon S3 存储桶中创建和删除文件的权限。

Note

这些权限不授予创建 S3 存储桶的权限；必须使用部署 | 高级堆栈组件 | S3 存储 | 创建更改类型来完成。

JSON

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

AWSSupport访问权限

AWSSupportAccess

完全访问权限 支持。有关信息，请参阅[入门 支持](#)。有关 Premium Support 的信息，请参阅[支持](#)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "support:*"
    ],
    "Resource": "*"
  }]
}
```

AWSMarketplaceManageSubscriptions

AWSMarketplaceManageSubscriptions (公共 AWS管理政策)

订阅、取消订阅和查看订 AWS Marketplace 阅的权限。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "aws-marketplace:ViewSubscriptions",
      "aws-marketplace:Subscribe",
      "aws-marketplace:Unsubscribe"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

AWSCertificateManagerFullAccess

AWSCertificateManagerFullAccess

完全访问权限 AWS Certificate Manager。有关更多信息，请参阅 [AWS Certificate Manager](#)。

[AWSCertificateManagerFullAccess](#) 信息，(公共 AWS 托管政策)。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "acm:*"
    ],
    "Resource": "*"
  }]
}
```

AWSWAFFull访问权限

AWSWAFFullAccess

完全访问权限 AWS WAF。有关更多信息，请参阅 [AWS WAF -Web 应用程序防火墙](#)。

[AWSWAFFullAccess](#) 信息，(公共 AWS 管理政策)。此政策授予对 AWS WAF 资源的完全访问权限。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "waf:*",
      "waf-regional:*",
      "elasticloadbalancing:SetWebACL"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }]
}
```

ReadOnlyAccess

ReadOnlyAccess

对 AWS 控制台上所有 AWS 服务和资源的只读访问权限。AWS 启动新服务时，AMS 会更新 ReadOnlyAccess 政策，为新服务添加只读权限。更新的权限会应用于策略附加到的所有主体实体。

这并不能授予登录 EC2 主机或数据库主机的权限。

如果您有激活的政策 AWS 账户，则可以使用此[ReadOnlyAccess](#)链接查看整个 ReadOnlyAccess 政策。只要它为所有人提供只读访问权限，整个 ReadOnlyAccess 策略就会持续很长时间 AWS 服务。以下是该 ReadOnlyAccess 政策的部分摘录。

单账户着陆区 (SALZ)：要查看 AMS 单账户着陆区默认、未自定义的用户角色策略，请参阅“下一步”。[SALZ：默认 IAM 用户角色](#)

SALZ：默认 IAM 用户角色

默认 AMS 单账户 landing zone 用户角色的 JSON 政策声明。

Note

SALZ 默认用户角色是可自定义的，可能因每个账户而异。提供了有关如何找到您的角色的说明。

以下是默认 SALZ 用户角色的示例。要确保已为您设置了策略，请运行 [get-role](#) 命令。或者，登录 AWS Identity and Access Management 控制台 <https://console.aws.amazon.com/iam/>，然后选择“角色”。

客户只读角色是多个策略的组合。以下是该角色的细分 (JSON)。

Managed Services 审计政策：

托管服务 IAM ReadOnly 政策

Managed Services 用户政策

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCustomerToListTheLogBucketLogs",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "aws/*",
            "app/*",
            "encrypted",
            "encrypted/",
            "encrypted/app/*"
          ]
        }
      }
    }
  ]
}
```

```

    ]
  }
}
},
{
  "Sid": "BasicAccessRequiredByS3Console",
  "Effect": "Allow",
  "Action": [
    "s3:ListAllMyBuckets",
    "s3:GetBucketLocation"
  ],
  "Resource": [
    "arn:aws:s3::*"
  ]
},
{
  "Sid": "AllowCustomerToGetLogs",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject*"
  ],
  "Resource": [
    "arn:aws:s3::mc-a*-logs-*/aws/*",
    "arn:aws:s3::mc-a*-logs-*/encrypted/app/*"
  ]
},
{
  "Sid": "AllowAccessToOtherObjects",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteObject*",
    "s3:Get*",
    "s3:List*",
    "s3:PutObject*"
  ],
  "Resource": [
    "*"
  ]
},
{
  "Sid": "AllowCustomerToListTheLogBucketRoot",
  "Effect": "Allow",
  "Action": [
    "s3:ListBucket"
  ]
}

```



```

    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
        "StringEquals": {
            "s3:prefix": [
                "",
                "/"
            ]
        }
    }
},
{
    "Sid": "AllowCustomerCWLConsole",
    "Effect": "Allow",
    "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:*"
    ]
},
{
    "Sid": "AllowCustomerCWLAccessLogs",
    "Effect": "Allow",
    "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
    ]
},
{
    "Sid": "AWSManagedServicesFullAccess",
    "Effect": "Allow",
    "Action": [
        "amscm:*",
        "amsskms:*"
    ]
}

```

```
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "ModifyAWSBillingPortal",
    "Effect": "Allow",
    "Action": [
        "aws-portal:Modify*"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "DenyDeleteCWL",
    "Effect": "Deny",
    "Action": [
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:*"
    ]
},
{
    "Sid": "DenyMCCWL",
    "Effect": "Deny",
    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
    ]
},
{
    "Sid": "DenyS3MCNamespace",
    "Effect": "Deny",
```

```

    "Action": [
      "s3:*"
    ],
    "Resource": [
      "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
      "arn:aws:s3:::mc-a*-logs-*/mc/*",
      "arn:aws:s3:::mc-a*-logs-*--audit/*",
      "arn:aws:s3:::mc-a*-internal-*/*",
      "arn:aws:s3:::mc-a*-internal-*"
    ]
  },
  {
    "Sid": "ExplicitDenyS3CfnBucket",
    "Effect": "Deny",
    "Action": [
      "s3:*"
    ],
    "Resource": [
      "arn:aws:s3:::cf-templates-*"
    ]
  },
  {
    "Sid": "DenyListBucketS3LogsMC",
    "Action": [
      "s3:ListBucket"
    ],
    "Effect": "Deny",
    "Resource": [
      "arn:aws:s3:::mc-a*-logs-*"
    ],
    "Condition": {
      "StringLike": {
        "s3:prefix": [
          "auditlog/*",
          "encrypted/mc/*",
          "mc/*"
        ]
      }
    }
  },
  {
    "Sid": "DenyS3LogsDelete",
    "Effect": "Deny",
    "Action": [

```

```

        "s3:Delete*",
        "s3:Put*"
    ],
    "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
    ]
},
{
    "Sid": "DenyAccessToKmsKeysStartingWithMC",
    "Effect": "Deny",
    "Action": [
        "kms:*"
    ],
    "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
    ]
},
{
    "Sid": "DenyListingOfStacksStartingWithMC",
    "Effect": "Deny",
    "Action": [
        "cloudformation:*"
    ],
    "Resource": [
        "arn:aws:cloudformation::*:stack/mc-*"
    ]
},
{
    "Sid": "AllowCreateCWMetricsAndManageDashboards",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricData"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowCreateandDeleteCWDashboards",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
    ]
}

```

```

    ],
    "Resource": [
        "*"
    ]
  }
]
}

```

客户 Secrets Manager 共享政策

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager::*:secret:ams-shared/*",
        "arn:aws:secretsmanager::*:secret:customer-shared/*"
      ]
    },
    {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager::*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ]
    }
  ]
}

```

```
    ],  
    "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"  
  }  
]  
}
```

客户市场订阅政策

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "AllowMarketPlaceSubscriptions",  
      "Effect": "Allow",  
      "Action": [  
        "aws-marketplace:ViewSubscriptions",  
        "aws-marketplace:Subscribe"  
      ],  
      "Resource": [  
        "*"   
      ]  
    }  
  ]  
}
```

安全事件日志记录和监控

AMS 持续监控托管环境中是否存在安全威胁。AMS 或您可能会检测到安全事件。AMS 根据美国国家标准与技术研究院 (NIST) 的《计算机安全事件处理指南》定期更新其自动化流程，以更好地检测安全威胁。

端点安全 (EPS)

您在 AMS Advanced 环境中配置的资源自动包括安装端点安全 (EPS) 监控客户端。此过程可确保全天候监控和支持 AMS Advanced 管理的资源。此外，AMS Advanced 会监控所有代理活动，如果检测到任何安全事件，就会创建事件。

 Note

安全事件作为事件处理；有关更多信息，请参阅[事件响应](#)。

端点安全提供反恶意软件保护，具体而言，支持以下操作：

- EC2 向 EPS 注册的实例
- EC2 从 EPS 取消注册的实例
- EC2 实例实时反恶意软件保护
- EPS 代理启动的心跳
- EPS 恢复隔离的文件
- EPS 事件通知
- 每股收益报告

AMS Advanced 使用趋势科技实现端点安全 (EPS)。这些是默认 EPS 设置。要了解有关趋势科技的更多信息，请参阅趋势科技[趋势科技服务器深度安全防护系统帮助中心](#)；请注意，非亚马逊链接可能会更改，恕不另行通知。

以下章节介绍了 AMS 高级多账户着陆区 (MALZ) 的默认设置；有关非默认 AMS 多账户着陆区 EPS 设置，[请参阅 AMS 高级多账户着陆区 EPS 非默认设置](#)。

 Note

你可以自备 EPS，请参阅 [AMS 自带 EPS](#)。

常规 EPS 设置

端点安全常规网络设置。

每股收益默认值

设置	Default
防火墙端口（实例的安全组）	EPS 趋势科技服务器深度安全防护系统管理中心代理 (DSMs) 必须打开端口 4120 Agent/Relay 才能与管理中心通信，为管理中心控制台

设置	Default
	打开端口 4119。EPS 中继必须打开端口 4122 Manager/Agent 才能与中继通信。不应为客户实例的入站通信打开特定的端口，因为代理会启动所有请求。
沟通方向	客户端/设备已启动
心跳间隔	十分钟
警报前错过的心跳次数	二
服务器时间之间允许的最大偏差（差）	无限制
对处于非活动状态（已注册但未联机）的虚拟机引发脱机错误	否
默认策略	基本政策（下文将介绍）
使用相同主机名激活多台计算机	被允许
已发出待定更新的警报	七天后
更新日程安排	AMS 的目标是趋势科技趋势科技服务器深度安全防护系统管理中心 (DSM) /趋势科技服务器深度安全防护系统客户端 (DSA) 软件更新的每月发布周期。但是，AMS 不维护更新的 SLA。在部署期间，AMS 开发团队在整个舰队范围内执行更新。 DSA/DSA 更新记录在趋势科技 DSM 系统事件中，AMS 默认在本地保留这些事件 13 周。有关供应商文档，请参阅趋势科技趋势科技服务器深度安全防护 系统帮助中心中的系统事件。日志还会导出到亚马逊 CloudWatch 的日志组/ aws/ ams/eps/var/log/DSM .log。
更新源代码	趋势科技更新服务器 (https://ipv6-iaus.trendmicro.com/iau_server.dll/)

设置	Default
删除事件或日志数据	事件和日志将在七天后从 DSM 数据库中删除。
代理软件版本已保留	最多五个
最新规则更新已保存	最多十个
日志存储	默认情况下，日志文件安全地存储在 Amazon S3 中，但您也可以将其存档到 Amazon Glacier，以帮助满足审计和合规要求。

基本政策

端点安全基础策略默认设置。

每股收益基本政策

设置	Default
已启用的模块	防恶意软件
已禁用的模块	网络信誉
	防火墙
	入侵防护
	完整性监控
	日志审查
	应用程序控制

反恶意软件

端点安全防恶意软件设置。

EPS 防恶意软件默认值

设置	Default	备注
实时扫描	扫描所有内容 每 Day/All 天 (24 小时)	隔离所有可疑病毒。 启用 IntelliTrap 和 spyware/grayware 保护。 间谍软件和灰色软件会触发防恶意软件并导致该项目被隔离。
手动扫描	扫描所有内容	必须请求，然后遵循默认的实时扫描配置。
预设扫描	扫描所有内容	定于每个月的最后一个星期日，早上 6 点。
智能防护	已禁用	不适用
隔离的文件	趋势科技趋势科技服务器深度安全防护系统管理中心 (DSM)	预留大约 1GB 的磁盘用于隔离。
扫描限制	趋势科技 DSM	扫描各种大小的文件。
允许的间谍软件或灰色软件	无	不适用
本地事件通知	是	不适用

恶意软件缓解流程

AMS 使用趋势科技的趋势科技服务器深度安全防护平台（反恶意软件系统）来检测和响应您的 AMS 托管实例上的恶意软件。默认情况下，趋势科技检测代理在所有 Amazon EC2 实例上运行，包括共享服务和私有子网中的实例，适用于 Windows 和 Linux 操作系统。反恶意软件系统连接到 AMS 监控，

因此每当检测到恶意软件时都会生成事件。如果对客户造成影响，则事件将上报至事件管理流程（有关详细信息，请参阅[AMS 事件响应](#)）。在 AMS 评估影响时，您会收到通知，并尝试减轻影响。

趋势科技发布更新时，趋势科技的防恶意软件定义会自动更新。

在应用程序启动期间，您需要指明在实例上发现恶意软件时希望 AMS 采取的操作：

- 确保隔离文件在允许列表中，将其从隔离区中删除，然后将其释放回文件系统。
- 删除隔离文件，将其从实例中移除。
- 暂停实例并替换它。然后，您可以挂载暂停的实例以进行取证研究。

申请入职后：

- 当反恶意软件系统在实例上发现恶意软件时，AMS 会自动隔离该恶意软件。这会触发事件和后续调查。
- AMS 通过服务通知将事件通知您，并开始遵循您选择的默认缓解措施。
- 如果您尚未选择默认操作，AMS 会询问您要采取哪项操作。收到您的指示后，AMS 会运行所选操作并通知您。操作完成后，AMS 会再次通知您，包括取证分析所需的详细信息（如果适用）。

在趋势科技趋势科技服务器深度安全防护系统中启用 IDS 和 IPS

您可以请求 AMS 为您的账户启用趋势科技入侵检测系统 (IDS) 和入侵防护系统 (IPS)（非默认功能）。

为此，请提交更新请求（管理 | 其他 | 其他 | 更新），并附上用于接收 IDS 和 IPS 通知的电子邮件地址列表。这些地址将添加到您账户中的 SNS 主题中，AMS 会为您创建该主题。

Note

AMS 不能添加任何可能干扰我们提供其他 AMS 服务的趋势科技服务。

全系统恶意软件扫描

支付卡行业数据安全标准 (PCI DSS) 要求进行完整的系统恶意软件扫描，默认情况下，AMS 管理的 VPC 上已启用这些扫描。完整系统扫描设置为凌晨 2 点（服务器上设置的时区）进行，因为它们会占用大量 CPU。除了不占用大量 CPU 的常规恶意软件扫描之外，还会进行全面的系统扫描。

新增了管理更改类型 (CT)，即禁用恶意软件扫描，允许您禁用完整的系统恶意软件扫描。您可以在管理 | 主机安全 | 完整系统扫描 | 禁用分类，更改 ID ct-1pybwg08h8qsz 中找到 CT。要重新启用扫描，请使用管理 | 其他 | 其他 | 更新 CT。禁用完整系统扫描不会禁用常规恶意软件扫描。

亚马逊 Inspector 安全

Amazon Inspector 服务监控 AMS 管理的堆栈的安全。Amazon Inspector 是一项自动安全评估服务，可帮助识别部署在其上的基础设施在安全与合规方面的差距 AWS。Amazon Inspector 安全评估使您能够通过检查您的亚马逊实例中是否存在意想不到的网络可访问性和漏洞，自动评估堆栈的漏洞、漏洞以及与最佳实践的偏差。EC2 执行评估后，Amazon Inspector 将生成按严重性级别优先排序的安全调查发现详细列表。Amazon Inspector 评估以预定义规则包的形式提供，这些规则包与常见的安全最佳实践和定义相对应。这些规则由 AWS 安全研究人员定期更新。有关 Amazon Inspector 的更多信息，请访问[亚马逊 Inspector](#)。

AMS 亚马逊 Inspector FAQs

- 我的 AMS 账户是否默认安装了 Amazon Inspector？

不是。Amazon Inspector 不是默认 AMI 版本或工作负载摄取的一部分。

- 如何访问和安装 Amazon Inspector？

向 Inspector 提交 RFC (管理 | 其他 | 其他 | 创建) 以申请账户访问和安装，AMS 运营团队将修改 Customer_ReadOnly_Role 以提供 Amazon Inspector 控制台访问权限 (没有 SSM 访问权限)。

- 我想要评估的所有亚马逊 EC2 实例上都必须安装 Amazon Inspector 代理吗？

不需要，使用网络可访问性规则包的 Amazon Inspector 评估可以在没有代理的情况下运行任何亚马逊 EC2 实例。主机评估规则包需要代理。有关代理安装的更多信息，请参阅[安装 Amazon Inspector 代理](#)。

- 这项服务需要额外费用吗？

是。Amazon Inspector 的定价可以在[亚马逊 Inspector 定价](#)网站上找到。

- Amazon Inspector 的发现是什么？

调查结果是指在 Amazon Inspector 对所选评估目标进行评估期间发现的潜在安全问题。调查结果显示在 Amazon Inspector 控制台或 API 中，其中包含对安全问题的详细描述和解决这些问题的建议。

- Amazon Inspector 评估报告是否可用？

是。评估报告是一种文档，用于详细介绍评估运行的测试内容和评估结果。评估结果采用标准报告格式，可用于在团队内部分享实施修正措施的结果，丰富合规性审计数据，或存储以供将来参考。成功完成评估后，可以为评估运行生成 Amazon Inspector 评估报告。

- 我能否使用标签来识别我要针对哪些堆栈运行 Amazon Inspector 报告？

是。

- AMS 运营团队能否获得 Amazon Inspector 的评估结果？

是。任何有权访问 AWS 中的 Amazon Inspector 控制台的人都可以查看调查结果和评估报告。

- AMS 运营团队会根据亚马逊 Inspector 报告的调查结果提出建议或采取行动吗？

不是。如果您想根据 Amazon Inspector 报告的调查结果进行更改，则必须通过 RFC（管理 | 其他 | 其他 | 其他 | 更新）申请更改。

- 当我运行 Amazon Inspector 报告时，AMS 会收到通知吗？

当您申请 Amazon Inspector 访问权限时，运行 RFC 的 AMS 操作员会将请求通知您的 CSDM。

有关更多信息，请参阅 [Amazon Inspector FAQs](#)。

AMS 事件响应

AMS 使用传统的 IT 服务管理 (ITSM) 事件管理最佳实践，在需要时尽快恢复服务。

我们通过遍布全球的多个运营中心提供全天候 follow-the-sun 支持，专门的操作员会主动监控仪表板和事件队列。

我们的运营工程师使用内部事件跟踪工具来识别、记录、分类、确定优先级、诊断、解决和关闭事件，并通过 AMS 控制台或支持 API 向您提供所有这些活动的最新信息。我们的操作员中有许多人曾在 AWS Premium Support 担任过各种技术背景和职务，他们利用各种内部支持工具来帮助完成所有这些活动。这些运营商对 AMS 支持的基础设施非常熟悉，并且具有解决所有已确定的支持问题的专家级技术技能。在极少数情况下，我们的操作员需要帮助，Premium Support 和 AWS 服务团队可以根据需要提供帮助。

如果高优先级事件影响您的关键工作负载，AMS 将建议恢复基础架构。通常需要在故障排除问题或从已知良好的备份中恢复之间进行权衡，而客户风险和服务停机造成的影响是决定性因素。如果您有时间解决问题，AMS 将为您提供帮助，但如果恢复的紧迫性很高，我们可以立即启动恢复。

 Note

不属于堆栈模板或数据恢复的临时数据会丢失。当 AWS 服务不可用时，AMS 会尽合理努力执行基础设施恢复。提供 AWS 服务后，基础架构恢复即告完成。

如果您未按照 AMS 的建议授权恢复基础架构，则您将没有资格在事件解决时间内获得 AMS 服务承诺的服务积分。

合规性验证

AMS 部署并管理 AWS Config 规则和补救措施库，以防出现可能降低账户安全性和运营完整性的错误配置。

例如，创建 Amazon S3 存储桶时，AWS Config 可以根据要求 Amazon S3 存储桶拒绝公开读取访问的规则来评估 Amazon S3 存储桶。如果 Amazon S3 存储桶策略或存储桶访问控制列表 (ACL) 允许公共读取权限，则会将存储桶和规则 AWS Config 标记为不合规。它们根据评估结果将资源 AWS Config 规则 标记为“合规”、“不合规”或“不适用”。有关 AWS Config 服务的更多信息，请参阅《[AWS Config 开发人员指南](#)》。

您可以使用 AWS Config 控制台、AWS CLI 或 AWS Config API 来查看您的账户中部署的规则以及规则和资源的合规状态。有关更多信息，请参阅 AWS Config 文档：[查看配置合规性](#)。

 Note

有关此主题的更多信息，请访问 AWS Artifact 报告。有关更多信息，请参阅[在 Amazon Artifact 中下载报告](#)。要访问 AWS Artifact，您可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。此信息未包含在本用户指南中，因为它包含敏感的安全内容。

多账户登录区查看您的合规状态 AWS Config 规则

AMS 多账户 landing zone 利用 AWS Config 聚合器服务来创建所有账户合规的集中视图。这意味着您可以在安全账户的聚合 AWS Config 器下查看 AWS Config 规则 所有 AMS 多账户 landing zone 环境中的合规状态。

以下是展示 AWS Config 规则 跨账户集中合规状态的 AWS Config 聚合器示例。

有关更多信息，请参阅 [Config Aggregator](#) 的 AWS 文档。

- AMS 如何使用 AWS Config 规则？

AMS 创建的 AWS Config 规则 目的是让您可以根据规则中指定的条件查看您的 AWS 资源配置。如果规则不合规，您可以申请更改，AMS Ops 团队将与您合作采取纠正措施。

- 在这种情况下，您会看到您的 AMS 账户中出现以下更改：
 - AWS Config 规则 在 AWS Config > 规则下
 - 您的账户中存在带有 Lambda 函数的自定义 Config 规则
 - 安全账户中的 Config Aggregator 和所有账户中的 Config 授权（仅限多账户登录区域）

以下是样本，其 AWS Config 规则 合规性评估结果如下所示：

要了解有关 AWS Config 的更多信息，请参阅：

- AWS Config：[什么是配置？](#)
- AWS Config 规则：[使用规则评估资源](#)
- AWS Config 规则：[动态合规性检查：AWS Config 规则 — 云资源的动态合规性检查](#)
- AWS Config 聚合器：[多账户多区域](#)数据聚合

AMS 多账户 landing zone 服务控制策略限制

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。

恢复能力

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础结构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅[AWS 全球基础设施](#)。

基础结构安全性

Note

有关此主题的更多信息，请访问 AWS Artifact 报告。有关更多信息，请参阅在 [Amazon Artifact 中下载报告](#)。要访问 AWS Artifact，您可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。此信息未包含在本用户指南中，因为它包含敏感的安全内容。

end-of-support操作系统的控制

不在操作系统制造商的“end-of-support”或 EOS 的常规支持期内，并且未收到安全更新的操作系统的安全风险会增加。

AWS 提供一些服务来帮助处理操作系统 end-of-support。有关 Windows 的信息 end-of-support，请参阅适用于 [Windows 服务器的 End-of-Support 迁移程序](#)。

Note

有关此主题的更多信息，请访问 AWS Artifact 报告。有关更多信息，请参阅在 [Amazon Artifact 中下载报告](#)。要访问 AWS Artifact，您可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。此信息未包含在本用户指南中，因为它包含敏感的安全内容。

使用安全组

安全组起着虚拟防火墙的作用，可控制一个或多个实例的流量。AMS 安全组允许您在实例级别上设置入站流量规则和出站流量规则。您可以创建安全组并指定要与安全组关联的 AMS 账户、Amazon EC2 实例、Amazon RDS 数据库实例、负载均衡器、趋势科技服务器深度安全防护系统管理中心 (DSM) 复制实例、EFS 挂载目标和 ElastiCache 集群中的资源。关联后，进出这些实例的流量将受到安全组中设置的规则的限制。

要更好地了解 AWS 的一般安全性，请参阅[安全、身份与合规最佳实践和适用于 Linux 实例的 Amazon EC2 安全组](#)。

AMS 现在有一组用于创建和管理安全组的更改类型：

- 部署 | 高级堆栈组件 | 安全组 | 创建 (ct-10xx2g2d7hc90)

- 管理 | 高级堆栈组件 | 安全组 | 删除 (ct-3cp96z7r065e4)
- 管理 | 高级堆栈组件 | 安全组 | 更新 (ct-3memthlcmvc1b)

有关示例，请参阅[安全组](#)。

安全组

在 AWS 中 VPCs，AWS 安全组充当虚拟防火墙，控制一个或多个堆栈（一个或一组实例）的流量。堆栈启动时，它会与一个或多个安全组相关联，这些安全组决定了允许哪些流量到达堆栈：

- 对于公有子网中的堆栈，默认安全组接受来自所有位置（互联网）的 HTTP (80) 和 HTTPS (443) 流量。这些堆栈还接受来自您的公司网络和 AWS 堡垒的内部 SSH 和 RDP 流量。然后，这些堆栈可以通过任何端口导出到互联网。它们还可以输出到您的私有子网和公有子网中的其他堆栈。
- 私有子网中的堆栈可以输出到私有子网中的任何其他堆栈，并且堆栈中的实例可以通过任何协议相互完全通信。

Important

私有子网上堆栈的默认安全组允许私有子网中的所有堆栈与该私有子网中的其他堆栈通信。如果要限制私有子网内堆栈之间的通信，则必须创建描述限制的新安全组。例如，如果您想限制与数据库服务器的通信，使该私有子网中的堆栈只能通过特定端口从特定的应用程序服务器进行通信，请请求特殊的安全组。本节将介绍如何执行此操作。

默认安全组

MALZ

下表描述了堆栈的默认入站安全组 (SG) 设置。SG 名为

“SentinelDefaultSecurityGroupPrivateOnly-vpc-id”，其中是 **ID** AMS 多账户着陆区账户中的 VPC ID。允许所有流量通过此安全组出站到 SentinelDefaultSecurityGroupPrivateOnly “mc-initial-garden-”（允许堆栈子网内的所有本地流量）。

第二个安全组 “” 允许所有流量出站到 0.0.0.0/0。SentinelDefaultSecurityGroupPrivateOnly

 Tip

如果您为 AMS 更改类型（例如 EC2 创建或 OpenSearch 创建域）选择安全组，则应使用此处描述的默认安全组之一，或者使用您创建的安全组。您可以在 AWS EC2 控制台或 VPC 控制台中找到每个 VPC 的安全组列表。

还有其他用于内部 AMS 目的的默认安全组。

AMS 默认安全组（入站流量）

类型	协议	端口范围	源
所有流量	All	全部	SentinelDefaultSecurityGroupPrivateOnly（限制同一安全组成员的出站流量）
所有流量	All	全部	SentinelDefaultSecurityGroupPrivateOnlyEgressAll（不限制出站流量）
HTTP、HTTPS、SSH、	TCP	80/443（来源 0.0.0.0/0） 允许从堡垒访问 SSH 和 RDP	SentinelDefaultSecurityGroupPublic（不限制出站流量）
MALZ 堡垒：			
SSH	TCP	22	SharedServices VPC CIDR 和 DMZ VPC CIDR，以及客户提供的本地部署 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 堡垒：			
SSH	TCP	22	mc-initial-garden-LinuxBastion SG
SSH	TCP	22	mc-initial-garden-LinuxBastion DMZSG

类型	协议	端口范围	源
RDP	TCP	3389	mc-initial-garden-WindowsBastion SG
RDP	TCP	3389	mc-initial-garden-WindowsBastion DMZSG

SALZ

下表描述了堆栈的默认入站安全组 (SG) 设置。SG 名为 “mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly-**ID**”，其中 **ID** 是唯一标识符。允许所有流量通过此安全组出站到 SentinelDefaultSecurityGroupPrivateOnly “mc-initial-garden-” (允许堆栈子网内的所有本地流量) 。

第二个安全组 “mc-initial-garden--” 允许所有流量出站到 0.0.0.0/0。SentinelDefaultSecurityGroupPrivateOnlyEgressAll **ID**

 Tip

如果您为 AMS 更改类型 (例如 EC2 创建或 OpenSearch 创建域) 选择安全组，则应使用此处描述的默认安全组之一，或者使用您创建的安全组。您可以在 AWS EC2 控制台或 VPC 控制台中找到每个 VPC 的安全组列表。

还有其他用于内部 AMS 目的的默认安全组。

AMS 默认安全组 (入站流量)

类型	协议	端口范围	源
所有流量	All	全部	SentinelDefaultSecurityGroupPrivateOnly (限制同一安全组成员的出站流量)
所有流量	All	全部	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (不限制出站流量)
HTTP、HTTPS、SSH、	TCP	80/443 (来源 0.0.0.0/0)	SentinelDefaultSecurityGroupPublic (不限制出站流量)

类型	协议	端口范围	源
		允许从堡垒访问 SSH 和 RDP	
MALZ 堡垒：			
SSH	TCP	22	SharedServices VPC CIDR 和 DMZ VPC CIDR , 以及客户提供的本地部署 CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
SALZ 堡垒：			
SSH	TCP	22	mc-initial-garden-LinuxBastion SG
SSH	TCP	22	mc-initial-garden-LinuxBastion DMZSG
RDP	TCP	3389	mc-initial-garden-WindowsBastion SG
RDP	TCP	3389	mc-initial-garden-WindowsBastion DMZSG

创建、更改或删除安全组

您可以请求自定义安全组。如果默认安全组不能满足您的应用程序或组织的需求，则可以修改或创建新的安全组。此类申请将被视为需要批准，并将由AMS运营团队进行审查。

要在堆栈之外创建安全组 VPCs，请使用Deployment | Advanced stack components | Security group | Create (review required)更改类型 (ct-1oxx2g2d7hc90) 提交 RFC。

要修改活动目录 (AD) 安全组，请使用以下更改类型：

- 添加用户：使用管理 | Directory Service | 用户和群组 | 将用户添加到群组 [ct-24pi85mjtza8k] 提交 RFC
- 要移除用户：使用管理 | Directory Service | 用户和群组 | 从群组中移除用户 [ct-2019s9y3nfml4] 提交 RFC

Note

使用“需要审核”时 CTs，AMS 建议您使用“尽快安排”选项（在控制台中选择“尽快”，在 API/CLI 中将开始和结束时间留空），因为这些选项 CTs 要求 AMS 操作员检查 RFC，并可能在批准和运行之前与您沟通。如果您安排这些活动 RFCs，请务必留出至少 24 小时的时间。如果在预定开始时间之前未获得批准，RFC 将被自动拒绝。

查找安全组

要查找附加到堆栈或实例的安全组，请使用 EC2 控制台。找到堆栈或实例后，您可以看到与其关联的所有安全组。

有关在命令行中查找安全组并筛选输出的方法，请参阅[describe-security-groups](#)。

AMS 预防和侦探控制库

AWS Managed Services (AMS) 为您提供 library/catalog 一系列行之有效的服务控制策略 (SCPs) ConfigRules，这些策略可以用来改善您的安全状况并缩小 AMS 账户中的合规漏洞。

主题

- [精选规则 SCPs 和 Config 规则](#)
- [Config 规则的自定义通知](#)

精选规则 SCPs 和 Config 规则

AMS Advanced 的精选规则 SCPs 和 Config 规则。

- 服务控制策略 (SCPs)：提供的策略 SCPs 是默认 AMS 策略的补充。

您可以将这些库控件与默认库控件配合使用，以满足特定的安全要求。

- 配置规则：作为基准衡量标准，AMS 建议应用一致性包（参见 AWS Config 指南中的[一致性包](#)）以及默认 AMS 配置规则（有关默认规则，请参阅 AMS Artifacts）。合规包涵盖了大部分合规要求，AWS 会定期对其进行更新。

此处列出的规则可用于弥补一致性包未涵盖的特定用例差距

 Note

随着 AMS 默认规则和一致性包会随着时间的推移而更新，您可能会看到这些规则的重复内容。

一般而言，AMS 建议定期清理重复的 Config 规则。

对于 AMS Advanced，为了避免更改，配置规则不应使用自动修复（请参阅[通过 AWS Config 规则修复不合规的 AWS 资源](#)）。out-of-band

SCP-AMS-001：限制 EBS 的创建

如果您未启用加密，请阻止创建 EBS 卷。

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:CreateVolume",
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-002：限制 EC2 启动

如果 EBS 卷未加密，则禁止启动 EC2 实例。这包括拒绝未加密的 EC2 启动，AMIs 因为此 SCP 也适用于根卷。

```
{
  "Condition": {
    "Bool": {
      "ec2:Encrypted": "false"
    }
  },
  "Action": "ec2:RunInstances",
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Effect": "Deny"
}
```

SCP-ADV-001：限制 RFC 提交

限制默认 AMS 角色自动提交特定的角色，RFCs 例如创建 VPC 或删除 VPC。如果您想对联合角色应用更精细的权限，这会很有用。

例如，您可能希望默认 `AWSManagedServicesChangeManagement Role` 用户能够提交大部分可用信息，但允许创建和删除 VPC、创建其他子网、退出应用程序账户、更新或删除 SAML 身份提供商的 RFCs 除外：

SCP-AMS-003：限制在 AMS 中创建 RDS EC2 或 RDS

防止创建没有特定标签的 Amazon EC2 和 RDS 实例，同时允许 AMS 默认 `AMS Backup IAM` 角色这样做。这是灾难恢复或灾难恢复所必需的

```
{
  "Sid": "DenyRunInstanceWithNoOrganizationTag",
  "Effect": "Deny",
  "Action": [
    "ec2:RunInstances",
    "rds:CreateDBInstance"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:rds:*:*:db:*"
  ],
  "Condition": {
    "Null": {
      "aws:RequestTag/organization": "true"
    },
    "StringNotLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::<Account_Number>:role/ams-backup-iam-role"
      ]
    }
  }
}
```

SCP-AMS-004：限制 S3 的上传

防止上传未加密的 S3 对象。

```
{
```



```

        "Sid": "DenyUnencryptedS3Uploads",
        "Effect": "Deny",
        "Action": "s3:PutObject",
        "Resource": "*",
        "Condition": {
            "StringNotLike": {
                "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]
            },
            "Null": {
                "s3:x-amz-server-side-encryption": "false"
            }
        }
    }
}
]
}

```

SCP-AMS-005：限制 API 和控制台访问权限

阻止 AWS 控制台和 API 以确定的客户身份访问来自已知不良 IP 地址的请求 InfoSec。

SCP-AMS-006：阻止 IAM 实体从组织中移除成员账户

防止 AWS Identity and Access Management 实体从组织中移除成员帐户。

```

{
  "Effect": "Deny",
  "Action": ["organizations:LeaveOrganization"],
  "Resource": ["*"]
}

```

SCP-AMS-007：防止与组织外部的账户共享资源

防止与 AWS 组织外部帐户共享资源

```

{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": [
    "*"
  ]
}

```

```

    ],
    "Condition": {
      "Bool": {
        "ram:AllowsExternalPrincipals": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": [
      "ram:CreateResourceShare",
      "ram:UpdateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "ram:RequestedAllowsExternalPrincipals": "true"
      }
    }
  }
}

```

SCP-AMS-008：防止与组织或组织单位共享 (OUs)

防止与组织中的账户 and/or OU 共享资源。

```

{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "ram:Principal": [
        "arn:aws:organizations::*:account/o-${OrganizationId}/${AccountId}",
        "arn:aws:organizations::*:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
      ]
    }
  }
}

```

SCP-AMS-009：阻止用户接受资源共享邀请

阻止成员账户接受加入资源共享 AWS RAM 的邀请。此 API 不支持任何条件，并且只能阻止来自外部账户的共享。

```
{
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}
```

SCP-AMS-010：禁止使用账户区域启用和禁用操作

防止为您的 AWS 账户启用或禁用任何新 AWS 区域。

```
{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

SCP-AMS-011：阻止账单修改操作

防止修改账单和付款配置。

```
{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ],
  "Resource": "*"
}
```

SCP-AMS-012：防止对特定内容进行删除或修改 CloudTrails

防止修改特定 AWS CloudTrail 路径。

```
{
```

```
"Effect": "Deny",
"Action": [
  "cloudtrail:DeleteEventDataStore",
  "cloudtrail:DeleteTrail",
  "cloudtrail:PutEventSelectors",
  "cloudtrail:PutInsightSelectors",
  "cloudtrail:UpdateEventDataStore",
  "cloudtrail:UpdateTrail",
  "cloudtrail:StopLogging"
],
"Resource": [
  "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"
]
}
```

SCP-AMS-013 : 防止禁用默认 EBS 加密

防止禁用默认 Amazon EBS 加密。

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

SCP-AMS-014 : 防止创建默认 VPC 和子网

防止创建默认 Amazon VPC 和子网。

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc"
  ],
  "Resource": "*"
}
```

SCP-AMS-015 : 防止禁用和修改 GuardDuty

GuardDuty 防止亚马逊被修改或禁用。

```
{
  "Effect": "Deny",
  "Action": [
    "guardduty:AcceptInvitation",
    "guardduty:ArchiveFindings",
    "guardduty:CreateDetector",
    "guardduty:CreateFilter",
    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty>DeleteDetector",
    "guardduty>DeleteFilter",
    "guardduty>DeleteInvitations",
    "guardduty>DeleteIPSet",
    "guardduty>DeleteMembers",
    "guardduty>DeletePublishingDestination",
    "guardduty>DeleteThreatIntelSet",
    "guardduty:DisableOrganizationAdminAccount",
    "guardduty:DisassociateFromMasterAccount",
    "guardduty:DisassociateMembers",
    "guardduty:InviteMembers",
    "guardduty:StartMonitoringMembers",
    "guardduty:StopMonitoringMembers",
    "guardduty:TagResource",
    "guardduty:UnarchiveFindings",
    "guardduty:UntagResource",
    "guardduty:UpdateDetector",
    "guardduty:UpdateFilter",
    "guardduty:UpdateFindingsFeedback",
    "guardduty:UpdateIPSet",
    "guardduty:UpdateMalwareScanSettings",
    "guardduty:UpdateMemberDetectors",
    "guardduty:UpdateOrganizationConfiguration",
    "guardduty:UpdatePublishingDestination",
    "guardduty:UpdateThreatIntelSet"
  ],
  "Resource": "*"
}
```

SCP-AMS-016 : 防止 root 用户活动

阻止 root 用户执行任何操作。

```
{
  "Action": "*",
  "Resource": "*",
  "Effect": "Deny",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:root"
      ]
    }
  }
}
```

SCP-AMS-017 : 阻止为 root 用户创建访问密钥

阻止为 root 用户创建访问密钥。

```
{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

SCP-AMS-018 : 防止禁用 S3 账户公共访问封锁

防止禁用 Amazon S3 账户的公开访问封锁。这样可以防止账户中的任何存储桶被公开。

```
{
  "Effect": "Deny",
  "Action": "s3:PutAccountPublicAccessBlock",
  "Resource": "*"
}
```

SCP-AMS-019 : 防止禁用 AWS Config 或修改配置规则

防止禁用或修改 AWS Config 规则。

```
{
```

```
"Effect": "Deny",
"Action": [
  "config:DeleteConfigRule",
  "config:DeleteConfigurationRecorder",
  "config:DeleteDeliveryChannel",
  "config:DeleteEvaluationResults",
  "config:StopConfigurationRecorder"
],
"Resource": "*"
}
```

SCP-AMS-020 : 阻止所有 IAM 操作

阻止所有 IAM 操作。

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": "*"
}
```

SCP-AMS-021 : 防止删除 CloudWatch 日志组和流

防止删除 Amazon CloudWatch 日志组和直播。

```
{
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": "*"
}
```

SCP-AMS-022 : 防止 Glacier 被删除

防止删除 Amazon Glacier。

```
{
  "Effect": "Deny",
```

```
"Action": [  
    "glacier:DeleteArchive",  
    "glacier:DeleteVault"  
],  
"Resource": "*" ]}
```

SCP-AMS-023 : 防止删除 IAM 访问分析器

防止删除 IAM 访问分析器。

```
{  
  "Action": [  
    "access-analyzer:DeleteAnalyzer"  
  ],  
  "Resource": "*",  
  "Effect": "Deny"  
}
```

SCP-AMS-024 : 防止对 Security Hub 进行修改

防止删除 AWS Security Hub CSPM。

```
{  
  "Action": [  
    "securityhub:DeleteInvitations",  
    "securityhub:DisableSecurityHub",  
    "securityhub:DisassociateFromMasterAccount",  
    "securityhub:DeleteMembers",  
    "securityhub:DisassociateMembers"  
  ],  
  "Resource": "*",  
  "Effect": "Deny"  
}
```

SCP-AMS-025 : 防止在 Directory Service 下删除

防止删除下的资源 Directory Service。

```
{  
  "Action": [  
    "ds:DeleteDirectory",  
    "ds:DeleteUser"
```



```

    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",
    "ds:DisableLDAPS",
    "ds:DisableRadius",
    "ds:DisableSso",
    "ds:UnshareDirectory"
  ],
  "Resource": "*",
  "Effect": "Deny"
}

```

SCP-AMS-026：禁止使用列入拒绝名单的服务

防止使用被拒绝名单的服务。

Note

*service2*用您的服务名称替换*service1*和。示例*access-analyzer*或*IAM*。

```

{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:", "service2:"]
}

```

SCP-AMS-027：禁止在特定地区使用被拒绝名单的服务

禁止在特定 AWS 地区使用被拒绝名单的服务。

Note

*service2*用您的服务名称替换*service1*和。示例*access-analyzer*或*IAM*。
*region2*用您的服务名称替换*region1*和。示例*us-west-2*或*use-east-1*。

```

{
  "Effect": "Deny",

```

```

"Resource": "*",
"Action": ["service1:", "service2:"],
"Condition": {
  "StringEquals": {
    "aws:RequestedRegion": [
      "region1",
      "region2"
    ]
  }
}
}

```

SCP-AMS-028：禁止除授权委托人之外修改标签

防止除授权委托人之外的任何用户修改标签。使用授权标签对委托人进行授权。授权标签必须与资源和委托人关联。user/role 只有当资源和主体上的标签都匹配时，才会将A视为已授权。有关更多信息，请参阅以下资源：

- [使用中的服务控制策略保护用于授权的资源标签 AWS Organizations](#)
- [防止除授权委托人以外的其他人修改标签](#)

```

{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::ACCOUNT_ID:RESOURCE_TYPE/RESOURCE_NAME"
    },
    "Null": {
      "ec2:ResourceTag/access-project": false
    }
  }
},
{
  "Effect": "Deny",

```

```

"Action": [
  "ec2:CreateTags",
  "ec2:DeleteTags"
],
"Resource": [
  "*"
],
"Condition": {
  "StringNotEquals": {
    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
    "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
  },
  "ForAnyValue:StringEquals": {
    "aws:TagKeys": [
      "access-project"
    ]
  }
}
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalArn": "arn:aws:iam::${ACCOUNT_ID}:${RESOURCE_TYPE}/${RESOURCE_NAME}"
    },
    "Null": {
      "aws:PrincipalTag/access-project": true
    }
  }
}
}

```

SCP-AMS-029：防止用户删除亚马逊 VPC 流日志

防止删除 Amazon VPC 流日志。

```

{
  "Action": [

```

```

    "ec2:DeleteFlowLogs",
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:PutLifecycleConfiguration",
    "firehose:DeleteDeliveryStream"
  ],
  "Resource": "*",
  "Effect": "Deny"
}

```

SCP-AMS-030：防止与网络账户以外的账户共享 VPC 子网

防止与网络账户以外的账户共享 Amazon VPC 子网。

Note

NETWORK_ACCOUNT_ID 替换为您的网络账户 ID。

```

{
  "Effect": "Deny",
  "Action": [
    "ram:AssociateResourceShare",
    "ram:CreateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "ram:Principal": "NETWORK_ACCOUNT_ID"
    },
    "StringEquals": {
      "ram:RequestedResourceType": "ec2:Subnet"
    }
  }
}

```

SCP-AMS-031：防止启动具有违禁实例类型的实例

防止启动禁止的 Amazon EC2 实例类型。

Note

将`instance_type1`和`instance_type2`替换为要限制的实例类型，例如`t2.micro`或通配符字符串，例如。`*.nano`

```
{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}
```

SCP-AMS-032：防止在没有的情况下启动实例 IMDSv2

防止不 EC2 使用亚马逊实例 IMDSv2。

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
```

```

    "NumericGreaterThan": {
      "ec2:MetadataHttpPutResponseHopLimit": "3"
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*"
  }
]

```

SCP-AMS-033 : 防止修改特定 IAM 角色

防止修改指定的 IAM 角色。

```

{
  "Action": [
    "iam:AttachRolePolicy",
    "iam>DeleteRole",
    "iam>DeleteRolePermissionsBoundary",
    "iam>DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:UntagRole",
    "iam:UpdateAssumeRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
}

```

```
"Effect": "Deny"
}
```

SCP-AMS-034 : 防止 AssumeRolePolicy 修改特定 IAM 角色

防止修改指定 AssumeRolePolicy IAM 角色的。

```
{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
    "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}
```

ConfigRule: 必填标签

检查 EC2 实例是否具有您所需的自定义标签。此外 InfoSec，这对您的成本管理也很有用

```
ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the required tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
  SourceIdentifier: REQUIRED_TAGS
```

ConfigRule: 访问密钥已轮换

检查访问密钥是否在指定的时间段内轮换。根据典型的合规性要求，通常将其设置为 90 天。

```
ConfigRuleName: access-keys-rotated
Description: >-
  A config rule that checks whether the active access keys are rotated
  within the number of days specified in maxAccessKeyAge. The rule is
  NON_COMPLIANT if the access keys have not been rotated for more than
```

```
maxAccessKeyAge number of days.  
InputParameters:  
  maxAccessKeyAge: '90'  
Source:  
  Owner: AWS  
  SourceIdentifier: ACCESS_KEYS_ROTATED  
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: AMS 中的 IAM 根访问密钥

检查账户上是否没有根访问密钥。对于 AMS 高级账户，这应该是合规的 out-of-the-box。

```
ConfigRuleName: iam-root-access-key-check  
Description: >-  
  A config rule that checks whether the root user access key is available. The  
  rule is COMPLIANT if the user access key does not exist.  
Source:  
  Owner: AWS  
  SourceIdentifier: IAM_ROOT_ACCESS_KEY_CHECK  
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: SSM 托管 EC2

检查您的系统 EC2s 是否由 SSM Systems Manager 管理。

```
ConfigRuleName: ec2-instance-managed-by-systems-manager  
Description: >-  
  A Config rule that checks whether the EC2 instances in the  
  account are managed by AWS Systems Manager.  
Scope:  
  ComplianceResourceTypes:  
    - 'AWS::EC2::Instance'  
    - 'AWS::SSM::ManagedInstanceInventory'  
Source:  
  Owner: AWS  
  SourceIdentifier: EC2_INSTANCE_MANAGED_BY_SSM
```

ConfigRule: AMS 中未使用的 IAM 用户

检查是否有在指定持续时间内未使用的 IAM 用户证书。与密钥轮换检查一样，根据典型的合规性要求，这通常默认为 90 天。

```
ConfigRuleName: iam-user-unused-credentials-check
```



```
Description: >-
  A config rule that checks whether IAM users have passwords
  or active access keys that have not been used within the
  specified number of days provided.
InputParameters:
  maxCredentialUsageAge: '90'
Source:
  Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: S3 存储桶日志

检查账户中的 S3 存储桶是否已启用日志记录。

```
ConfigRuleName: s3-bucket-logging-enabled
Description: >-
  A Config rule that checks whether logging is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_LOGGING_ENABLED
```

ConfigRule: S3 存储桶版本控制

检查所有 S3 存储桶上是否启用了版本控制和 mfa-Delete (可选)

```
ConfigRuleName: s3-bucket-versioning-enabled
Description: >-
  A Config rule that checks whether versioning is enabled for S3
  buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::Bucket'
Source:
  Owner: AWS
SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED
```

ConfigRule: S3 公共访问权限

检查账户中的公共访问设置 (公共 ACL、公共策略、公共存储桶) 是否受到限制

```
ConfigRuleName: s3-account-level-public-access-blocks
Description: >-
  A Config rule that checks whether the required public access block
  settings are configured from account level. The rule is only
  NON_COMPLIANT when the fields set below do not match the corresponding
  fields in the configuration item.
Scope:
  ComplianceResourceTypes:
    - 'AWS::S3::AccountPublicAccessBlock'
InputParameters:
  IgnorePublicAcls: 'True'
  BlockPublicPolicy: 'True'
  BlockPublicAcls: 'True'
  RestrictPublicBuckets: 'True'
Source:
  Owner: AWS
SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
```

ConfigRule: 未存档 GuardDuty 的调查结果

检查是否存在超过指定持续时间的未存档搜索 GuardDuty 结果。低sev的默认持续时间为30天，中sev的默认持续时间为7天，高sev发现的默认持续时间为1天。

```
ConfigRuleName: guardduty-non-archived-findings
Description: >-
  A Config rule that checks whether the Amazon GuardDuty has findings that
  are non archived. The rule is NON_COMPLIANT if GuardDuty has non
  archived low/medium/high severity findings older than the specified number.
InputParameters:
  daysLowSev: '30'
  daysMediumSev: '7'
  daysHighSev: '1'
Source:
  Owner: AWS
  SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: 已删除 CMK

检查是否有计划删除 (又名待处理CMKs) 的 AWS Key Management Service 自定义主密钥 ()。这一点至关重要，因为对删除 CMK 一无所知会导致数据无法恢复

```
ConfigRuleName: kms-cmk-not-scheduled-for-deletion
Description: >-
  A config rule that checks whether customer master keys (CMKs) are not
  scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is
  NON_COMPLIANT if CMKs are scheduled for deletion.
Source:
  Owner: AWS
SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION
MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: 密钥轮换

检查账户中的每个 CMK 是否启用了自动轮换

```
ConfigRuleName: cmk-backing-key-rotation-enabled
Description: >-
  A config rule that checks that key rotation is enabled for each customer
  master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
  for specific key object. The rule is not applicable to CMKs that have
  imported key material.
Source:
  Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
MaximumExecutionFrequency: TwentyFour_Hours
```

Config 规则的自定义通知

可能会出现严重的不合规的 Config 规则，需要 InfoSec 您和领导团队直接提高认识。对于此类情况，AMS 建议您配置不合规事件驱动的自定义通知。

例如：

```
ConfigRuleName: required-tags
Description: >-
  A Config rule that checks whether EC2 instances have the mandated tags.
Scope:
  ComplianceResourceTypes:
    - 'AWS::EC2::Instance'
InputParameters:
  tag1Key: COST_CENTER
  tag2Key: APP_ID
Source:
  Owner: AWS
```

```
SourceIdentifier: REQUIRED_TAGS
NotificationEventRule:
  Type: 'AWS::Events::Rule'
  Properties:
    Name: CWEventForrequired-tags
    Description: >-
      SNS Notification for Non-Compliant Events of Config Rule:
      required-tags
    State: ENABLED
    EventPattern:
      detail-type:
        - Config Rules Compliance Change
      source:
        - aws.config
      detail:
        newEvaluationResult:
          complianceType:
            - NON_COMPLIANT
        configRuleARN:
          - 'Fn::GetAtt':
              - RequiredEC2Tags
              - Arn
    Targets:
      - Id: RemediationNotification
        Arn:
          Ref: SnsTopic
        InputTransformer:
          InputTemplate: >-
            "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
            COST_CENTER, APP_ID, Name, and Backup."
          InputPathsMap:
            instance_id: $.detail.resourceId
  SnsTopic:
    Type: 'AWS::SNS::Topic'
    Properties:
      Subscription:
        - Endpoint: Cloud_Ops_Leaders@customer.com
          Protocol: email
      TopicName: noncompliant-instance-notification
  SnsTopicPolicy:
    Type: 'AWS::SNS::TopicPolicy'
    Properties:
      PolicyDocument:
        Statement:
```

```

- Sid: __default_statement_ID
  Effect: Allow
  Principal:
    AWS: '*'
  Action:
    - 'SNS:GetTopicAttributes'
    - 'SNS:SetTopicAttributes'
    - 'SNS:AddPermission'
    - 'SNS:RemovePermission'
    - 'SNS:DeleteTopic'
    - 'SNS:Subscribe'
    - 'SNS:ListSubscriptionsByTopic'
    - 'SNS:Publish'
    - 'SNS:Receive'
  Resource:
    Ref: SnsTopic
  Condition:
    StringEquals:
      'AWS:SourceOwner':
        Ref: 'AWS::AccountId'
- Sid: TrustCWEToPublishEventsToMyTopic
  Effect: Allow
  Principal:
    Service: events.amazonaws.com
  Action: 'sns:Publish'
  Resource:
    Ref: SnsTopic
Topics:
  - Ref: SnsTopic

```

适用于 AMS 高级版的 Amazon EventBridge 规则服务相关角色

AMS Advanced 使用名为的服务相关角色 (SLR) `AWSServiceRoleForManagedServices_Events`— 此角色信任其中一位 AWS 托管服务委托人 (`events.managedservices.amazonaws.com`) 代您担任该角色。该服务使用该角色来创建 EventBridge 托管规则。此规则是您的账户中将警报状态更改信息从您的 AWS 账户传送到 Managed Services 所需的基础架构。 AWS

AMS 高级 EventBridge 版单反相机的权限

`AWSServiceRoleForManagedServices_Events` 服务相关角色信任以下服务代入该角色：

- `events.managedservices.com`

该角色附带的是 `AWSManagedServices_EventsServiceRolePolicy` AWS 托管策略 (参见 [AWS 托管策略: `AWSManagedServices\_EventsServiceRolePolicy`](#)) 。该服务使用该角色将警报状态更改信息从您的账户传送到 Managed Services。您必须配置权限，允许 IAM 实体 (如用户、组或角色) 创建、编辑或删除服务相关角色。有关更多信息，请参阅 AWS Identity and Access Management 用户指南中的 [服务相关角色权限](#)。

您可以下载这个压缩文件 `AWSManagedServices_EventsServiceRolePolicy` 中的 JSON : [EventsServiceRolePolicy.zip](#)。

为 AMS Advanced EventBridge 创建单反相机

您无需手动创建服务相关角色。当您在 AWS 管理控制台、或 AWS API 中加入 AMS 时 AWS CLI，AMS Advanced 会为您创建服务相关角色。

Important

如果您在 2023 年 2 月 7 日之前使用 AMS Advanced 服务，则该服务相关角色可以出现在您的账户中，AMS Advanced 服务开始支持服务相关角色，然后 AMS Accelerate 在您的账户中创建了该 `AWSServiceRoleForManagedServices_Events` 角色。要了解更多信息，请参阅[我的 IAM 账户中出现新角色](#)。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您加入 AMS 时，AMS Advanced 会再次为您创建与服务相关的角色。

为 AMS Advanced EventBridge 编辑单反相机

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

删除 AMS EventBridge 高级版单反相机

无需手动删除 `AWSServiceRoleForManagedServices_Events` 角色。当您在 AWS 管理控制台、AWS CLI 或 AWS API 中退出 AMS 时，AMS Advanced 会清理资源并为您删除服务相关角色。

您也可以使用 IAM 控制台、AWS CLI 或 AWS API 手动删除服务相关角色。为此，必须先手动清除服务相关角色的资源，然后才能手动删除。

Note

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

删除 AWSServiceRoleForManagedServices_Events 服务相关角色使用的 AMS 高级资源

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForManagedServices_Events 服务相关角色。

有关更多信息，请参阅《IAM 用户指南》中的[删除服务相关角色](#)。

安全最佳实践

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。

AMS 多账号 landing zone EPS 非默认设置

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。

AMS 护栏

护栏是一项高级规则，可为您的整个 AMS 环境提供持续治理。

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。

MALZ 服务控制策略

此部分已被删除，因为它包含与 AMS 安全相关的敏感信息。此信息可通过 AMS 控制台文档获得。要访问 AWS Artifact，您可以联系您的 CSDM [获取说明或前往 AWS Artifact 入门](#)。

AMS 中的安全事件响应

安全是 AWS Managed Services (AMS) 的重中之重。AMS 在您的账户中部署资源和控制来对其进行管理。AWS 有一个责任共担模式：AWS 管理云的安全，你负责云中的安全。AMS 通过使用安全控制

和主动监控安全问题，保护您的数据和资产，并帮助确保您的 AWS 基础设施安全。这些功能可帮助您为在 AWS 云中运行的应用程序建立安全基准。AMS 通过安全事件响应与您合作，评估其影响，然后根据最佳实践建议进行遏制和补救。

当出现偏离基线的情况（例如配置错误或外部因素的变化）时，您需要做出回应并进行调查。要成功做到这一点，您需要了解 AMS 环境中安全事件响应的基本概念。您还必须了解在安全问题发生之前做好准备、教育和培训云团队的要求。重要的是要了解您可以使用的控制和功能，针对常见的安全问题（例如用户帐户受损或滥用特权帐户）制定应对计划，并确定使用自动化来提高响应速度和一致性的补救方法。此外，您需要了解您的合规和监管要求，因为它们与制定安全事件响应计划以满足这些要求有关。

安全事件响应可能很复杂，但是通过实施迭代方法，您可以简化流程，并允许事件响应团队通过提供早期和持续的检测和响应来让资产利益相关者满意。在本指南中，我们向您提供 AMS 用于事件响应的方法、AMS 责任矩阵 (RACI)、如何为安全事件做好准备、如何在安全事件期间与 AMS 接触，以及 AMS 使用的一些事件响应操作手册。

AMS 安全事件响应的工作原理

AWS Managed Services 与 NIST 800-61 [安全事件响应计算机安全事件处理指南](#)保持一致。通过与该行业标准保持一致，我们提供了一种一致的安全事件管理方法，并遵守保护和响应云端安全事件的最佳实践。

事件响应生命周期

当检测发现并生成安全警报，或者您请求安全帮助时，AWS Managed Services Operations 团队会确保及时进行调查，自动执行数据收集、分类和分析，通知您分析情况，执行调查和任何遏制活动，然后发布事件分析。

事件响应期间执行的数据收集、分类、分析和遏制活动因所调查的安全事件的类型而异。本文档末尾列出了特定场景的安全事件响应工作流程示例。

在事故发生期间，AMS 会动态确定正确的行动方案，这可能会导致对记录在案的步骤进行重新排序或酌情绕过，以确保产生正确的结果。

准备

随着威胁形势的演变，AMS 继续扩大检测和响应能力。随着新检测的增加，AMS 会将这些新检测产生的警报整合到检测和响应平台中。AMS 安全响应人员经过培训，可以在整个安全事件响应生命周期中进行调查并与您合作。

由于这种合作方式，您的安全和应用团队必须做好与 AMS 合作的准备，以便在这些事件发生时处理这些事件，这一点非常重要。本文档解释了安全事件期间的预期，并帮助您为安全事件发生时的快速响应做好准备。

本文档使用 NIST 800-61 的定义，将事件定义为系统或网络中任何可观察到的事件，将事件定义为违反政策、可接受使用策略或标准安全实践的违规行为或迫在眉睫的威胁。

准备清单

与您的 AMS 云解决方案交付经理 (CSDM) 和 AMS 云架构师 (CA) 一起完成以下清单：

- 了解哪些工作负载在哪些账户中运行。
- 了解哪些内部团队负责各种工作负载，并在工作负载中对其进行适当标记。
- 在内部保留在安全事件调查和控制决策期间可能需要的其他团队的联系方式。
- 确认安全联系人是最新的，并已添加到所有托管 AWS 账户。联系人按账户进行管理。
- 知道如何向 AMS 举报安全事件，并熟悉严重程度和预期的响应时间。
- 确保在收到安全通知时，将它们发送给相应的人员和系统，例如寻呼机或您的安全运营中心。
- 了解哪些日志源可供您使用，这些日志源存储在您的账户中的位置以及谁有权访问它们。
- 了解如何在调查期间使用 CloudWatch Insights 查询日志。
- 了解按资源（EC2、IAM、S3 等）可供您使用的控制选项，以及处于控制状态时对工作负载可用性的影响。

Detect

在管理您的 AWS 账户期间，AMS 会使用从检测来源和控件（包括但不限于亚马逊、亚马逊、GuardDuty VPC 流日志、Amazon Macie 和 CloudWatch 亚马逊内部威胁情报源）收集的数据来监控用户行为、账户活动 AWS Config 和潜在安全事件中的异常情况。

AMS 使用原生 AWS 服务和其他检测技术来响应由以下原因创建的安全事件：

- Config 一致性查找类型
- GuardDuty 查找类型
- Macie 查找类型
- 亚马逊 Route 53 解析器 DNS 防火墙事件
- AMS 安全事件（云监视警报）

随着服务、产品和威胁生态系统的发展，还增加了其他发现。

向 AMS 报告安全事件

通过 AMS Support 门户或 支持 中心举报事件，向 AMS 通报安全事件或请求调查。

分析

识别并报告安全事件后，下一步是分析报告的事件是误报事件还是真实事件。AMS 使用自动化和手动调查技术来处理安全事件。分析包括调查来自不同检测源的日志，例如网络流量日志、主机日志、CloudTrail 事件、AWS 服务日志等。该分析还通过相关性寻找显示异常行为的模式。

您的合作伙伴关系需要了解特定于账户环境的背景，并确定您的账户和工作负载的正常情况。这有助于 AMS 更快地识别异常并加快事件响应。

处理来自 AMS 的有关安全事件的通信

在调查期间，AMS 会通过事件单与您的安全联系人联系，随时向您通报情况。在主动安全调查期间，您的 AMS 云服务交付经理 (CSDM) 和 AMS 云架构师 (CA) 是联系人，可以联系他们进行任何沟通。

通信包括在生成安全警报时自动通知、事件分析后进行通信、建立呼叫桥接以及持续交付项目（例如日志文件、受感染资源的快照），以及在安全事件期间向您提供调查结果。

AMS 安全警报通知中包含的标准字段如下所示。这些字段为您提供信息，以便您可以将事件发送给组织内的相应团队进行补救。

- 查找类型
- 查找标识符（如果相关）
- 查找严重性
- 查找描述
- 查找创建日期和时间
- AWS 账户编号
- 区域（如果相关）
- AWS 资源（IAM user/role/policy、EC2、S3、EKS）

根据查找结果类型，还会提供其他字段，例如，EKS Finding 包括 Pod、容器和集群详细信息。

遏制

AMS 的遏制方法是与您合作。您了解您的业务以及遏制活动可能对工作负载产生的影响，例如网络隔离、IAM 用户或角色取消预配、实例重建等。

遏制的一个重要部分是决策。例如，关闭系统、将资源与网络隔离开来，或者关闭访问或结束会话。如果有预先确定的策略和程序来遏制事件，则更容易做出这些决定。AMS 提供遏制策略，然后在您考虑实施遏制措施所涉及的风险后实施解决方案。

根据所分析的资源，有不同的控制选项。AMS 预计，在事故调查期间，将同时部署多种类型的遏制措施。其中一些例子包括：

- 应用保护规则来阻止未经授权的流量（安全组、NACL、WAF 规则、SCP 规则、拒绝列出、将签名操作设置为隔离或阻止）
- 资源隔离
- 网络隔离
- 禁用 IAM 用户、角色和策略
- 修改/减少 IAM 用户、角色权限
- 终止/暂停/删除计算资源
- 限制公众访问受影响资源
- 轮换访问密钥、API 密钥和密码
- 清理披露的凭据和敏感信息

AMS 鼓励您考虑风险偏好范围内的每种重大事件类型的遏制策略类型，并明确记录标准，以帮助在发生事件时做出决策。确定适当策略的标准包括：

- 资源潜在损害程度
- 保存证据
- 服务不可用性（如网络连接、向外部提供的服务）
- 实施策略所需的时间与资源
- 策略的有效性（例如，部分遏制、完全遏制）
- 解决方案的永久性（例如，单向门与双向门的决策）
- 解决方案的持续时间（例如，紧急变通方案将在四小时内删除，临时变通方案将在两周内删除，永久解决方案）。
- 应用您可以开启的安全控制措施来降低风险，并留出时间来定义和实施更有效的遏制措施。

遏制速度至关重要，AMS建议采取分阶段的方法，通过制定短期和长期方法来实现高效和有效的遏制。

使用本指南来考虑您的遏制策略，该策略涉及基于资源类型的不同技术。

- 遏制策略
 - AMS 能否确定安全事件的范围？
 - 是：标记所有相关资源（用户、系统、资源）。
 - 否：对已识别资源执行下一步，同时继续调查。
 - 资源是否能被隔离？
 - 是：立即隔离受影响资源。
 - 否：协同系统负责人确定替代遏制方案。
 - 所有受影响的资源是否都已与未受影响的资源隔离开来？
 - 是：进入下一阶段。
 - 如果不是，则继续隔离受影响的资源，直到完成短期遏制，以防止事件进一步升级。
- 系统备份
 - 是否已创建受影响系统备份用于分析？
 - 取证副本是否已加密并安全存储？
 - 是：进入下一阶段。
 - 否：立即加密取证映像并安全存储，防止意外使用、损坏或篡改。

根除

事件得到控制后，在进入下一个恢复阶段之前，可能需要根除威胁以完全消除威胁源，从而保护系统。根除步骤可能包括删除恶意软件和移除受感染的用户帐户，以及识别和缓解所有被利用的漏洞。在根除期间，重要的是要识别环境中所有受影响的账户、资源和实例，以便对其进行补救。

最佳做法是分阶段进行根除和恢复，以便确定补救措施的优先顺序。对于大规模事件，恢复可能需要几个月的时间。早期阶段的目的必须是通过相对较快（几天到几周）的高价值更改来提高整体安全性，以防止将来发生事件。后期阶段必须侧重于长期变革（例如基础架构变更）和持续的工作，以尽可能确保企业的安全。

对于某些事件，要么没有必要，要么在恢复期间进行消除。

请考虑以下事项：

- 能否对系统进行重新映像，然后通过补丁或其他对策进行强化以防止或降低攻击风险？
- 攻击者留下的所有恶意软件和其他工件是否都被清除，受影响的系统是否已得到加强，可以抵御进一步的攻击？

恢复

AMS 与您合作，将系统恢复到正常运行，确认系统运行正常，并（如适用）修复漏洞以防止发生类似事件。

请考虑以下事项：

- 受影响的系统是否经过修补和强化，可以抵御最近的攻击和未来可能的攻击？
- 哪一天和什么时间可以将受影响的系统恢复到生产状态？
- 您将使用哪些工具来测试、监控和验证恢复到生产环境的系统是否不容易受到初始攻击技术的攻击？

事故后报告

事件发生后，AMS 会对所有安全事件进行调查审查。而且，AMS 启动了错误更正 (COE) 流程，以解决由系统或程序失误引起的安全事件，这些事件可能还有改进余地。AMS 与您合作，不断改善安全调查体验。COE 流程可帮助 AMS 识别影响客户的事件的促成因素，并将这些原因与下一步的行动项目联系起来，这些项目可以防止类似事件再次发生，或者有助于缓解影响的持续时间或程度。

安全事件调查审查流程涉及以下事项，以确定改进机会：

- 从事件开始到事件发现，到最初的影响评估，再到事件处理过程的每个阶段（例如遏制、恢复），经过了多长时间？
- 事件响应小组花了多长时间才对事件的初步报告做出回应？
- 进行初步影响分析花了多长时间？
- 这是可以预防的吗？如何预防？有没有可以阻止这种情况的工具或流程？
- 我们能早点发现吗？如何发现？
- 什么能让调查更快地进行？
- 是否遵循了记录在案的事故响应程序？它们足够吗？
- 与其他利益相关者的信息共享是否及时？如何加以改进？
- 与其他团队（AWS 安全、客户团队、AWS 开发团队和客户安全团队）的合作是否有效？如果不是，还有什么可以改进的地方？

- 缺少了哪些可能有所帮助的准备步骤，升级矩阵、RACI、分担责任模型等等？是否需要更新任何 Runbook？
- 初步影响评估和最终影响评估有什么区别？在事件响应的早期阶段，我们可以做些什么来提高评估的准确性？
- 经验教训中的行动项目有哪些？

AMS 中的安全事件响应操作手册

本节包含两个运行手册：

- [对 root 用户活动的响应](#)
- [对恶意软件事件的响应](#)

对 root 用户活动的响应

[root 用户](#)是您 AWS 账户中的超级用户。请注意，AMS 会监控根用户使用情况。最佳做法是仅将根用户用于少数需要它的任务，例如更改账户设置、激活 AWS Identity and Access Management (IAM) 账单和成本管理权限、更改根密码以及开启多重身份验证 (MFA)。有关更多信息，请参阅[需要 root 用户凭据的任务](#)。

有关如何通知 AMS 计划的 root 用户使用情况的更多信息，请参阅[何时以及如何在 AMS 中使用根账户](#)。

当检测到 root 用户活动时，无论是登录尝试失败（可能表示暴力攻击）或成功登录后账户中的活动，都会生成一个事件并将事件发送给您定义的安全联系人。

AWS Managed Services Operations 调查计划外的根用户活动，执行数据收集、分类和分析，并按照您的指示执行遏制活动，然后进行事件后分析。

如果您使用的是 AMS Advanced 操作模式，则会收到来自 AMS CSDM 和 AMS Ops 工程师的额外通信，这些通信确认了由于 AMS 有责任保护根用户凭证而导致的计划外根用户活动。AMS 会调查 root 用户活动，直到您确认前进方向。

准备

通过提交 AMS 服务请求，告知 AMS 计划使用 root 用户的情况，包括计划中的事件的数据和时间，以防止不必要的事件响应活动。

定期 GameDays 与 AMS 合作，验证 AMS 的客户事件响应流程、人员和系统是否处于最新状态，并与负责的个人建立肌肉记忆，以实现更快的事件响应。

阶段 A：检测

AMS 通过检测源（包括 GuardDuty AMS 监控）来监控账户中的根用户活动。

如果您有 AMS Accelerate，则操作模型会对请求对意外根用户活动进行调查的事件做出响应。发生这种情况时，AMS 运营部门会启动被盗账户操作手册。

如果您有 AMS Advanced，则运营模式会对事件做出响应，或者将 root 用户的任何计划活动通知给 CSDM，以终止正在进行的账户泄露调查。

B 阶段：分析

当确定根用户事件未获得授权时，AMS 会对该活动进行彻底调查。使用自动化和 AMS 安全响应团队，对日志和事件进行分析，以确定根用户的异常和意外行为。向您提供日志是为了帮助您确定活动是否未知、是否是授权的 root 用户事件，或者是否需要进一步调查。

调查期间为支持内部检查而提供的信息的一些示例包括：

- 账户信息：root 账户用于哪个账户？
- root 用户的电子邮件地址：每个 root 用户都与贵组织中的一个电子邮件地址相关联
- 身份验证详情：root 用户从何时何地访问您的环境？
- 活动记录：用户以 root 身份登录后做了什么？这些记录以 CloudWatch 事件的形式出现。了解如何阅读这些日志有助于调查。

最佳做法是准备好接收分析信息，并计划如何联系组织内客户的授权联系人。由于 root 用户不是以个人身份命名的，因此确定谁有权访问组织内用于该帐户的根电子邮件地址有助于在内部快速传递问题。

C 阶段：遏制和消灭

AMS 与您的安全团队合作，在您授权的客户安全联系人的指导下进行遏制。密封选项包括：

- 轮换适当的凭证和密钥。
- 终止与账户和资源的活动会话。
- 清除已创建的资源。

在控制活动期间，AMS 会与您的安全团队密切合作，确保最大限度地减少对您的工作负载的任何干扰，并适当保护根凭证。

控制计划完成后，您可以根据需要与 AMS 运营团队合作采取任何恢复行动。

事故后报告

根据要求，AMS 启动调查审查流程，以确定任何经验教训。作为完成 COE 的一部分，AMS 会将所有相关发现传达给受影响的客户，以帮助他们改善事件响应流程。

AMS 记录调查的所有最终细节，收集适当的指标，然后将事件报告给任何需要信息的 AMS 内部团队，包括您分配的 CSDM 和 CA。

对恶意软件事件的响应

Amazon EC2 实例用于托管各种工作负载，包括由组织内部应用程序团队部署的第三方软件和定制开发的软件。AMS 提供并鼓励您在由 AMS 持续修补和维护的映像上部署工作负载。

在实例运行期间，AMS 通过各种安全检测控件（包括 Amazon、Endpoint Protection、网络流量和亚马逊 GuardDuty 内部威胁情报源）来监控行为或活动中的异常情况。

采用 AMS Advanced 操作模式的 AMS 客户会自动在已配置的资源上安装端点安全 (EPS) 监控客户端。这样可以确保资源得到全天候监控和支持，包括在检测到事件时制造安全事件。

AMS 还会监控 GuardDuty 恶意软件发现。如果启用，它们在 AMS Advanced 和 AMS Accelerate 上都可用。有关更多信息，请参阅 [Amazon GuardDuty 中的恶意软件防护](#)。

Note

如果您选择了 [Bring Your Own EPS](#)，则事件响应的流程与本页上概述的流程不同。有关更多信息，请参阅参考文档。

当检测到恶意软件时，就会创建事件并向您通知该事件。在此通知之后，将显示已发生的任何补救活动。AMS Operations 负责调查、执行数据收集、分类和分析，然后按照您的指示执行遏制活动，然后进行事后分析。

阶段 A：检测

AMS 通过端点安全解决方案监控 GuardDuty 和端点安全解决方案监控实例上的事件。AMS 确定适当的浓缩和分类活动，以帮助您根据发现或警报类型做出遏制或风险接受决策。

数据收集是根据发现类型进行的。数据收集涉及查询受影响账户内部和外部的多个数据源，以了解观察到的活动或关注的配置。

AMS 将发现结果与来自任何受影响账户或 AMS 威胁情报平台的任何其他警报和警报或遥测数据进行关联。

B 阶段：分析

收集数据后，对其进行分析以确定任何活动或令人担忧的指标。在调查的这一阶段，AMS 将与您合作，整合实例和工作负载的业务和领域知识，以帮助了解预期情况和异常情况。

调查期间为支持内部检查而提供的信息的一些示例包括：

- 账户信息：在哪个账户上观察到恶意软件活动？
- 实例详情：哪些实例与恶意软件事件有关？
- 事件时间戳：警报是什么时候触发的？
- 工作负载信息：实例上正在运行什么？
- 恶意软件详细信息（如果相关）：恶意软件系列和有关恶意软件的开源信息。
- 用户或角色详情：哪些用户或角色受活动影响并参与其中？
- 活动记录：实例上记录了哪些活动？它们以 CloudWatch 事件和来自实例的系统事件的形式出现。了解如何阅读这些日志将有助于您进行调查
- 网络活动：哪些终端节点正在连接到实例，实例正在连接什么，以及流量分析是什么？

最佳做法是做好接收调查信息的准备，并就如何联系组织内的客户、实例和工作负载的相应联系人制定计划。了解您的网络拓扑和预期的连接有助于加快影响分析。了解环境中计划的渗透测试以及应用程序所有者最近执行的部署也可以加快调查速度。

如果您确定该活动已计划并已获得授权，则会更新事件并结束调查。如果确认妥协，则您和 AMS 将确定适当的控制计划。

C 阶段：遏制和消灭

AMS 与您合作，根据收集的数据和已知信息确定适当的遏制活动。封闭选项包括但不限于：

- 通过快照保留数据
- 修改网络规则以限制进出实例的流量
- 修改 SCP、IAM 用户和角色策略以限制访问权限
- 终止、暂停或关闭实例
- 终止所有持久连接
- 轮换适当的凭据/密钥

如果您选择对实例执行清除活动，那么 AMS 将支持您实现这一目标。选项包括但不限于：

- 正在删除所有不需要的软件
- 从干净的完全修补的映像重建实例，然后重新部署应用程序和配置
- 从之前的备份中恢复实例
- 将应用程序和服务部署到您账户中可能适合托管工作负载的另一个实例。

在恢复服务之前，必须确定恶意软件是如何传递和在实例上运行的，以确保应用任何其他控制措施来防止恶意软件在实例上再次出现。AMS 根据需要向您的取证合作伙伴或团队提供其他见解或信息，以支持取证。

此时，您将与 AMS 运营部门合作开展恢复活动。AMS 与您密切合作，以最大限度地减少对工作负载的干扰并保护实例。

事故后报告

根据要求，AMS 启动调查审查流程，以总结经验教训。作为完成 COE 的一部分，AMS 会向您传达相关调查结果，以帮助您改进事件响应流程。

AMS 记录调查的最终细节，收集适当的指标，并将事件报告给 AMS 内部团队，这些团队需要信息，包括您分配的 CSDM 和 CA。

在 AMS Advanced 中更改请求安全审查

AWS Managed Services 变更请求审核流程可确保 AMS 在您的账户中代表您实施变更时对请求的更改进行安全审查。

[AMS 高级技术标准](#)定义最低安全标准、配置和流程，以建立账户的基本安全性。当 AMS 实施所要求的变更时，我们会遵循这些标准。

AMS 根据 AMS 技术标准评估所有变更请求。任何可能因偏离技术标准而降低账户安全状况的变更都要经过安全审查流程。在此过程中，AMS 会强调相关风险，并由您的授权风险审批人进行审查和批准，以平衡安全和业务需求。

客户安全风险管理体系

AMS 高级客户安全风险管理体系 (CSRM) 流程有助于清楚地识别风险并将其传达给合适的所有者。此过程可最大限度地降低您环境中的安全风险，并减少已识别风险的持续运营开销。

默认情况下，当贵组织中的某人请求 AMS 对您的托管环境进行更改时，AMS 会审查更改以确定该请求是否超出了技术标准，这可能会改变您账户的安全状况。如果存在高或非常高的安全风险，则您的授权安全人员会接受或拒绝变更审查。还会评估所要求的变更是否会对AMS的账户运营能力产生不利影响。如果审查发现可能的不利影响，则需要在AMS内部进行额外的审查和批准。

对于高风险或非常高的风险，您可以选择退出 CSRM 流程中基于审批的工作流程。要将特定账户的 CSRM 选项从标准 CSRM 更改为“仅限通知”，请与您的云服务交付经理合作创建一次性风险承受单。如果您选择继续使用“仅限通知”选项，则无论风险类别如何，AMS 都会实施所请求的更改。而且，AMS 会向您的授权风险批准者发送风险通知，而不是在变更实施之前寻求批准。请咨询您的云架构师或云服务交付经理，了解有关 AMS CSRM 流程、如何在注册新 AMS 账户时更改默认 CSRM 选项或如何更新现有账户的更多信息。

 Note

AMS 强烈建议您在所有账户中使用默认的标准 CSRM 选项。

AMS 高级技术标准

以下是 AMS 高级技术标准类别：

ID	类别
AMS-STD-001	标记配置
AMS-STD-002	AWS Identity and Access Management
AMS-STD-003	网络安全性
AMS-STD-004	渗透测试
AMS-STD-005	Amazon GuardDuty
AMS-STD-006	主机安全
AMS-STD-007	日志系统
AMS-STD-008	AMS-MAD
AMS-STD-009	其他

AMS 高级版中的标准控件

以下是 AMS 中的标准控件：

AMS-STD-001-标记配置

以下是 001-标记配置的标准控件。

1. AMS 团队出于运营和管理目的所需的所有 AWS 资源都必须具有以下键值对。
 - AppId= AMSInfrastructure
 - 环境= AMSInfrastructure
 - AppName = AMSInfrastructure
 - AMSResource=没错
2. 除了先前列出的标签外，AMS 团队要求的所有标签都必须具有 AMS 前缀列表中提到的前缀（参见注意）。
3. AMS 团队（AppId、环境和 AppName）要求的标签值可以根据您的更改请求在您创建的任何资源上进行更改。
4. 不得根据您的更改请求删除 AMS 要求的堆栈上的任何标签。
5. 如第 2 点所述，您不能对基础设施使用 AMS 标签命名约定。
6. 您可以在 AMS 所需的资源中创建自定义标签（通常用于账单和成本报告用例）。如果资源是通过堆栈更新而不是通过更新模板来更新的，则会保留自定义标签。

Note

AMS 前缀列表

1. ams-*
2. AWSManaged服务*
3. /ams/ *
4. 上午*
5. 上午*
6. Ams*
7. mc*
8. MC*
9. 麦克*

10.哨兵*

11.哨兵*

12.托管服务*

13.Newams*

14.AWS_*

15.啊*

16.VPC_*

17.CloudTrail*

18.Cloudtrail *

19/aws_reserved/

20.摄取*

21.EPSDB*

22.MMS*

23.TemplateId*

24.StackSet-ams*

25.StackSet-AWS 着陆区

26.IAMPolicy*

27.客户-mc-*

28.根*

29.LandingZone*

30.StateMachine*

31.代码部署服务角色

32.管理主机

33.sentinel.int。

34.eps

35.UnhealthyInServiceBastion

36.ms-

AMS-STD-002- AWS Identity and Access Management (IAM)

ID	技术标准
1.0	超时持续时间
1.1	联邦用户的默认超时会话为一小时，最多可以增加至四小时。
1.2	默认堆栈访问时间为 12 小时。
2.0	AWS 主账号使用情况
2.1	如果出于任何原因使用了根账户，则 GuardDuty 必须将 Amazon 配置为生成相关调查结果。
2.2	对于单账户着陆区 (SALZ) 账户和多账户着陆区 (MALZ) 管理账户（以前称为账户），根用户 Master/Billing 账户必须启用虚拟 MFA，并且在账户注册期间丢弃 MFA 软令牌，这样 AMS 和客户都无法以 root 身份登录。必须与 AMS 云服务交付管理器 (CSDM) 一起执行标准的 AWS root 密码丢失流程。此配置必须在 AMS 托管账户的生命周期内保留。
2.3	您不得为 root 账户创建访问密钥。
3.0	用户创建和修改
3.1	无需任何时间限制策略即可创建 users/roles 具有编程访问权限和只读权限的 IAM。但是，不允许读取账户中所有 Amazon Simple Storage Service 存储桶中的对象（例如 S3:GetObject）的权限。
3.1.1	可以使用时间限制策略（最长 180 天）创建用于控制台访问和只读权限的 IAM 人类用户，而时间限制策略将生成风险通知。removal/renewal/extension但是，不允许读取账户中所有

ID	技术标准
	S3 存储桶中的对象（例如 S3:GetObject）的权限。
3.2	在不接受风险的情况下，不得在客户账户中创建具有任何基础架构变更权限（写入和权限管理）的 IAM 用户和用于控制台和编程访问的角色。S3 对象级写入权限存在例外情况，只要特定的存储桶在范围内，并且对非 AMS 相关标签进行标记操作，则无需接受风险即可使用这些权限。
3.3	无需任何时间限制政策，即可创建具有编程访问权限、已命名customer_servicenow_user 并customer_servicenow_logging_user 需要 ServiceNow 集成到 SALZ 或 MALZ 应用程序账户以及*核心账户*的 IAM 用户。
3.4	可以创建具有编程访问权限、在 SALZ customer_cloud_endure_policy 和 MALZ 账户中 CloudEndure 集成所需的和customer_cloud_endure_deny_policy（具有只读访问权限）的 IAM 用户，但需要在计划迁移期间制定有时间限制的策略。时间限制最长可为 180 天，无需任何 RA。SCP 还被授权更改MALZ账户，以允许这些政策在规定的期限内发挥作用。您可以根据需要定义适当的迁移窗口，并根据需要进行调整。
4.0	政策、行动和 APIs
4.1	您在 SALZ 账户中的所有 IAM 用户和角色都必须附加默认的客户拒绝政策 (CDP)，以保护 AMS 基础设施免受意外或故意损坏。
4.2	SCPs 必须在 MALZ 的所有 AMS 托管账户中启用 AMS。

ID	技术标准
4.3	能够对 KMS 密钥执行管理操作 (例如 PutKeyPolicy ScheduleKeyDeletion 、 和) 的身份必须仅限于 AMS 操作员和自动化主体。
4.4	在不接受风险的情况下，策略不得向管理员提供等同于“效果”：“允许”和“操作”：“*”而不是“资源”：“*”的语句。
4.5	IAM 策略不得包含任何包含在不接受风险的情况下对任何存储桶执行“允许 S3: ***”操作的操作。
4.6	不得允许针对客户 IAM 策略中的 AMS 基础设施密钥的 KMS 密钥策略进行 API 调用。
4.7	不得允许绕过变更管理流程 (RFC) 的操作，例如启动或停止实例、创建 S3 存储桶或 RDS 实例等。
4.8	不得允许对 Amazon Route 53 中的 AMS 基础设施 DNS 记录进行更改的操作。
4.9	按照正当程序创建的具有控制台访问权限的 IAM 人类用户，除了信任策略、代入角色和限时策略外，不得直接附加任何策略。
4.10	可以在同一账户中创建对特定密钥或命名空间具有读取 AWS Secrets Manager 权限的 Amazon EC2 实例配置文件。
4.11	可以将 AWS Managed Services 变更管理 (AMSCM) 或 AWS Managed Services 服务知识管理系统 (AMSSKMS) 权限添加到任何角色 (可以打开)。SR/Incident/RFC

ID	技术标准
4.12	IAM 策略不得包含任何包含在任何 AMS Amazon 日志组上的“允许日志:DeleteLogStream ” DeleteLogGroup 和“日 CloudWatch 志:”操作的操作。
4.13	不得允许创建多区域密钥。
4.14	要提供对您的账户中尚未创建 ARNs 的 S3 存储桶的访问权限，请使用特定于服务的 S3 条件密钥s3:ResourceAccount 来指定账号。
4.15	您可以对自定义控制面板拥有查看、创建、列出和删除权限，但只能在 Amazon 控制面板上查看和列 CloudWatch 出。
4.15.1	您可以查看、创建、列出和删除您的 S3 存储镜头自定义仪表板。
4.16	可以授予与 SQL Workbench 相关的完全权限，roles/users 允许其使用 Amazon Redshift 数据库。
4.17	可以将任何 AWS CloudShell 权限授予客户角色作为 CLI 的替代方案。
4.18	以可信委托人 AWS 服务 为的 IAM 角色也必须符合 IAM 技术标准。
4.19	服务关联角色 (SLRs) 不受 AMS IAM 技术标准的约束，因为它们由 IAM 服务团队构建和维护。

ID	技术标准
4.20	IAM 策略不得允许对账户中所有存储桶的 Amazon S3 存储桶对象 (例如 Amazon S3:GetObject) 进行不受限制的读取权限 : • 在开发者模式账户中 : 违规行为会导致风险通知 • 在非开发者模式账户中 : 违规行为需要接受风险
4.21	可以向客户授予资源类型 “savingsplan” 的所有 IAM 权限。
4.22	AMS 工程师不得在任何数据存储服务 (例如 Amazon S3、Amazon Relational Database Service、Amazon DynamoDB 等) 或操作系统文件系统中手动复制或移动客户数据 (文件、S3 对象、数据库) 。
4.23	不得修改 SCP 策略以允许任何 AMS 托管账户中的任何其他访问权限。
4.24	不得允许对 SCP 政策进行任何可能破坏 AMS 基础设施或管理能力的更改。(注意 : AMS 资源带有标签 AppId= AMSInfrastructure , 紧随其后的是 AMS 受保护的命名空间) 。
4.25	AMS 自动 IAM 配置功能必须作为可选功能在您的账户中启用。
4.26	AMS 人工扮演的角色或用户不得访问客户在 S3、RDS、DynamoDB、Redshift、Elasticache、Elasticache、EFS 和中的内容。FSx此外, 在操作员角色中, 必须明确拒绝访问其他 AWS 服务 人 APIs 发布的已知新内容, 且授予客户内容访问权限。

ID	技术标准
5.0	联合身份验证
5.1	必须在 AMS 托管账户中使用联合身份验证进行配置。
5.2	从 AMS AD 到您的活动目录只能存在单向传出信任（AMS AD 信任本地 AD）。
5.3	AMS 托管应用程序账户中不得存在用于向 AMS 进行身份验证的身份存储。
6.0	跨账户政策
6.1	根据客户记录，可以配置属于同一客户的 AMS 账户之间的 IAM 角色信任策略。
6.2	只有当非 AMS 账户由同一 AMS 客户拥有时，才必须配置 AMS 账户和非 AMS 账户之间的 IAM 角色信任策略（通过确认他们属于同一个 AWS Organizations 账户或将电子邮件域名与客户的公司名称进行匹配）。
6.3	如果不接受风险，则不得配置 AMS 账户和第三方账户之间的 IAM 角色信任策略。
6.4	可以配置跨账户策略，以便在同一客户的 AMS 账户 CMKs 之间访问任何客户管理的账户。
6.5	可以配置跨账户策略，通过 AMS 账户访问非 AMS 账户中的任何 KMS 密钥。
6.6	在不接受风险的情况下，不得允许第三方账户访问 AMS 账户内的任何 KMS 密钥的跨账户政策。
6.6.1	只有当非 AMS 账户由同一 AMS 客户拥有时，才能配置跨账户策略，允许非 AMS 账户访问 AMS 账户内的任何 KMS 密钥。

ID	技术标准
6.7	可以配置跨账户策略，用于访问可在同一客户的 AMS 账户之间存储数据的任何 S3 存储桶数据或资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。
6.8	可以配置跨账户策略，从具有只读访问权限的 AMS 账户访问可在非 AMS 账户中存储数据的任何 S3 存储桶数据或资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。
6.9	只有在非 AMS 账户归同一 AMS 客户所有（通过确认他们属于同一个账户或将电子邮件域名与客户匹配）的情况下，才必须配置跨账户策略，才能访问任何 S3 存储桶数据或可以存储数据的资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift），并拥有从 AMS 到非 AMS 账户（或非 AMS 到 AMS 账户）的写入权限的公司名称）。AWS Organizations
6.10	可以配置跨账户策略，从具有只读权限的 AMS 账户访问第三方账户中可以存储数据的任何 S3 存储桶数据或资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。
6.11	不得配置跨账户策略，用于从具有写入权限的 AMS 账户访问第三方账户中可以存储数据的任何 S3 存储桶数据或资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）。

ID	技术标准
6.12	未经风险接受，不得配置第三方账户用于访问 AMS 客户 S3 存储桶或可以存储数据的资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）的跨账户策略。
7.0	用户组
7.1	允许具有只读权限和非变异权限的 IAM 群组。
8.0	基于资源的策略
8.1	必须通过附加基于资源的策略来保护 AMS 基础设施资源，使其免受未经授权的身份的管理。
8.2	除非您明确指定不同的策略，否则您的资源必须使用基于资源的最低权限策略进行配置。
9.0	自助配置服务 (SSP)
9.1	无论是否接受任何风险，都不得修改 AMS 默认 IAM 角色或策略（包括实例配置文件、SSP、模式）。信任策略允许例外（不接受风险）。默认 SSP 角色还允许对角色、策略或用户更改进行标记。
9.3	除默认角色外，Systems Manager Automation 控制台角色的 SSP 策略不能附加到任何自定义角色。只有在确保将策略关联到自定义角色不会为默认 SSP 服务的预期设计之外提供额外权限之后，才能将其他 SSP 策略附加到自定义 IAM 角色。

AMS-STD-003-网络安全

以下是 003-网络安全的标准控件：

ID	技术标准
	联网
1.0	只能通过堡垒主机、堡垒主机 VPC CIDR 范围或同一 EC2 实例 VPC CIDR 范围通过 SSH 或 RDP 访问所有实例。
2.0	允许在 EC2 实例上使用弹性 IP
3.0	必须使用 AMS 控制平面，进而在数据平面中使用 TLS 1.2+。
4.0	所有出口流量都必须使用账户 IGW 或 TGW 通过。
5.0	如果安全组未按照 9.0 连接到负载均衡器，则其入站规则中不得将源设置为 0.0.0.0/0
6.0	未经风险接受，不得将 S3 存储桶或对象公开。
7.0	服务器管理端口 SSH/22 或 SSH/2222 (不是 SFTP/2222)、TELNET/23、RDP/3389、winRM/5985-5986、VNC/ 5900-5901 TS/CITRIX/1494 或 1604、LDAP/389 或 636 以及 RPC/135、NETBIOS/137-139 上的访问权限。
8.0	不得允许公共端口 (mySQL/3306、PostgreSQL/5432、Oracle/1521、MSSQL/1433) 或自定义端口进行数据库管理访问，不得允许未通过 DX、vpc-Peer 或通过安全组通过 VPC 路由到 VPC 的公共端口。 IPs
8.1	任何可以存储客户数据的资源都不应直接暴露在公共互联网上。
9.0	仅允许负载均衡器通过端口 HTTP/80、H TTPS/8443 和 HTTPS/443 直接访问应用程序，

ID	技术标准
	但不允许直接访问任何计算资源，例如实例、容器等。EC2 ECS/EKS/Fargate
10.0	可以允许应用程序通过端口 HTTP/80 和 HTTPS/443 从客户私有 IP 范围进行访问。
11.0	未经风险接受，不得允许对控制 AMS 基础设施访问权限的安全组进行任何更改。
12.0	每次请求将安全组附加到实例时，AMS Security 都会参考这些标准。
13.0	只有通过 DX、vpc-Peer 或 VPN 路由到 VPC 的私有 IP 范围才能允许客户通过端口 3389 和 22 访问堡垒。
14.0	只有当非 AMS 账户由同一 AMS 客户（通过确认他们属于同一 AWS 组织账户或通过将电子邮件域与客户的公司名称进行匹配）时，才必须使用内部工具配置私有托管区域与 VPCs 从 AMS 到非 AMS 账户（或非 AMS 到 AMS 账户）的跨账户关联。
15.0	可以允许属于同一客户的账户之间的 VPC 对等连接。
16.0	只要两个账户均归同一个客户所有（通过确认他们属于同一个账户，或者将电子邮件域名与客户的公司名称进行匹配），AMIs 即可使用内部工具与非 AMS AWS Organizations 账户共享 AMS 库。
17.0	未经风险认可，不得在任何安全组中配置 FTP 端口 21。
18.0	只要所有账户均归客户所有，则允许通过公交网关进行跨账户网络连接。

ID	技术标准
19.0	不允许将私有子网设为公有子网
20.0	不得允许与第三方账户（不归客户所有）的 VPC 对等连接。
21.0	不得允许使用第三方账户（不归客户所有）连接 Transit Gateway。
22.0	AMS 向客户提供服务所需的任何网络流量都不得在客户网络出口点被屏蔽。
23.0	允许与同一客户共享由同一客户 AWS 账户 拥有的解析规则，并附上风险通知
19.0	ICMP
19.1	EC2 从买家基础设施向 Amazon 发出的入库 ICMP 请求需要风险通知。
19.2	允许通过安全组通过 DX、vpc-Peer 或 VPN 从公共 IPs 路由到 Amazon VPC 的入站请求。
19.3	来自公众的入站请求 IPs 如果未通过 DX、vpc-Peer 或 VPN 通过安全组路由到 Amazon VPC，则需要接受风险。
19.4	允许从 Amazon EC2 向任何目的地发出出站 ICMP 请求。
20.0	安全组共享
20.1	如果安全组符合此安全标准，则可以在同一个账户和同一组织 VPCs 中的账户之间共享该安全组。

ID	技术标准
20.2	如果安全组不符合此标准，并且此安全组以前需要接受风险，则 VPCs 在不接受新的 VPC 或账户风险的情况下，不允许在同一账户之间或同一组织中的账户之间使用安全组共享功能。

AMS-STD-004-渗透测试

以下是 004-渗透测试的标准控件

1. AMS 不支持 pentest 基础架构。这是客户的责任。例如，Kali 不是 AMS 支持的 Linux 发行版。
2. 客户需要遵守[渗透测试](#)。
3. 如果客户想在账户内进行基础设施渗透测试，则应提前 24 小时预先通知 AMS。
4. AMS 将根据客户在变更请求或服务请求中明确说明的客户要求提供客户渗透测试基础设施。
5. 客户渗透测试基础设施的身份管理由客户负责。

AMS-STD-005- GuardDuty

以下是 005 的标准控件- GuardDuty

1. GuardDuty 必须始终在所有客户账户中启用。
2. GuardDuty 来自 MALZ 客户托管应用程序账户 (CMA) 的调查结果不会给运营团队带来警报。
3. GuardDuty 警报必须存储在单一账户或同一组织下的任何其他托管账户中。
4. GuardDuty 不得使用的“可信 IP 列表”功能。相反，可以将自动存档用作替代方案，这对于审计目的很有用。
5. GuardDuty 不得在 MALZ 中启用管理员委派，因为委派的管理员可以在不接受风险的情况下执行高权限操作，例如 GuardDuty 在其他账户中禁用。
6. GuardDuty 自动存档过滤器应使用最小范围来获得最大回报。例如，如果 AMS IPs 在不同的 CIDR 区块中看到多个不可预测的，并且有适合使用的公司 ASN，则使用 ASN。但是，如果您可以将范围缩小到特定范围或 /32 地址，则可以将范围缩小到这些范围或 /32 地址。

AMS-STD-006-主机安全

以下是 006-主机安全的标准控件

- 必须始终在所有 EC2 实例上运行防病毒代理。（例如，趋势科技 DSM）。
- 必须启用防恶意软件模块。
- EPS 代理必须包含所有要扫描的目录和文件。
- 通过防病毒解决方案隔离的文件可以按需与您共享。
- 不应安装第三方端点安全解决方案。
- 必须将防病毒签名更新频率设置为每天至少更新一次。
- 必须将计划扫描频率设置为每月至少一次。
- 必须启用实时（按访问时）扫描并始终处于运行状态。
- AMS 不得在您的实例上执行任何非 AMS 拥有或创作的自定义脚本。（注意：您可以通过堆栈管理员访问权限 CT 使用堆栈管理员访问权限或使用[AWS Systems Manager 自动化 \(AMS SSP\)](#) 来实现。
- 不得在 Windows 主机上禁用网络级身份验证 (NLA)。
- 根据配置的补丁周期，主机操作系统必须安装最新的安全补丁。
- AMS 托管账户的账户中不得有非托管实例。
- 不得允许 AMS 在您的实例上创建本地管理员账户。
- EC2 不得在开启时创建密钥对。
- 您不得使用声明为寿命终止 (EOL) 的操作系统，也不得使用供应商或第三方不提供进一步安全支持的操作系统。

AMS-STD-007-日志记录

以下是 007-Logging 的标准控件

ID	技术标准
1.0	日志类型
1.1	操作系统日志：所有主机都必须记录最少的主机身份验证事件、所有使用提升权限的访问事件以及访问和权限配置的所有更改的访问事件，包括成功和失败。
1.2	AWS CloudTrail：必须启用并配置 CloudTrail 管理事件日志以将日志传送到 S3 存储桶。

ID	技术标准
1.3	VPC 流日志：必须通过 VPC 流日志记录所有网络流量日志。
1.4	Amazon S3 服务器访问日志：AMS 强制存储日志的 S3 存储桶必须启用服务器访问日志记录。
1.5	AWS Config 快照：AWS Config 必须记录所有区域中所有受支持资源的配置更改，并且每天至少将配置快照文件传送到 S3 存储桶一次。
1.6	端点保护系统 (EPS) 日志：必须启用并配置 EPS 解决方案日志记录，才能将日志传送到 CloudWatch 日志日志组。
1.7	应用程序日志：客户有权在其应用程序中启用日志记录并存储在 CloudWatch 日志日志组或 S3 存储桶中。
1.8	S3 对象级日志记录：客户有权在其 S3 存储桶中启用对象级日志记录。
1.9	服务日志：客户可以像任何核心服务一样启用和转发 SSP 服务的日志。
1.10	Elastic Load Classic/Application Load Balancer/Network Load Balancing (Load Balancer) 日志：访问和错误日志条目必须存储在 AMS 2.0 托管的 S3 存储桶中。
2.0	访问控制
2.1	您不得拥有存储日志和日志; CloudWatch 日志组的 AMS 要求的 S3 存储桶中的写入或删除权限。
2.2	您必须对账户中的所有日志具有只读访问权限。

ID	技术标准
2.3	作为存储桶策略中的原则，AMS 规定的存储日志的 S3 存储桶不得允许第三方账户用户使用。
2.4	未经您的授权安全联系人明确批准，不得删除来自 CloudWatch 日志日志组的日志。
3.0	日志保留
3.1	AMS 规定的 CloudWatch 日志日志组的日志保留期必须至少为 90 天。
3.2	AMS 规定的用于存储日志的 S3 存储桶的日志保留期必须至少为 18 个月。
3.3	AWS Backup 在支持的资源上，快照应至少保留 31 天。
4.0	加密
4.1	必须在 AMS Teams 要求的存储日志的所有 S3 存储桶中启用加密。
4.2	从客户账户向任何其他账户转发的任何日志都必须经过加密。
5.0	完整性
5.1	必须启用日志文件完整性机制。必须在 AMS 团队要求的 AWS CloudTrail 跟踪中配置“日志文件验证”。
6.0	日志转发
6.1	任何日志都可以从一个 AMS 账户转发到同一客户的另一个 AMS 账户。
6.2	只有当非 AMS 账户由同一 AMS 客户拥有时，才能将任何日志从 AMS 转发到非 AMS 账户。

ID	技术标准
6.3	不得将客户账户中的任何日志转发到第三方账户（该账户不归客户所有）。

AMS-STD-008-AMS-MAD

以下是 008-AMS-MAD 的标准控件

ID	技术标准
1.0	访问控制
1.1	只有具有交互式登录和自动化任务的 AMS 特权用户才能登录管理主机，以管理客户账户中的托管 AD。
1.2	AD 管理员只能拥有委派的管理员权限（AMS 委派管理员组）。
1.3	登录客户 AD 环境（管理主机或实例）的工程师必须具有有时限的访问权限。
1.4	客户在 EC2 实例中使用远程服务器管理员工具对 AD 对象具有只读访问权限。
1.5	不得允许活动目录用户或组拥有管理权限。
1.6	AWS 允许与同一客户 AWS 账户 拥有的目录共享，并附有风险通知。
2.0	服务账号
2.1	必须在应用程序支持的地方使用群组托管服务帐户 (GMSA)，而不是标准服务帐户。
2.2	所有其他服务账户都必须在风险接受流程之后创建。

ID	技术标准
2.3	除非客户明确要求，否则不得重复使用 AD 安全组。应创建新的 AD 组。必须将请求访问服务帐户的计算机对象添加到新的安全组中。
2.4	必须在“托管服务账户”组织单位 (OU) 下添加任何 GMSA 服务帐户。
2.5	必须在“用户→服务帐户” OU 下添加任何非 GMSA 服务帐户。
3.0	组策略对象 (GPO)
3.1	如果“Windows 设置 > 安全设置” GPO 下的任何设置以任何方式降低了当前状态下的帐户安全状况，则不得对其进行修改。
3.2	在 MALZ 中，从申请创建 GPO 的应用程序账户 RFCs 提交，GPO 必须关联到与应用程序账户对应的 OU。任何 GPOs 影响所有帐户的内容都必须来自共享服务帐户。
3.3	必须将 Active Directory 域下所有服务器的默认 RDP 空闲会话超时设置为 15 分钟。
4.0	活动目录信任
4.1	如果条件转发器通过 DX、vpc-Peer 或 VPN 路由到 VPC，则允许单向出站信任 (AMS 托管目录到客户目录)。IPs
5.0	其他
5.1	必须启用日志文件完整性机制。必须在 AMS 团队要求的 AWS CloudTrail 跟踪中配置“日志文件验证”。
6.0	日志转发

ID	技术标准
6.1	客户用户、群组、计算机对象、OU 或其他实体不得按照 AMS 命名惯例使用 AMS 命名惯例。
6.2	所有这些都 OUs 必须由 AMS 管理。

AMS-STD-009-其他

以下是 009-杂项的标准控件

- 如果在资源、对象、数据库或文件系统中启用了加密，则不得将其禁用。

在您的环境中引入高或非常高的安全风险의更改

以下更改会给您的环境带来高或非常高的安全风险：

AWS Identity and Access Management

- High_risk-iam-001：为根账户创建访问密钥
- High_risk-iam-002：修改 SCP 策略以允许其他访问权限
- High_risk-iam-003：SCP 政策修改可能会破坏 AMS 基础设施
- High_risk-iam-004：在客户账户中创建 role/user 基础架构变更权限（写入、权限管理或标记）
- High_risk-iam-005：AMS 账户和第三方账户（不归客户所有）之间的 IAM 角色信任策略
- High_risk-iam-006：跨账户政策，允许第三方账户从 AMS 账户访问任何 KMS 密钥）
- High_risk-iam-007：来自第三方账户的跨账户政策，用于访问 AMS 客户 S3 存储桶或可以存储数据的资源（例如 Amazon RDS、Amazon DynamoDB 或 Amazon Redshift）
- High_risk-iam-008：为客户账户中的任何基础设施变更权限分配 IAM 权限
- High_risk-iam-009：允许列出和读取账户中的所有 S3 存储桶
- High_risk-iam-010：带权限的自动化 IAM 预配置 read/write

网络安全

- High_risk-net-001：从互联网上打开操作系统管理端口 SSH/22 或 SSH/2222（不是 SFTP/2222）、TELNET/23、RDP/3389、winrm/5985-5986、VNC/ 5900-5901 TS/CITRIX/1494 或 1604、LDAP/389 或 636 和 NETBIOS/137-139

- High_risk-net-002 : 打开数据库管理端口
mysql/3306、PostgreSQL/5432、Oracle/1521、MSSQL/1433 或互联网上的任何管理客户端口
- High_risk-net-003 : 直接在任何计算资源上打开应用程序端口 HTTP/80、HTTPS/8443 和 HTTPS/443。例如，来自互联网的 EC2 实例、ECS/EKS/Fargate 容器等
- High_risk-net-004 : 对控制 AMS 基础设施访问权限的安全组所做的任何更改
- High_risk-net-006 : 与第三方账户 (不归客户所有) 的 VPC 对等
- High_risk-net-007 : 添加客户防火墙作为所有 AMS 流量的出口点
- High_risk-net-008 : 不允许与第三方账户连接 Transit Gateway
- High_Risk-S3-001 : 在 S3 存储桶中配置或启用公共访问权限

日志系统

- High_risk-log-001 : 禁用。CloudTrail (需要运营现场经理批准)
- High_risk-log-002 : 禁用 VPC 流日志。(需要运营现场经理批准)
- High_risk-log-003 : 通过任何方法 (S3 事件通知、SIEM 代理提取、SIEM 代理推送等) 将日志从 AMS 托管账户转发到第三方账户 (不归客户所有)
- high_risk-log-004 : 使用非 AMS 跟踪进行 CloudTrail

主机安全

- High_risk-host-001 : 出于任何原因在账户中禁用端点安全。(需要运营现场经理批准)
- high_risk-host-002 : 在资源或账户级别禁用修补。
- high_risk-host-003 : 在账户中部署非托管实例。EC2
- High_risk-host-004 : 运行客户提供的自定义脚本。
- High_risk-host-005 : 在实例上创建本地管理员帐户。
- High_risk-host-006 : 趋势科技 EPS 文件类型/扩展名扫描排除项或在端点上禁用恶意软件防护。

Note

对于与渗透测试或漏洞扫描相关的 EPS 反恶意软件排除或 GuardDuty 抑制规则，或者需要采取主动措施的影响 events/known 性能的服务问题，无需接受风险。在这种情况下，风险通知就足够了。

- high_risk-host-007 : 为 KeyPair EC2

- High_risk-host-008 : 在中禁用端点安全 EC2
- High_risk-host-009 : 使用生命周期终止 (EOL) 操作系统的账户

其他

- High_risk-enc-001 : 如果启用了任何资源的加密，则将其禁用

托管活动目录

- High_risk-ad-001 : 为活跃的导演用户或组提供管理员权限
- High_risk-ad-002 : 能够降低账户安全状况的 GPO 策略

AMS 高级版中的连续性管理

作为连续性管理的一部分，AWS Managed Services (AMS) 提供对 AWS Backup本机服务的自动访问 AWS。这便于访问支持亚马逊 EBS、亚马逊、亚马逊 RDS EC2、Amazon EFS 等的服务。

要了解更多信息，请参阅 [AWS Backup：工作原理](#)。

主题

- [什么是连续性管理？](#)
- [连续性管理的工作原理](#)
- [灾难恢复响应](#)
- [灾难恢复计划](#)

什么是连续性管理？

连续性管理是 AMS 用来为您的账户提供备份和快照的流程。

AMS AWS Backup 通过更改类型提供访问权限，您可使用这些更改类型来创建和管理备份任务和计划。

连续性管理的工作原理

AMS [AWS Backup](#)用于连续性管理。

开始 AWS Backup 在 AMS 中使用时：

1. 运行按需备份
2. 创建备份计划（可选，AMS 提供默认备份计划）
3. 使用默认 AMS a 备份存储库（可选）
4. 管理（运行、完善、删除等）您的备份计划和恢复点

AMS 备份计划

备份计划是一种策略表达式，用于定义何时以及如何备份支持的 AWS 资源，例如 RDS 数据库、EBS 卷、DynamoDB 表和 EFS 文件系统。计划和保留策略通过自定义备份计划进行管理，您可以在 AMS

Advanced 中使用更改类型 (CT) 或与 AMS Accelerate AWS Backup 一起使用更改类型 (CT) 来创建这些计划。使用标签为备份计划分配资源，并根据定义的备份计划 AWS Backup 自动备份和保留已分配资源的备份。如果您的工作负载具有不同的备份要求，则可以创建多个备份计划。

一个备份计划最多可以有六条备份规则，用于定义时间表和保留期以及其他详细信息。备份时间表决定何时 AWS Backup 启动备份任务以及创建备份的频率。您可以选择每小时、每天、每周或每月的频率。删除天数设置决定了快照在自动删除之前要存储多少天。

Note

AMS Advanced：如果您从旧版 AMS 备份系统迁移，AMS 会创建默认备份计划以实现向后兼容。在这种情况下，密钥:值对是 Backup: True。为了支持向后兼容，此处的值不区分大小写，因此 Backup: True 或 backup: True 都是有效的标签。所有其他 key: value 对都区分大小写。AWS Backup 可以在 EBS 卷级别或 Amazon EC2 实例级别运行，但不能同时运行两者，因为这可能会导致备份可能发生冲突的争用情况。

默认备份计划，多账户 landing zone

在新的账户创建 RFC 期间，AMS 确保在账户级别有一个总体默认备份计划来保护您的工作负载。必填字段的值是默认设置的，如下节所示：

默认 AMS 备份计划

default-backup-plan

标签密钥：Backup

标签值：True

```
RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for
23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for
23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for
23:30 UTC time on day 1 of the month, only in January)
```

RuleForYearlyBackups delete after years: 2 years

默认 AMS 备份计划	Start Time	保留
每小时备份	不适用	不适用
每日备份	世界标准时间每天晚上 11:30	7 days
每周备份	每周世界标准时间晚上 11:30，仅在星期六	4 个星期
每月备份	每月世界标准时间晚上 11:30，每月第 1 天	26 个星期
年度备份	世界标准时间下午 11:30，每月第一天	2 年

增强的默认 AMS 备份计划

该计划是防范勒索软件攻击 AWS Backup 的最佳实践蓝图。它实施每日、每周、每月和每年的备份策略。AWS Backup 在[支持的资源](#)上启用了[连续备份](#)，保留期最长（31 天）。

ams-enhanced-default-backup-计划

标签密钥：backup-orchestrator-enhanced

标签值：true

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00 UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for 02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00 UTC time on day 1 of the month, only in January)
```

RuleForYearlyBackups delete after years: 2 years

增强的 AMS 备份计划	Start Time	保留
每小时备份	不适用	不适用
每日备份	世界标准时间每日 4:00	31 天
每周备份	世界标准时间星期六 2:00	6 个星期
每月备份	本月 1 日，世界标准时间 2:00	26 个星期
年度备份	世界标准时间 1 月 1 日 2:00	2 年

数据敏感的 AMS 备份计划

该计划是 AWS Backup 最佳实践的蓝图，用于防范数据敏感型应用程序的勒索软件攻击。它实施每小时、每天、每周、每月和每年的备份策略。AWS B [ackup 连续备份](#)在[支持的资源](#)上启用了最长保留期（31 天）。

ams-data-sensitive-backup-计划

标签密钥：backup-orchestrator-data-sensitive

标签值：true

```
RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

数据敏感型 AMS 备份计划	Start Time	保留
每小时备份	在小时大关	7 days
每日备份	世界标准时间每日 4:00	31 天
每周备份	世界标准时间星期六 2:00	6 个星期
每月备份	本月 1 日，世界标准时间 2:00	26 个星期
年度备份	世界标准时间 1 月 1 日 2:00	2 年

AMS 备份保管库

AWS Backup 将快照组织到称为文件库的逻辑存储单元中。

您可以使用标签控制单个存储库级别的备份库通知。您可以通过在特定文件库True上添加标签AMSNotificationOptOut并将该值设置为，来选择不接收针对特定文件库的通知。要恢复从文件库中获取通知，请移除标签。

要查看您的 AMS 备份列表，请打开[AWS Backup 控制台](#)。在导航窗格中，选择 Backup 保管库，然后从下表选择一个 AMS 备份存储库。在“备份”部分，查看备份库中所有备份的列表。选择要编辑、删除或恢复的备份。

AMS 备份计划的保管库

AMS 保管库名称	说明
ams-automated-backups	此保管库会接收 AMS 高级默认 AWS Backup 计划使用的所有恢复点default-backup-plan。
ams-automated-enhanced-backups	此保管库接收由 AMS 高级增强版默认 AWS Backup 计划 ams-enhanced-default-backup-计划获取的所有恢复点。
ams-automated-data-sensitive-备份	此保管库收到 AMS 高级 AWS Backup 计划 ams-data-sensitive-backup-计划使用的所有恢复点。

AMS 保管库名称	说明
ams-manual-backups	如果未定义存储库名称，则这是 Start Backup Job RFC (ct-2hhud2lx01tq7) 备份计划中所有备份的默认位置。
ams-custom-backups	这是 AMS 在使用 Patch Orchestrator 修补实例或每月补丁活动之前拍摄的快照的默认位置。根据 AMS 补丁生命周期默认政策 (60 天)，它们会自动删除。

AMS 备份更改类型

AMS 提供了多种备份计划 CTs 供您创建和使用备份计划。

Important

请勿编辑您的 AMS 默认备份计划，因为您所做的更改可能会丢失。取而代之的是，为您的自定义配置制定新的计划。

- [Backup 计划：创建](#)
- [Backup Job：开始](#)
- [Backup Job：停止](#)
- [恢复点：删除](#)
- [DynamoDB | 从备份创建](#)
- [EBS 卷：从 Backup 创建](#)
- [亚马逊 Elastic File System \(EFS\)：从备份创建](#)

AMS 备份监控和报告

Important

AMS 备份监控和报告仅在 AMS 支持的地区提供。它们是美国东部 (弗吉尼亚州)、美国西部 (加利福尼亚北部)、美国西部 (俄勒冈)、美国东部 (俄亥俄州)、加拿大 (中部)、南

美洲 (圣保罗) 、欧洲 (爱尔兰) 、欧洲 (法兰克福) 、欧洲 (伦敦) 、欧洲 (巴黎) 、亚太地区 (孟买) 、亚太地区 (首尔) 、亚太地区 (新加坡) 、亚太地区 (悉尼) 、亚太地区 (东京) 。

AMS 生成每日自助服务报告以及有关资源覆盖率和备份任务状态的月度报告。月度报告在《月度商业评论》(MBRs) 中共享。要了解有关每日备份报告的更多信息，请参阅[每日备份报告](#)。

AMS 专家会监控您使用配置的所有备份任务 AWS Backup。如果备份失败，AMS 会调查故障并通知您根本原因和补救选项 (如果有) 。为了避免警报噪音，在导致您的账户出现大量备份失败的事件中，AMS 会通过您的 CSDM 提出集体建议，而不是就每个故障通知您。

请注意，AMS 不会监控使用 AWS 服务的独立备份功能配置的任何备份。

灾难恢复响应

除了以下各节中描述的选项外，您最好知道要采取哪些步骤来启动 AMS 的灾难恢复 (DR) 。

如果您遇到灾难并需要启动恢复，请遵循以下一般准则：

1. 打开“可用性”类别的高优先级事件。AMS 将打开会议桥并邀请您的团队加入。
2. 了解需要恢复的资源清单。
3. 了解需要恢复到的目标着陆区 (LZ) (例如，同一个账户、不同的可用区或不同的账户和不同的区域) 。
4. 为目标 landing zone 中的每个资源提交恢复请求。遵循您现有的灾难恢复计划或查看下一节中的选项 (例如[在 AMS 上 EC2 使用 EBS 快照提供灾难保护](#)、或[在 AMS 上 EC2 使用 Elastic 灾难恢复实现灾难保护](#)) 。
5. 恢复应用程序功能并使用 AMS 帮助来解决与基础设施相关的问题。

AMS 可以帮助您为本次活动做准备，并为您的组织制定灾难恢复计划以涵盖这些问题。有关更多详细信息，请联系您的云服务交付经理 (CSDM) 或云架构师 (CA) 。

灾难恢复计划

灾难恢复 (DR) 是企业业务连续性和合规性的关键服务。AMS 与您合作，帮助您规划、实施和维护 AMS 灾难恢复策略。

AMS landing zone (LZ) (多账户和单账户) 为满足大多数灾难保护场景的 AMS 基础设施组件提供原生、多可用区、高可用性。但是，根据您企业的地理覆盖范围，您可能需要区域保护。为了实现跨区域可用性和灾难恢复，需要在不同的地区使用另一个 AMS 账户 (对于多账户 landing zone 和单账户着陆区都是如此)。

AMS 符合本博客“在灾难中[快速恢复任务关键型系统](#)”中所述的 [AWS 灾难恢复指南](#)，并支持以下四个选项：

- 多站点 (或高可用性)
- 热待机
- 飞行员灯
- 备份与还原

以下各节将介绍这些选项以及对它们的 AMS 支持。

多站点或高可用性 (HA)

HA 解决方案通常由应用程序的内置功能提供，例如集群或同步复制。用户会被定向到 Prod 和 HA/DR 节点。DNS 可以直接指向节点，也可以通过弹性负载均衡器 (ELB) 指向节点。

作为您 Well-Architected-Review 和灾难恢复规划的一部分，您的 AMS 云架构师 (CA) 将与您合作。

HA DR 利用应用程序和 AWS 原生服务和功能，如下图所示：

灾难恢复站点可以是相同的，也可以是不同的 AWS 区域。

Note

不同的区域 (跨区域) 将具有不同的活动目录环境。

DR (故障转移) 步骤：自动故障转移，无需手动步骤。如果主 LZ 出现故障，用户将被自动重新路由到该节点。DR/HA 这是通过 DNS 和应用程序配置实现的。

HA DR 指标：

- 恢复点目标 (RPO)：<5 分钟

- 恢复时间目标和 (RTO) : <5 分钟
- 维护 : 高 (两种环境都需要同步更改 , 例如应用程序配置、修补、SG 或 ALB、证书等) 。
- 成本 : 高

温备用

“热备用”一词用于描述灾难恢复 (DR) 场景 , 在这种场景中 , 缩小版本的环境正在云中运行。

数据复制通常由应用程序层异步处理到在线实例 , 而其余实例 (例如应用程序层和 Web 层) 可能会关闭以节省成本。用户只能被定向到生产站点。其他 AWS 资源 , 例如弹性负载均衡器 (ELB) , 也可以在灾难恢复站点中预配置。

作为您 Well-Architected-Review 和灾难恢复规划的一部分 , 您的 AMS 云架构师 (CA) 将与您合作。

Warm Standby DR 利用应用程序和 AWS 本机服务和功能 , 如下图所示 :

灾难恢复站点可以是相同的 , 也可以是不同的 AWS 区域。

Note

不同的区域 (跨区域) 将具有不同的活动目录环境。

DR (故障转移) 步骤 :

1. 停止数据复制 , 将灾难恢复站点中的数据实例设为主实例
2. 根据需要更新应用程序配置 (新 IP、服务器名称等)
3. 将 DNS 重定向到灾难恢复站点 (ELB)
4. AD 依赖关系 (如果需要) (服务帐号 SPNs GPOs、 、 等)

HA DR 指标 :

- 恢复点目标 (RPO) : <1 小时
- 恢复时间目标和 (RTO) : <1 小时 (取决于实例数量和编排)
- 维护 : 高 (两个环境都需要同步更改 , 例如应用程序配置、补丁、安全组 (SG) 或应用程序负载均衡器 (ALB)、证书等) 。

- 成本：中等

指示灯

在这种灾难恢复 (DR) 方法中，您可以为一组有限的核心服务复制 Prod 环境的一部分。基础架构的一小部分始终处于运行状态，同时同步可变数据（例如数据库或文档），而基础架构的其他部分则处于关闭状态，仅在测试期间使用。与备份和恢复方法不同，您必须确保最关键的元素已经配置好并在 DR landing zone（指示灯）中运行。

作为您 Well-Architected-Review 和灾难恢复规划的一部分，您的 AMS 云架构师将与您合作。

Pilot Light DR 利用应用程序和 AWS 原生服务和功能，如下图所示：

灾难恢复站点可以是相同的，也可以是不同的 AWS 区域。

Note

不同的区域（跨区域）将具有不同的活动目录环境。

DR（故障转移）步骤：

1. 停止数据复制，将灾难恢复站点中的数据实例设为主实例
2. 启动已关闭的实例和基础架构
3. 根据需要更新应用程序配置（新 IP、服务器名称等）
4. 根据需要实例添加到 ELB
5. 将 DNS 重定向到灾难恢复站点 (ELB)
6. AD 依赖关系（如果需要）（服务帐号 SPNs GPOs、等）

指示灯灾难恢复指标：

- 恢复点目标 (RPO)：<1 小时
- 恢复时间目标和 (RTO)：约 1 小时（取决于实例数量和编排）
- 维护：中等
- 成本：中等

备份与还原

这种简单而低成本的灾难恢复 (DR) 方法可以将您的数据和应用程序从任何地方备份到 DR landing zone，以便在灾难恢复期间使用。

作为备份和灾难恢复计划的一部分，您的 AMS 云架构师会与您合作。

Backup and Restore DR 使用 AMS 自动工具和流程，如下图所示：

可以使用两种备份和复制方法：

- EBS 快照（恢复点目标 (RPO) > 1 小时），被称为“EBS”
- AWS Elastic Disaster Recovery（恢复点目标 (RPO) ~ 0.25 小时），被称为“DRS”

灾难恢复站点可以位于相同或不同位置 AWS 区域。

Note

不同的区域（跨区域）具有不同的活动目录环境。

DR（故障转移）步骤：

1. 从快照还原实例（两步流程，先使用占位符实例）
2. 更新应用程序配置（新 IP、服务器名称等）
3. 根据需要设置其他基础架构（SG、ELB 等）
4. 将 DNS 重定向到灾难恢复站点 (ELB)
5. 根据需要更新或恢复 AD 依赖关系（服务帐号、服务主体名称 (SPNsGPOs)、组策略对象 () 等）

Backup 和 Restore 灾难恢复指标：

- 恢复点目标 (RPO)：>1 小时或大约 0.25 小时（取决于所选的解决方案-EBS 或 DRE）
- 恢复时间目标和 (RTO)：约 1 小时（取决于实例数量和编排）
- 维护：高（在两个环境中都需要同步更改，例如应用程序配置、补丁、安全组或应用程序负载均衡器、证书等。

- 成本：中等

在 AMS 上 EC2 使用 EBS 快照提供灾难保护

先决条件：

- AMS Prod 着陆区（来源）
- AMS DR 着陆区（灾难目标）
- 已为 EC2 实例启用 EBS 快照 (AWS Backup)

快照复制解决方案：

- 跨可用区：不适用-根据设计，EBS 快照在该区域内的可用性很高
- 跨区域：AWS Backup

下图显示了从 AMS 上的 EBS 快照 EC2 恢复的过程：

EC2 AMS 上的 DR 步骤：

1. 提出 RFC 以与目标账户共享 EBS 快照（跨区域灾难恢复所必需的）。

更改类型：管理、高级堆栈组件、EBS 快照、共享

2. 在目标子网（灾难恢复站点子网）中创建占位符 EC2 AMS 堆栈。建议使用 CFN 摄取来创建堆栈，因为客户可以在同一个堆栈中组合分配安全组和其他（例如将实例添加到 ELB）的步骤。

更改类型：部署、接收、CloudFormation 模板堆栈、创建

3. 提高 RFC 以执行 EC2 堆栈卷恢复。

更改类型：管理、高级堆栈组件、EC2 实例堆栈、恢复卷。

CT 从步骤 1 中共享的快照中恢复卷，并连接到步骤 2 中创建的占位符实例。

音量恢复 CT 功能：

- 关闭占位符实例
- 从快照恢复卷

- 换出音量
- 启动实例
- 留下旧域名
- 更改主机名
- 重新启动。AMS 引导脚本在启动时将实例加入目标 (DR) 域

音量恢复 CT 输入：

- InstanceId (占位符实例 ID)
- RootDeviceSnapshotId , 已恢复的根卷的 EBS 快照
- KMSKeyId、KMS 密钥标识符或 ARN , 用于加密实例上所有已恢复的卷 EC2
- DeviceNames , 最多 25 个 (可选)
- SnapshotIds , 最多 25 个 (可选) 。要恢复的卷的快照列表

在 AMS 上 EC2 使用 Elastic 灾难恢复实现灾难保护

先决条件：

- AMS Prod 着陆区 (来源)
- AMS DR 着陆区 (灾难目标)
- 您必须先为计划在其中使用的所有 AWS 区域 内容初始化 Elastic 灾难恢复服务。

在您的 DR 着陆区 (LZ) 中创建一个 IAM 角色以访问 Elastic 灾难恢复控制台。

- 重要：SSM 文档是在 DRS 中作为启动后操作创建的。必须在所有服务器的 PostLaunch 设置中启用此操作。
- 目标 (占位符) 实例必须具有标签键：AWSDRS“”，值：“AllowLaunchingIntoThisInstance”。占位符实例必须处于停止状态。否则，AMS 无法在启动设置下选择占位符实例，Elastic 灾难恢复也无法在占位符实例之上进行恢复。

有关 AMS EC2 上的 Elastic 灾难恢复设置和恢复过程的示意图，请参阅 [AWS Elastic Disaster Recovery \(AWS DRS\) 通用架构](#)。

EC2 AMS 上的 Elastic 灾难恢复的灾难恢复步骤：

1. 使用适当的标签在目标子网（灾难恢复站点子网）中创建占位符 EC2 AMS 堆栈，有关更多信息，请参阅上一节。我们建议使用 CFN 摄取来创建堆栈，因为您可以将分配安全组和标记实例、EBS 卷及其他（例如将实例添加到 ELB）的步骤组合到同一个堆栈中。

更改类型：部署、接收、CloudFormation 模板堆栈、创建

2. 停止占位符实例。

更改类型：管理、高级堆栈组件、EC2 实例、停止

3. 如果未在步骤 1 中完成，请使用密钥："AWSDRS"，value:"" 标记占位符实例及其 EBS 卷。AllowLaunchingIntoThisInstance

更改类型：管理、高级堆栈组件、标记、更新。

4. 使用步骤 1 中的占位符实例作为源服务器的“启动到实例 ID”、“DRS 启动设置”下的目标。从 Elastic 灾难恢复控制台为源服务器启动实例恢复演练。

Note

占位符实例卷保留在账户中。要删除这些卷，请在灾难恢复操作结束时提交管理 | 高级堆栈组件 | EBS 卷 | 删除更改类型 (ct-3e3h8u0sp5z80)。

弹性灾难恢复恢复工作流程：

- 目标（占位符）实例必须处于停止状态
- 交换卷并删除源（占位符）根卷
- 启动实例
- 运行“启动后操作”以完成以下项目：
 - 激活 SSM 代理。
 - 交换卷并删除源（占位符）根卷。
 - 启动实例
- 运行 PostLaunchScript SSM 文档。本文档执行以下操作：
 1. 离开旧域名。
 2. 更改主机名。
 3. 重新启动。AMS 引导脚本在启动期间将实例加入目标 (DR) 域。

AMS 中的补丁管理

主题

- [AMS Patch Orchestrator：基于标签的修补模型](#)
- [使用补丁编排器](#)
- [按需修补](#)
- [AMS 标准补丁](#)
- [修补服务承诺](#)

在 AMS 中，补丁管理是一项服务，可帮助您在亚马逊弹性计算云 (Amazon EC2) 实例上维护操作系统供应商的更新。您可以自由自定义修补您的 Amazon EC2 实例的频率和流程。

您可以在入职期间配置补丁管理，也可以使用 RFC 流程对其进行更新。使用变更管理系统和补丁兼容模板（适用于 Amazon、Amazon EC2 Auto Scaling 组、HA 一层或两层堆栈）创建的堆栈会自动订阅补丁管理。

AMS 提供了一项名为 Patch Orchestrator（基于标签的修补）的功能，用于配置补丁。

有关修补术语的定义，请参见[AMS 关键术语](#)。

Important

- 如果创建堆栈的 AMS 模板与补丁管理兼容，则堆栈或堆栈的组成实例就无法选择退出补丁管理。目前，修补与以下堆栈模板兼容：
 - Amazon EC2 stack | 创建，然后亚马逊 EC2 堆栈 | 创建（使用其他卷）
 - Amazon EC2 实例已通过 CloudFormation 摄取启动
 - Auto Scaling 组 | 创建（组中的亚马逊 EC2 实例已修补）
 - 高可用性单层堆栈 | 创建和高可用性双层堆栈 | 创建
- 如果持续发生影响堆栈的事件，AMS 操作员可以重新安排或取消预定的补丁。
- 默认情况下，特定补丁兼容堆栈中的所有实例都已就地修补。要使用 AM latest/patched S AMI 替换亚马逊系统映像 (AMI) 来修补 Auto Scaling 群组，请提交服务请求。每个月都会将更新内容 AMIs 分享给账户。

Important

您可以为托管节点指定备用补丁存储库。在 AMS 实施您请求的补丁配置时，您负责选择和验证所选存储库的安全性。您还必须接受使用这些存储库所带来的任何风险，例如供应链风险。以下是确保补丁管理流程安全性的最佳实践：

- 仅使用可信、经过验证的存储库来源
- 如果可能，默认为标准操作系统供应商存储库
- 定期审核自定义存储库配置

Tip

AMS 建议您为具有重要应用程序或服务的实例启用备份。有关启用备份的信息，请参见[AMS 高级版中的连续性管理](#)。

AMS Patch Orchestrator：基于标签的修补模型

如果您已加入新的 AMS Patch Orchestrator 基于标签的修补模型，则可以使用标签将补丁配置应用于一组精确的资源（称为补丁组），范围从一个实例到所有实例。有关 AMS 标签的信息，请参阅[使用标签](#)。以下部分提供了有关设置 Patch Orchestrator 标签的说明。

修补程序是在您使用 [SSM 补丁窗口 | Create 定义的补丁窗口](#) 中安装的。每个补丁窗口都是一个 AWS Systems Manager 维护窗口，该窗口按您选择的时间表运行，具有配置的持续时间，适用于一个补丁组。不属于显式补丁窗口的实例将在您加入 Patch Orchestrator 时定义的默认维护时段内进行修补。

Important

如果计划同时运行多个补丁维护窗口，则在任何给定时间处理的实例数必须少于 1001 个。这是 AWS Systems Manager 的限制。AMS 建议每五十个实例至少使用一小时。

默认情况下，操作系统 (OS) 供应商提供的所有补丁都是在维护时段或按需补丁期间安装的。这称为默认补丁基准。如果您想限制安装哪些补丁，则可以使用其中一个补丁基准来定义自定义补丁基准 CTs（每个 OSes），请参阅[修补子类别](#)。例如，您可以使用自定义补丁基准，以便仅为一个或多个补丁组安装关键和重要的安全更新。

在实例上安装补丁后，实例将重启。补丁通知在修补之前和之后发送，并在预定启动前 96 小时内发送额外的提醒。此外，AMS 会在选定的维护时段内对基础设施管理工具（例如 AWS SSM 代理）进行更新。

Important

AMS 已弃用缺少补丁的实例的月度补丁合规性报告，并且不会发送月度报告。之所以做出这一更改，是因为最近发布了自助运营报告，这些报告每 24 小时更新一次，可按需提供给您，并提供最新和最精细的数据。要了解有关报告的更多信息，请参阅自助报告。要了解有关报告的更多信息，请参阅[自助报告](#)。

有关通知的更多信息，请参阅[补丁通知](#)。

使用补丁编排器

提交包含以下详细信息的服务请求，为您的账户启用 AMS Patch Orchestrator：

- 类别：其他
- 主题：入门 Patch Orchestrator
- 抄送电子邮件：当此入职 RFC 的状态发生变化时，抄送电子邮件地址会收到通知
- 详情：将以下信息粘贴到电子邮件中并提供您的价值观。请注意，ThirdTagKey 是可选的。有关建议和示例，请参阅下表。

```
Default maintenance window Schedule:
Default Maintenance Window Schedule TimeZone:
Default Maintenance Window Duration:
Default Maintenance Window Cutoff:
Default Patch Backup Retention In Days:
Default Maintenance Window Notification Emails:
First Tag Key:
Second Tag Key:
Third Tag Key:
```

下表描述了您提供的值的格式和建议。

Patch Orchestrator 基于标签的修补配置

参数的名称	信息	推荐或示例
默认维护时段计划	默认维护时段的计划，以 cron 或速率表达式形式出现。例如： • <code>cron(0 3 ? * 6L *)</code>: 每月最后一个星期五凌晨 03:00 • <code>rate(7 days)</code>: 每七天一次 有关创建 cron 表达式以及指向 cron 和速率表达式资源的链接的更多信息，请参阅维护时段的 Cron 和费率表达式。	我们建议在稳定的工作日每月至少运行一次窗口。
默认维护时段计划时区	默认维护时段所基于的时区采用互联网号码分配机构 (IANA) 格式。	例如： • 美洲/洛杉矶 • etc/UTC
默认维护时段持续时间	默认维护时段的持续时间（以小时为单位）。	每 50 个实例至少 1 小时，外加 2 小时的截止时间。
默认维护时段截止时间	默认维护时段结束前没有启动任何新的修补命令的小时数。存在此间隔是为了留出足够的时间在窗口结束之前完成修补。	至少 2 小时。
默认 Patch Backup 保留天数（可选）	在修补实例之前保留创建的 EBS 还原点的默认时间（以天为单位）。	我们建议保留默认值，即 60。

参数的名称	信息	推荐或示例
默认维护时段通知电子邮件	一到五个电子邮件地址或通讯组列表，用于接收有关默认维护时段修补状态的通知。	我们建议使用群组通讯组列表代替个人电子邮件。
第一个标签密钥	用于创建 Patch Group 标签值的第一个标签密钥。	例如 AppId。如果您已经使用修补程序组标签定义了自己的修补程序组，请指定 null。
第二个标签密钥	用于创建 Patch Group 标签值的第二个标签密钥。	例如，环境。如果您已经使用修补程序组标签定义了自己的修补程序组，请指定 null。
第三个标签密钥（可选）	用于创建 Patch Group 标签值的可选第三个标签键。	例如，群组。

在您加入新的 Patch Orchestrator 修补服务模型后，您账户中所有经过适当标记的实例都属于带有补丁组标签的补丁组。Patch Orchestrator 使用你现有的补丁组标签，或者使用 AMS 创建的标签，该标签由你在 Patch Orchestrator 入职期间指定的两个或三个串联的标签值组成。例如，{*Tag Value 1*}-{*Tag Value 2*}-{*Tag Value 3*}。AMS 每 12 小时更新这些 AMS 应用的补丁组标签。如果需要，您可以使用[标记 | 更新（需要审阅）](#)或[标记 | 更新（需要审阅）更改类型来更新补丁组标签值](#)。

例如，如果您的 Amazon EC2 实例具有以下标签键:值对：

- AppId:MyApplication
- Environment:Production
- Group:1

在入职期间，您指定了以下标签键：

- First Tag Key = AppId
- Second Tag Key = Environment
- Third Tag Key = Group

AMS 创建以下补丁组标签并将其应用于您的实例:Patch Group:MyApplication-Production-1.

Note

不会为操作系统不支持的实例创建补丁失败警报，也不会为在维护时段内停止的实例创建补丁失败警报。

补丁编排器先决条件

Patch Orchestrator 工作流程针对的是由最新版本的系统管理器自动化文档修补的亚马逊 EC2 实例：`AWSSManagedServices-PatchInstanceFromMaintenanceWindow`

作为文档工作流程的一部分，运行命令文档“AWS-RunPatchBaseline”是针对补丁组成员中的每个 Amazon EC2 实例运行的。要了解更多信息，请参阅[关于 SSM 文档 AWS-RunPatchBaseline](#)。

要求：

- 从 AMS 提供的亚马逊系统映像 (AMI) 部署的亚马逊 EC2 实例，或者通过“迁移合作伙伴迁移的实例堆栈”CT (ct-257p9zjk14ija) 在 AMI 上部署。
- 已启用出口互联网连接。对于 firewall/proxy 解决方案，要求允许 Windows 更新终端节点 and/or Linux 存储库镜像终端节点、AWS 系统管理器代理设置和元数据代理配置。有关更多信息，请参阅[将 SSM 代理配置为使用代理](#)和[使用 HTTP 代理](#)
- IAM 角色与 IAM 角色的 SSM 服务的最低许可访问权限相匹配。customer-mc-ec2-instance-profile
- 我们建议 10 GB 的可用根分区空间。对于 Linux 操作系统，该/var分区中至少有 2 GB 的可用空间。
- 适用于更新下载的有效证书颁发机构。
- Windows 服务器更新服务 (WSUS)-注册表包括但不限于：DisableWindowsUpdateAccess，NoWindowsUpdate；自动更新不得损害 Windows 更新过程的运行。

验证：

- 对于使用 yum 包管理器的 Linux 操作系统实例，你可以通过运行来验证更新的可用性 `#yum check-update`
- 对于 Linux OS RedHat 5.7 及更高版本、6.1 及更高版本以及 7.0 及更高版本；亚马逊 EC2 实例通过“迁移伙伴迁移的实例堆栈”CT (ct-257p9zjk14ija) 迁移到您的 AMS 账户，您需要验证订阅管理器状态以获得更新性能。

- 在 Windows 操作系统上，启用 Windows 服务器更新服务 (WSUS)。任何本地策略都不应阻止 WSUS 扫描或安装更新的功能。以管理员身份登录后，您可以通过从 Windows 更新服务控制台扫描可用更新来对其进行验证。包括 2012R2、2016 和 2019 年在内的 Windows 服务器操作系统版本都有默认 Windows 更新设置可供下载和安装。您可以在扫描之前配置所需的设置。在更高版本的操作系统中，此操作可能会触发安装；请事先配置所需的行为。
- 通过提交服务请求，请求 AMS 运营团队进行验证：“用于评估补丁准备情况的 Amazon EC2 实例的 AWSManagedServices-CheckPatchingPrerequisites 自动化文档。”

Note

不会为操作系统不支持的实例创建补丁失败警报，也不会为在维护时段内停止的实例创建补丁失败警报。

补丁窗口

特定补丁组中的实例将在一个或多个补丁窗口内进行修补。补丁窗口按定义为 cron 或速率表达式的计划运行，并且具有可配置的持续时间，旨在将与修补相关的中断保持在选定的时间间隔内。AMS 建议创建多个补丁窗口，共同覆盖您的所有实例，以匹配您组织的特定修补例程，并使用默认维护窗口作为备用窗口。补丁窗口是使用 RFC 更改类型 Deployment | Patching | SSM 补丁窗口 | 创建 (ct-0e12j07llrxs7) 创建的。所有不属于补丁窗口的实例都将在入职期间创建的默认维护时段内进行修补。

通常，补丁窗口不需要更新以包含新实例。通常，这是通过修改实例标签来完成的。例如，考虑以下事件顺序：

1. 两个实例标有 AppId:MyApplication、Environment:Production、Group:1。

假设第一个标签密钥 = ，第二个标签密钥 = 环境，第三个标签密钥 = 组 AppId，并且创建了-Producti MyApplication on-1 补丁组的补丁窗口，则会在这些实例上生成一个标签。

2. 又创建了三个实例，并标有 AppId:MyApplication、Environment:Production、Group:1。

这将为补丁组生成一个标签：MyApplication-Production-1。

无需更改补丁窗口，因为它会在下次计划运行时选取所有五个实例。

有关使用此更改类型的更详细的讨论和演练，请参阅 [SSM 补丁窗口 | 创建](#)。

补丁通知

Important

从 2025 年 2 月 1 日起，AMS 客户将不再在其托管账户中收到补丁维护窗口为空的通知。

在补丁维护窗口开始之前，订阅的电子邮件地址（最多五个）会收到一封类似于以下内容的电子邮件：

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME was started at:
2020-02-21T12:02:18.196Z.
Details:
  Maintenance Window AccountId: YOUR_ACCOUNT_ID
  Maintenance Window Region:   YOUR_ACCOUNT_REGION
  Maintenance Window Id:       THE_MAINTENANCE_WINDOW_ID
  Maintenance Window Name:     THE_MAINTENANCE_WINDOW_NAME
  Maintenance Window Description: MaintenanceWindow for patching patch
  Group PATCH_GROUP_NAME
  Maintenance Window Patch Group: PATCH_GROUP_NAME
  Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
  InstanceId      InstanceName      StackId
  -----
  THE_INSTANCE_ID  THE_INSTANCE_NAME  THE_STACK_NAME

A follow-up message with a detailed report is sent as soon as the maintenance window is
over.

Please raise a service request if you have any inquires about AMS Patch Orchestrator by
following this URL:
https://console.aws.amazon.com/managedservices/servicerequest/new

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
```

补丁活动结束后，订阅的电子邮件地址会收到一封类似于以下内容的电子邮件：

```
Dear Customer,
```

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* ended at:
2020-02-21T12:03:20.058Z, with status: SUCCESS.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
Maintenance Window Region: *YOUR_ACCOUNT_REGION*
Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*
Maintenance Window Name: *THE_MAINTENANCE_WINDOW_NAME*
Maintenance Window Description: MaintenanceWindow for patching patch

Group *PATCH_GROUP_NAME*

Maintenance Window Patch Group: *PATCH_GROUP_NAME*
Maintenance Window ExecutionId: *THE_EXECUTION_ID*

Targets:

RfcId	InstanceId	InstanceName	StackId

Status

-----	-----	-----	-----

-----	-----	-----	-----

<i>THE_RFC_ID</i>	<i>THE_INSTANCE_ID</i>	<i>THE_INSTANCE_NAME</i>	<i>THE_STACK_NAME</i>
<i>STATUS</i>			

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

Please raise an Incident if an issue is impacting one of your production applications by following this URL:

<https://console.aws.amazon.com/managedservices/incident/new>

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

AMS 修补系统每 96 小时就会识别出这 96 小时内所有即将到来的补丁托管维护窗口，并向所有 96 小时内订阅的电子邮件地址发送提醒通知。这可能在窗口开始前一小时，或者整整96个小时。例如：

Dear Customer,

The AMS Patch Maintenance Window *THE_MAINTENANCE_WINDOW_NAME* will start at:
2020-05-06T16:35:36.523Z.

Details:

Maintenance Window AccountId: *YOUR_ACCOUNT_ID*
Maintenance Window Region: *YOUR_ACCOUNT_REGION*
Maintenance Window Id: *THE_MAINTENANCE_WINDOW_ID*


```

Maintenance Window Name:      THE_MAINTENANCE_WINDOW_NAME
Maintenance Window Description: MaintenanceWindow for patching patch
Group PATCH_GROUP_NAME
Maintenance Window Patch Group: PATCH_GROUP_NAME
Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z
Maintenance Window Schedule:   rate(24 hours)
Maintenance Window Timezone:    THE_TIMEZONE
At this time, these are the instances in the "PATCH_GROUP_NAME" Patch Group:
InstanceId      InstanceName      StackId      InstanceState
-----
THE_INSTANCE_ID  THE_INSTANCE_NAME  THE_STACK_NAME  running/stopped
THE_INSTANCE_ID  THE_INSTANCE_NAME  THE_STACK_NAME  running/stopped
THE_INSTANCE_ID  THE_INSTANCE_NAME  THE_STACK_NAME  running/stopped

```

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following this URL:

https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

If you would like to disable this maintenance window or you have inquires about the AMS Patch Orchestrator click on the following URL:

<https://console.aws.amazon.com/managedservices/servicerequest/new>

If you would like to delete this maintenance window, you can run the CT with id "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team

补丁基准

默认情况下，操作系统 (OS) 供应商提供的所有补丁都是使用 AMS 默认补丁基准安装的。如果要限制安装哪些补丁，则可以选择使用 RFC 更改类型部署 | 修补 | SSM 补丁基准 | 创建 **OS** (CT ID 因操作系统而异) 来创建补丁基准。

有关使用这些更改类型的信息，请参阅[修补子类别](#)。

补丁 Orchestrator 保留标签

Patch Orchestrator 还会生成以下无法修改的标签：

- **AMSPatch组**-此标签用于生成补丁组标签值。您不应修改群 AMSPatch组。如果要使用自定义“修补程序组”值，则可以修改“修补程序组”标签。Patch Orchestrator 会继续根据入职期间提供的标签键为 AMSPatch群组生成值，但如果您已将“补丁组”标签值设置为自定义值，则不会对其进行修改。要停止使用自定义“修补程序组”值，可以将“修补程序组”的值设置为与 AMSPatch组标签值相匹配。
- **AMSDefaultPatchGroup**— 此标签指示实例是否属于默认维护时段，其值为 True 或 False。如果未将实例的补丁组分配给维护时段，则此值将设置为 True。

按需修补

AMS 的更改类型适用于您的补丁基准，使您能够按需在实例上运行补丁。这可以是您在上线时设置的默认基准，也可以是您使用补丁基准更改类型设置的 Patch Orchestrator Systems Manager 补丁基准（CT ID 因操作系统而异）。

无论是否使用 Patch Orchestrator，您都可以使用按需修补更改类型。

有关使用此更改类型的信息，请参阅 On Demand Patching | [Run](#)。

Note

您不能在按需修补更改类型中使用属于 Auto Scaling 组的实例。

AMS 标准补丁

AMS 支持使用 AMS 标准修补模式的现有客户，但该模型不适用于新客户，现已停用，取而代之的是 AMS Patch Orchestrator。

AMS 标准补丁的典型补丁内容包括支持的操作系统的供应商更新以及预装在支持的操作系统（例如 IIS 和 Apache Server）中的软件。

在 AMS 入职期间，您可以指定修补要求、策略、频率和首选补丁窗口。这些配置意味着您可以避免为基础架构修补而同时使应用程序全部离线，因此您可以控制何时修补哪些基础架构。

 Note

本主题中描述的修补过程仅适用于您的堆栈。AMS 基础设施将在单独的过程中进行修补。AWS Managed Services 维护窗口 (或维护窗口) 为 AWS Managed Services (AMS) 执行维护活动，并在太平洋时间每个月的第二个星期四下午 3 点至下午 4 点重复。AMS 可能会在 48 小时通知后更改维护时段。您可以在入门时配置 AMS 补丁窗口，或者批准或拒绝每月补丁服务通知。

AMS 会定期扫描托管的 Amazon EC2 实例，寻找可通过操作系统更新功能获得的更新。我们还会定期更新我们环境中支持的 AMS 基础 Amazon 机器映像 (AMIs)。

经过验证后，AMS AMI 版本将与所有 AMS 账户共享。您可以使用 [DescribeImages](#) 亚马逊 EC2 API 调用或使用亚马逊 EC2 控制台查看可用的 AWS AMI 版本。要查找可用的 AMS AMIs，请参阅 [查找 AMI IDs、AMS](#)。

AMS 只有在您提出请求时才会执行临时修补计划。以前，AMS 会发送通知；目前，不发送通知。

 Note

默认情况下，AMS 使用 Systems Manager 来应用补丁，方法是让包管理器 (Linux) 或系统更新服务 (Windows) 查询其默认存储库以查看有哪些新软件包可用。如果您在 day-to-day 操作过程中使用默认的软件包管理器在 Linux 主机上安装了软件包，则该软件包管理器还会在该软件可用时为其提取新软件包。在这种情况下，您可能需要采取修补操作 (如本节所述) 来选择退出该实例。

支持的操作系统

支持的操作系统 (x86-64)

- Amazon Linux 2023
- 亚马逊 Linux 2 (预计 AMS 支持截止日期为 2026 年 6 月 30 日)
- 甲骨文 Linux 9.x、8.x
- 红帽企业 Linux (RHEL) 9.x、8.x
- SUSE Linux 企业服务器 15 SP6
- 适用于 SAP 15 SP3 及更高版本的 SUSE Linux 企业服务器

- 微软 Windows Server 2022、2019、2016
- Ubuntu 20.04、22.04、24.04

支持的操作系统 (ARM64)

- Amazon Linux 2023
- 亚马逊 Linux 2 (预计 AMS 支持截止日期为 2026 年 6 月 30 日)

支持的补丁

AWS Managed Services 主要支持操作系统级别的修补。安装的补丁可能因操作系统而异。

 Important

所有更新均从实例上配置的 Systems Manager 补丁基准服务远程存储库中下载，本主题后面将对此进行介绍。实例必须能够连接到存储库，才能执行修补。

要选择退出交付您想要自己维护的软件包的存储库的补丁基准服务，请运行以下命令来禁用存储库：

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

使用以下命令检索当前配置的存储库列表：

```
yum repolist
```

- Amazon Linux 预配置存储库 (通常是四个)：

存储库 ID	存储库名称
amzn-main/latest	amzn-Main-base
amzn-updates/latest	amzn-updates-base
epel/x86_64	适用于企业 Linux 6-x86_64 的额外软件包
pbis	PBIS 软件包更新

- 红帽企业 Linux 预配置存储库 (五个用于红帽企业 Linux 7 , 五个用于红帽企业 Linux 6) :

存储库 ID	存储库名称
rhi-Region-7/x86_64 client-config-server	红帽更新基础架构 2.0 客户端配置服务器
rhi-region-/7server/x86_64 rhel-server-releases	红帽企业 Linux 服务器 7
rhi-region-/7server/x86_64 rhel-server-releases	红帽企业 Linux 服务器 7 RH Common (RPMs)
epel/x86_64	适用于企业 Linux 7的额外软件包-x86_64
pbis	PBIS 软件包更新

存储库 ID	存储库名称
rhi-Region--6 client-config-server	红帽更新基础架构 2.0
RHUI 地区-rhel-server-releases	红帽企业 Linux 服务器 (6RPMs)
RHUI 地区-rhel-server-rh-common	红帽企业 Linux 服务器 6 RH Common (RPMs)
epel	适用于企业 Linux 6-x86_64 的额外软件包
pbis	PBIS 软件包更新

- CentOS 7 个预先配置的存储库 (通常是五个) :

存储库 ID	存储库名称
base/7/x86_64	centos-7-Base
updates/7/x86_64	Centos-7-最新消息
extras/7/x86_64	Centos-7-额外内容
epel/x86_64	适用于企业 Linux 7的额外软件包-x86_64

存储库 ID	存储库名称
pbis	PBIS 软件包更新

- 对于微软 Windows Server，所有更新都是使用 Windows 更新代理来检测和安装的，该代理配置为使用 Windows 更新目录（这包括来自微软更新的更新）。

在微软 Windows 操作系统上，补丁管理器使用微软的 cab 文件 wsusscn2.cab 作为可用操作系统安全更新的来源。此文件包含有关 Microsoft 发布的与安全相关的更新的信息。补丁管理器定期从 Microsoft 下载此文件，并使用它来更新可用于 Windows 实例的补丁集。此文件仅包含 Microsoft 确定与安全有关的更新。在处理文件中的信息时，Patch Manager 还会删除已被后续更新取代的更新。因此，Patch Manager 只显示最新更新，以供您安装。例如，如果 KB4 012214 替换 KB3135456，则补丁管理器中只有 KB4 012214 作为更新可用。

要了解有关 wsusscn2.cab 文件的更多信息，请参阅微软文章[使用 WUA 离线扫描更新](#)。

修补和基础架构设计

AMS 根据您的基础设施设计采用不同的修补方法：可变或不可变（有关详细定义，请参阅）。[AMS 关键术语](#)

对于可变基础架构，修补是使用传统的就地方法完成的，即由 AMS 运营工程师单独将更新直接安装到 Amazon EC2 实例。此修补方法用于不是 Auto Scaling 组且包含单个 Amazon EC2 实例或几个实例的堆栈。在这种情况下，替换实例或堆栈所基于的 AMI 会破坏自首次部署该系统以来对该系统所做的所有更改，因此事实并非如此。更新会应用于正在运行的系统，并且由于应用程序或系统重新启动，您可能会遇到系统停机（取决于堆栈配置）。这可以通过 Blue/Green 更新策略来缓解。有关更多信息，请参阅[Blue/Green 部署AWS CodeDeploy 简介](#)。

对于不可变的基础架构，修补方法是替换 AMI。不可变实例使用更新的 AMI 统一更新，该 AMI 取代了 Auto Scaling 组配置中指定的 AMI。AMS 版本 AMIs 每月更新（即已修补），通常是在补丁周二的那一周。下一节描述了其工作原理。

AMS 标准补丁的工作原理

AMS 使用 Systems Manager Run Command 服务进行每月定期补丁和根据需要进行关键修补，根据您的基础设施部署策略（可变与不可变），有两种主要的补丁方法，即就地和 AMI 替换。本节介绍 AMS 修补服务、类型、方法和流程。

AMS 定义了两种补丁类型，它们的计划方式不同：

- 关键补丁：在接受通知后，将尽快应用更新。
- 标准补丁：操作系统供应商定期更新，每月应用一次。

通过就地修补或 AMI 替换（根据要求）来应用补丁。

更新扫描

AMS 使用 [Amazon EC2 运行命令服务](#) 联系您的 Amazon EC2 堆栈并部署所需的扫描和修补脚本。AMS 使用已安装在支持的操作系统上的原生包管理组件在 Amazon EC2 堆栈上执行所有必需的扫描和修补行为。对于红帽和亚马逊 Linux，该服务使用 yum。对于 Windows，该服务使用 Windows 更新代理。

每天使用 [SSM 维护窗口](#) 和 AMS 默认 AWS RunPatchBaseline 文档执行扫描。使用适用于 Linux 和 Windows 的更新存储库对每个可访问的亚马逊 EC2 堆栈进行扫描。AMS 修补过程会检测所有可访问的 Amazon EC2 堆栈，然后以批处理方式执行扫描，这样即使在运行扫描时出现故障，堆栈也始终保持健康状态。然后保存每个 Amazon EC2 堆栈的扫描结果。

要查看堆栈或实例的扫描结果，请使用堆栈 ID 或实例 ID 提交服务请求。

默认 AMS 修补过程是安装所有可用的补丁，而不考虑补丁的分类或严重程度（例如，严重与标准）。唯一的例外是您已明确排除在堆栈中的补丁（不应排除 AMS 定义为必需的补丁）。

在建议的维护时段之前 14 天，您会收到一条修补服务通知。这使您有时间测试建议的补丁并接受或拒绝它们。如果您不回复修补服务通知，则您的实例不会被修补。当需要安装补丁时，AMS 会为每个堆栈创建一个更改请求 (RFC)，并且该 RFC 会出现在您账户的 RFC 列表中。

AMS 配置的维护时段和通知

通过配置 AMS 的补丁，每个账户都有每月维护时段，该窗口由您在注册账户时定义。AWS Managed Services 维护窗口（或维护窗口）为 AWS Managed Services (AMS) 执行维护活动，并在太平洋时间每个月的第二个星期四下午 3 点至下午 4 点重复。AMS 可能会在 48 小时通知后更改维护时段。

修补窗口不同。修补出站服务请求（也称为服务通知）包括建议的补丁窗口。

Note

有关回复修补服务通知的信息，请参阅 [您可以在 AMS 标准修补中采取的操作](#)

修补服务通知通过电子邮件发送到您账户中存档的联系人电子邮件地址。通知中包含一个指向 AWS Support 控制台的链接，您可以在其中进行回复。您也可以使用 AMS 服务请求页面回复通知。服务通知包括：

- 适用于堆栈的更新 IDs（CSUs IUs、和 OUs）列表以及您请求的那些更新不在修补范围内（如果有）。
- IDs 将受到影响的实例。
- 应用更新的建议修补窗口。您可以请求不同的修补窗口。
- 要求您接受建议的修补程序或要求提供更多信息。AMS 让您有时间测试更新的影响并批准或拒绝修补，或者要求排除特定的更新。如果您需要更多时间进行测试，并希望在测试后应用更新，请回复服务通知并描述您想要的内容，或者根据之前的 RFC 的详细信息提交新补丁 RFC 的服务请求。如果您根本不回复服务通知，则不会采取任何修补操作并取消 RFC。

如果您批准服务通知，AMS 将运行补丁 RFC，并根据服务承诺在商定的补丁窗口内应用更新。

修补完成后，AMS 会在服务请求中向您发送一封信件，其中包含修补活动结果（即成功或失败）的摘要。

就地修补

就地修补是指 AMS 登录到每个堆栈实例并应用补丁的方法。

使用运行支持的操作系统的 Amazon EC2 实例在可变基础设施上进行就地修补。修补将应用到目前为止所有可用的非排除更新。发布关键补丁时，还有一个额外的关键修补过程。

标准修补：就地修补

标准补丁按照补丁服务通知中建议的商定补丁计划进行，包括不被视为关键的定期补丁更新。

在提议的修补窗口之前，在您对通知的肯定回复后，将创建补丁 RFC 并显示在您的 RFC 控制面板中。

关键补丁：就地修补

当操作系统供应商发布关键安全更新时，AMS 会根据 AMS 服务承诺向您发送每个堆栈的服务通知（发送至您账户的联系人邮箱），从而通知您补丁 RFC。每次更新的服务通知均包含以下内容：

- 更新发布日期
- 更新重要性
- 更新详情（知识库参考等）

- IDs 受影响的堆栈数

您可以测试通知中列出的更新，并通过回复服务通知来批准或拒绝补丁。如果您批准该通知，则需要为每个堆栈提供一个特定的补丁窗口来安装更新。

 Note

在回复服务通知后 24 小时内的补丁窗口可能会根据可用容量重新安排。

如果您未在 10 天内回复或拒绝建议的修补，则补丁将被取消。

如果您想在允许的期限（通知中提供）之后应用更新，请根据之前通知的详细信息提交服务请求以获取新的补丁计划。

如果您批准服务通知，AMS 将根据服务承诺在您指定的补丁窗口内应用更新。

如果有多个更新，则可以在对服务通知的响应中指定要排除的更新，从而将特定更新排除在补丁之外。

AMS 会针对每个堆栈向您发送服务通知，告知每次更新的结果（即成功或失败）。

AMI 更新修补程序（使用为 Auto Scaling 群组打过 AMIs 的补丁）

AMI 替换补丁是通过更新配置为在 Auto Scaling 组中部署新 Amazon EC2 实例的 AMI ID 在不可变基础设施上完成的。

对于支持的操作系统，Amazon 系统映像 (AMIs) 会定期发布。操作系统供应商会定期发布新补丁。AMS 采用亚马逊提供的 AMI，使用最新补丁对其进行更新，然后添加相应的组件使其能够在 AMS 环境中运行。然后，它通过将新的 AMS AMI 共享给账户，向所有 AMS 客户提供该新的 AMS AMI。使用这些新发布的 AMS，可以每月刷新您的 Auto Scaling 群组堆栈。AMIs 下图说明了如何在 AMIs 您的环境中使用 AMS。

Auto Scaling 组根据为 Auto Scaling 组配置的 AMI 创建其实例。AMS 共享更新后 AMIs，根据您的管理 AMI 更新的方式，您可以选择以下选项：

- 如果您使用的是应用程序部署工具（例如 UserData CodeDeploy、等），该工具可在实例创建后自动对其进行自定义，则可以执行以下操作：
 - 回复修补服务通知或提交服务请求，要求使用最新的 AMS AMI 来替换您当前 Auto Scaling 组的配置 AMI。替换 Auto Scaling 组配置中的 AMI ID 后，AMS 将开始对您的实例进行滚动更新，并

且您的 Auto Scaling 组实例配置（例如，安装应用程序、启动脚本等）将自动应用于使用新 AMS AMI 创建的新实例。

- 如果您在 Auto Scaling 组的配置中使用 custom/golden AMI，则可以：
 - 使用新的 AMS AMI 创建实例，自定义该实例并创建新的金色 AMI。使用亚马逊 EC2 控制台与 AMS 共享新的黄金 AMI，然后向 AMS 提交服务请求，更新您的 Auto Scaling 组的配置以使用新的自定义 AMI。
 - 使用亚马逊 EC2 控制台与 AMS 共享您现有的金色 AMI，并提交服务请求，让 AMS 更新您的金色 AMI。为此，AMS 会根据您的黄金 AMI 创建一个实例，将补丁应用于该实例，为您创建一个新的黄金 AMI，然后更新您的 Auto Scaling 组的配置以使用新的 AMI。这里的缺点是 AMS 无法测试您的新自定义 AMI 是否按照您想要的方式运行。相反，在创建新的金色 AMI、共享该实例并请求 AMS 更新您的 Auto Scaling 群组之前，您应该测试使用新 AMI 创建的实例并验证一切是否正常。AMS 不建议使用此选项。

标准修补：AMI 更新

AMS 每个月都会发布新的 Amazon 系统映像 (AMIs)，其中包含服务改进和适用于的新补丁 AMIs。

Note

更新后 AMIs 的 AWS 将在周二补丁之后生成新的 AMS AMIs。然后，AMS 会在提供它们之前对其进行测试。新的 AMIs 通过测试后，AMS 的股票更新 AMIs 为托管账户。

关键补丁：AMI 更新

在需要时，AMS 会提供自上次月度 AMI 发布以来发布的关键安全补丁的 AMIs 更新。

对不可变基础设施进行关键安全更新的流程与不可变基础设施的每月 AMI 流程相同，唯一的不同的 AMS AMI 是在正常计划（补丁星期二）之外创建的，这是基于新的关键更新的发布。根据您的账户定义的服务级别协议 (SLAs)，AMS 提供带有关键安全补丁的新 AMI。AMS 仅根据请求更新 Auto Scaling 群组。使用服务请求提交 AMI 更换请求。

AMS 标准修补失败

如果更新失败，AMS 会进行分析以了解失败的原因，并将分析结果传达给您。如果故障归因于 AMS，则如果更新在维护时段内，我们会重试更新。否则，AMS 会为失败的实例更新创建服务通知并等待您的指示。

对于归因于您的系统的故障，您可以提交带有新补丁 RFC 的服务请求来更新实例。

您可以在 AMS 标准修补中采取的操作

除了测试新版本外 AMIs，您还可以采取以下几项措施来管理基础架构的修补：

- 如果测试更新的时间超过了补丁窗口允许的时间，您可以通过提交服务请求（使用原始服务通知中的详细信息作为基础），请求 AMS 应用在您准备就绪时取消的更新。
- 您可以提交服务请求，提供更新列表、适用实例和其他相关详细信息，从而请求在下一个自动更新窗口之前应用重要更新 (IU) 或其他更新 (OU)。由于这个 CT 不是自动的，因此需要更长的时间来安排和运行。检查相应时间的服务级别目标 (SLOs)。有关更多信息，请参阅 [AMS 服务级别目标 \(SLOs\)](#)。

此外，您还可以使用现有的、已修补的 AMS AMIs 来创建自定义 AMIs。有关信息，请参阅 [AMI | 创建](#)。

Note

在下一个维护时段之前，您不能根据重要更新或其他更新请求新的 AMS AMI，因为 AMS AMI 的发布流程遵循统一的节奏，以造福所有 AMS 客户。

改变 patched/opting 出来的东西

在 AMS 配置了修补后，在您对修补服务通知的响应或服务请求中，您可以更改要修补的资源。您可执行以下操作：

- 为每个堆栈和每个操作系统定义应排除在补救范围之外的补丁列表。
- 定义应从某些补丁或所有修补程序中排除的资源列表。
- 定义应始终排除在所有修补程序之外的资源列表。
- 定义应在某一天和特定时间修补的资源列表（如果您尚未定义维护时段，则不错）。

要排除一个或多个补丁，请使用下文提供的模板提交服务请求或回复修补服务通知。不要提交 RFC。在请求中包含您想要排除的一个或多个补丁名称以及原因。在服务请求中包含此信息，如下所示：

- 名称：补丁的名称。对于 Windows 补丁，这是知识库名称，例如 KB3145384。对于 Linux 补丁，这是软件包名称，例如 openssh-6.6.1p1-25.61.amzn1.x86_64。

- 原因：一条注释，说明为什么要排除补丁。
- 到期时间：排除的 date/time 到期时间。

如果已安装排除的修补程序，则将其删除。

如果排除这些补丁会带来重大安全风险，运营商将对请求进行审查，运营商将与您讨论。除外补丁的到期日期也需要协商。在商定的到期日期之后，排除将过期，并且该修补程序将安装在任何后续补丁中。

如果适用，排除列表中的补丁仍会在扫描结果中返回。

 Note

与 Windows 不同，Linux 补丁是特定版本的。这种区别很重要，因为排除的修补程序的新版本不会被自动排除在外。如果你想这样做，你有责任通知 AMS 排除新版本的 Linux 补丁。

补丁服务通知回复模板

您必须使用指定的格式回复修补服务通知，才能对您的实例执行修补。如果您尚未使用 AMS 设置维护时段，则应执行此操作。

回复服务通知时，请使用给定的格式。

如果未设置维护时段，请告诉我们何时需要修补内容，如下所示：

UTC	StartTime	StackId	InstanceId (Optional)
2019-04-01	15:00	stack-123456789012	i-1234566789
2019-04-01	15:00	stack-123456789013	i-1234566784
2019-04-01	15:00	stack-123456789014	i-1234566783
2019-04-01	15:00	stack-123456789015	i-1234566782

如果您设置了维护时段，并且希望将某些资源排除在某些补丁之外，请使用以下格式：

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	<i>PATCH</i>
stack-123456789013	i-1234566784	<i>PATCH</i>
stack-123456789014	i-1234566783	<i>PATCH</i>
stack-123456789015	i-1234566782	<i>PATCH</i>

如果您设置了维护时段，并且希望始终将某些资源排除在所有补丁之外，请使用以下格式：

StackId	InstanceId (Optional)	Exclude Patches
stack-123456789012	i-1234566789	ALL
stack-123456789015	i-1234566782	ALL

为修补做准备

为了让您的环境做好自动修补准备，我们建议您采取以下措施：

- 请确保您有要修补的所有实例的完整清单。
- 作为业务连续性战略的一部分，请确保定期备份您的资源。其他备份是作为补丁序列的一部分创建的，这些备份会根据您配置的 Patch Orchestrator 保留策略（默认为 60 天）自动删除。
- 确保所有相关许可证都是最新的。
- 修改堆栈维护窗口以错开修补程序，以便在生产堆栈之前先修补测试堆栈。这样，任何修补错误都可以在测试堆栈中找到，并且可以在修补生产堆栈之前进行识别。

查看补丁设置

要了解您当前的修补配置是什么，可以执行以下操作：

- 使用查询向 AMS 提交服务请求。
- 等待补丁服务通知。修补通知会告知您要应用的所有补丁和要修补的实例，还会建议您设置一个补丁窗口。

您可以提交服务请求来修改以下内容：

- 扫描间隔：在此堆栈的实例上执行合规性扫描之间的间隔时间，以分钟为单位。

默认为240（4 小时）。
- NotificationWindow：应在计划更改（补丁）之前多长时间（以分钟为单位）将通知发送给您。默认为10080（7 天）。

AMS 标准补丁 FAQs

本节提供一些常见问题的答案。

- 问：如何选择不在全球范围内修补？

答：要全局选择退出修补，请提交服务请求。请注意，您不能选择退出 AMS 强制补丁。将继续扫描所有堆栈，以便我们可以报告漏洞。

- 问：如何将特定的堆栈排除在修补之外？

答：要将特定堆栈永久排除在修补之外，请提交服务请求。要将某些堆栈排除在特定的补丁周期之外，请在即将发布的补丁通知中列出要排除的堆栈列表。有关信息，请参阅[改变 patched/opting 出来的东西](#)。请注意，您不能选择退出强制补丁。

- 问：如果我不批准修补服务通知会怎样？

答：您有 14 天的时间来批准标准补丁服务请求，有 10 天的时间来批准重要的补丁通知。如果您未在这段时间内批准服务请求，则服务承诺将失效，并且不会进行修补。在强制修补的情况下，无论对服务请求的响应如何，都会应用补丁。

- 问：如何将特定的修补程序和软件包排除在安装范围之外？

答：要永久排除特定的补丁或软件包，请提交服务请求。要将某些补丁或软件包排除在特定的补丁周期之外，请在即将发布的补丁通知中列出要排除的补丁或软件包列表。有关更多信息，请参阅[改变 patched/opting 出来的东西](#)。请注意，您不能选择退出强制补丁。

- 问：如果系统因修补而出现故障，会发生什么？

答：AMS 监控每个系统。AMS 会向您发送服务通知，告知每个堆栈和实例的每次更新结果（即成功或失败）。如果检测到故障，AMS 会进行调查，努力恢复实例，然后 AMS 运营工程师会尝试手动修补。有关信息，请参阅[AMS 标准修补失败](#)。

- 问：AMS 管理哪些更新？

答：AMS 管理供应商通知 AMS 的操作系统级更新。有关更多信息，请参阅[支持的补丁](#)。

- 问：哪些更新不由 AMS 管理？

- 答：应用程序级更新不由 AMS 管理。
- 问：Auto Scaling 群组是如何更新的？

答：Auto Scaling 组将使用 Auto Scaling 组配置中的 AMI 替代品进行更新，然后进行滚动更新。滚动更新会观察您的修补配置 HealthyHostThreshold 设置，该设置决定了堆栈中有多少个 Amazon EC2 实例在修补期间必须保持活动状态。有关更多信息，请参阅 [AMI 更新修补程序（使用为 Auto Scaling 群组打过 AMIs 的补丁）](#)。
- 问：如何在正常周期之外安装更新？

答：对于要在正常修补计划之外安装的操作系统级更新，请使用收到的修补通知提交服务请求。如果您对建议补丁的测试时间超过 21 天（对于标准补丁）或 14 天（对于关键补丁），则可能会发生这种情况。Out-of-band 可以就地为独立的 Ama EC2 zon 实例进行修补。
- 问：如何修补新部署的堆栈或实例？

答：在创建新的 Amazon EC2 堆栈实例或 Auto Scaling 组时，您应始终指定最新的 AMS AMI，该 AMS AMI 上已经有最新的补丁。对于可变基础架构，应在部署堆栈后立即执行内联修补。

修补服务承诺

根据您的基础设施部署类型和更新的重要性，我们为可变和不可变基础架构的关键安全更新以及可变和不可变基础设施的重要更新提供服务承诺。

标准修补

这些是针对标准修补的 AMS 服务承诺。

标准修补、可变基础架构（就地修补）

事件/动作	服务承诺衡量
重要更新将在一个月内发布。	时钟开始

事件/动作	服务承诺衡量
在创建标准补丁通知后的十四天内，AMS 将通过服务通知和电子邮件通知您即将进行的每个堆栈的修补计划。服务通知包括： • 适用于堆栈 IDs（需要 CSUs 和未应用 IUs）的更新（和）列表，以及不在修补范围内的更新 • IDs 受影响的堆栈数 • 应用更新的维护时段	发送服务通知后，时钟停止。
您可以测试更新的影响，然后批准或拒绝 RFC。如果您未在 14 天内回复，或者在回复服务通知时拒绝了补丁，则不会采取任何措施。 如果您的测试时间超过 14 天，并且希望在 14 天期限之后应用更新，请根据之前的 RFC 的详细信息提交新补丁 RFC 的服务请求。	如果您未在 14 天内批准或回复，则待处理的更改将被取消，且更新的服务承诺不适用。
如果您在 14 天内批准服务通知，AMS 将应用更新。 您可以通过在对服务通知的回复中指定要排除的更新来选择从 RFC 中排除特定更新。	如果您在收到服务通知后 14 天内批准服务通知，则时钟将开始。尝试安装更新后，时钟停止。
AMS 会向您发送服务通知，告知您每次尝试更新的结果。服务通知包括以下详细信息： • 亚马逊 EC2 实例 ID • 更新 1 成功/失败：ARN a1、ARN a2... • 更新 2 成功/失败：ARN b1、ARN b2... • 更新 N 成功/失败：ARN c1、ARN c2...	不适用。

事件/动作	服务承诺衡量
如果更新失败，AMS 会进行分析以了解失败的原因，并将分析结果传达给您。如果故障归因于 AMS，AMS 将在维护时段内重试更新，否则 AMS 会为失败的实例更新组合创建服务通知，并在维护时段等待您的指示。	不适用。
对于归因于您的故障，请提交服务请求以获取新的补丁 RFC 以更新实例。	不适用。

关键补丁

这些是针对关键安全更新的AMS服务承诺。

关键安全更新、可变基础架构

事件/动作	服务承诺衡量
科罗拉多州立大学获释。	时钟开始
AMS 通过每个堆栈的服务通知 (还会发送一封电子邮件) 通知您补丁 RFC。服务通知包括： - 更新发布日期 - 更新重要性 - 更新详情：KB 参考文献等 - IDs 受影响的堆栈数	发送服务通知后，时钟停止。
您可以测试 RFC 中列出的更新，并在 10 天内通过回复服务通知来批准或拒绝 RFC。	如果您未在 14 天内批准或回复，则待处理的变更将被取消，并且该更新的服务承诺不适用。
您可以为安装更新提供特定的维护时段 (每个堆栈)。在服务通知得到答复后 24 小时内指定的维护时段可能会根据可用容量重新安排。	
如果您未在 10 天内回复，或者拒绝补丁 RFC，则待处理的操作将被取消。	

事件/动作	服务承诺衡量
如果您想在 14 天后应用更新，请根据之前的 RFC 的详细信息提交新补丁 RFC 的服务请求。	
如果您批准服务通知，AMS 就会应用更新。 对于多个更新，您可以通过在对服务通知的响应中指定要排除的更新来选择将特定更新排除在更改之外。	如果所需的维护时段不在服务承诺时间范围内，则只有当 RFC 未在所需的维护时段内运行时，才会错过更新的服务承诺。
AMS 会向您发送服务通知，告知所应用的每次更新的结果。服务通知包括以下详细信息： • 亚马逊 EC2 实例 ID • 更新成功：ARN a1、ARN a2... • 更新失败：ARN c1、ARN c2...	不适用。
如果更新失败，AMS 会进行分析以了解失败的原因，并将分析结果传达给您。如果故障归因于 AMS，AMS 将在维护时段内重试更新，否则 AMS 会为失败的实例更新组合创建服务通知，并在新的维护窗口中等待您的指示。	不适用。
对于归因于您的故障，请提交服务请求以获取新的补丁 RFC 以更新实例。	不适用。

关键安全更新、不可变的基础架构

事件/动作	服务承诺衡量
科罗拉多州立大学获释。	时钟开始
AMS 通过服务通知通知您以下信息： • 更新发布日期 • 更新重要性 • 更新详细信息（知识库参考等）	时钟继续运转。

事件/动作	服务承诺衡量
- AMS Amazon 机器映像 (AMI) 受到影响 - 新更新的预计发布日期和时间 AMIs	
AMS 版本已 AMIs 在托管账户中更新。	时钟停止。
如果您批准服务通知，AMS 就会应用更新。 AMS 会通过服务通知和电子邮件通知您账户中 AMIs 共享的内容。	不适用。
如果测试新的 AMIs 时间超过了分配的时间（一周），则可以向 AMS 提交服务请求，要求使用新的 AMS AMI（按原样）更新您的 Auto Scaling 群组。如果您想使用您的配置修改新的 AMS AMI，请使用带有管理 其他 其他 更新 CT (ct-0xdawir96cy7k) 的 RFC 请求我们更新您的 Auto Scaling 组。	不适用。

报告和选项

AWS Managed Services (AMS) 整理来自各种原生 AWS 服务的数据，以提供有关主要 AMS 产品的增值报告。

AMS 提供两种类型的详细报告：

- **根据请求报告**：您可以通过云服务交付管理器 (CSDM) 临时请求某些报告。这些报告没有限制，因为在入职或关键事件期间，您可能需要多次请求这些报告。但是，请注意，这些报告并不是为了像每周报告那样按计划提供的。要更好地了解您的需求或了解有关使用自助报告的更多信息，请联系您的 CSDM。
- **自助报告**：AMS 自助服务报告允许您根据需要随时直接查询和分析数据。使用自助服务报告从 AMS 控制台访问报告，并通过 S3 存储桶（每个账户一个存储桶）报告数据集。这使您可以将数据集集成到您最喜欢的商业智能 (BI) 工具中，以便您可以根据自己的要求自定义报告。

主题

- [应要求报告](#)
- [自助报告](#)

应要求报告

主题

- [AMS 补丁报告](#)
- [AMS Backup 报告](#)
- [“已防止的事件和监控热门话题者”报告](#)
- [账单费用明细报告](#)
- [可信修正者报告](#)

AMS 整理来自各种原生 AWS 服务的数据，以提供有关主要 AMS 产品的增值报告。要获取这些报告的副本，请向您的云服务交付经理 (CSDM) 提出申请。

AMS 补丁报告

可用报告

- [补丁实例详细信息摘要报告](#)
- [补丁详细信息报告](#)
- [错过补丁的实例报告](#)
- [修补 SSM 覆盖率报告](#)

补丁实例详细信息摘要报告

补丁实例详细信息摘要报告提供了为已加入报告的实例收集的实例详细信息。这是一份信息报告，可帮助识别所有已加载的实例、账户状态、实例详细信息、维护时段覆盖范围、维护时段执行时间、堆栈详细信息和平台类型。该报告提供以下内容：

1. 有关账户生产和非生产实例的数据。注意：生产和非生产阶段源自账户名，而不是实例标签。
2. 按平台类型划分的实例分布数据。注意：“N/A”平台类型是 AWS Systems Manager 指无法检索平台信息。
3. 有关实例状态分布以及正在运行、停止或终止的实例数量的数据。

字段名	定义
报告日期时间	报告的生成日期和时间。
账户编号	实例 ID 所属的 AWS 账户 ID
账户名	AWS 账户名称
生产账户	AMS prod、非生产账户的标识符，具体取决于账户名称是否包含值“PROD”、“NONPROD”。 示例：PROD、NONPROD、不可用
账户状态	AMS 账户状态。例如：活动、非活动
AMS 账户服务承诺	溢价，再加上
着陆区	标记账号着陆区域类型。例如：MALZ、NON-MALZ
访问限制	访问受限的地区。例如：美国土壤

字段名	定义
实例 ID	EC2 实例的 ID
实例名称	EC2 实例名称
实例平台类型	操作系统 (OS) 类型。例如：Windows、Linux 等等
实例平台名称	操作系统 (OS) 名称。例如：Microsoft WindowsServer2012R2Standard，RedHatEnterpriseLinuxServer
堆栈名称	包含实例的堆栈名称
堆栈类型	AMS 堆栈（客户账户中的 AMS 基础架构）或客户堆栈（支持客户应用程序的 AMS 托管基础架构）。示例：AMS、客户
自动扩缩组名	包含实例的 Auto Scaling 组 (ASG) 的名称
实例补丁组	修补组名称用于将实例分组在一起并应用相同的维护时段。如果未分配补丁组，则该值将为“未分配”
实例补丁组类型	补丁组类型。 默认：默认补丁组，具有默认维护时段，由实例上的AMSDefaultPatchGroup:True 标签确定。 客户：客户创建的补丁组。 未分配：未分配补丁组
实例状态	EC2 实例生命周期内的状态。示例：已终止、正在运行、正在停止、已停止、正在关闭、待处理。 有关更多信息，请参阅实例生命周期。

字段名	定义
维护时段覆盖范围	此实例上是否有 future 维护时段。示例：已覆盖或未覆盖
维护时段执行日期/时间	下次预计会执行维护时段。如果为 NULL，则为单窗口执行，即不重复执行

补丁详细信息报告

AWS Managed Services (AMS) 补丁详情报告提供了各种实例的补丁详情和维护时段覆盖范围，包括：

- 1. 有关补丁组及其类型的数据。
- 2. 有关维护时段、持续时间、截止时间、维护时段执行的 future 日期（计划）以及每个窗口中受影响的实例的数据。
- 3. 账户下所有操作系统的数据以及安装该操作系统的实例数量。

字段名	定义
报告日期时间	报告的生成日期和时间。
账户 ID	实例 ID 所属的 AWS 账户 ID
账户名	AWS 账户名称
实例 ID	EC2 实例的 ID
生产账户	AMS prod、非生产账户的标识符，具体取决于账户名称是否包含值“PROD”、“NONPROD”。如果数据不可用，则值将为“不可用”
账户状态	AMS 账户状态。例如：活动、非活动
实例平台类型	操作系统 (OS) 类型。例如：Windows、Linux

字段名	定义
实例平台名称	操作系统 (OS) 名称。例如：Microsoft WindowsServer2012R2Standard，RedHatEnterpriseLinuxServer
堆栈类型	AMS 堆栈（客户账户中的 AMS 基础架构）或客户堆栈（支持客户应用程序的 AMS 托管基础架构）。例如：AMS、客户
实例补丁组	修补组名称用于将实例分组在一起并应用相同的维护时段。如果未分配补丁组，则该值将为“未分配”
实例补丁组类型	补丁组类型。 默认：默认补丁组/默认维护时段，由实例上的 AMSDefaultPatchGroup:True 标签确定 客户：客户创建的补丁组 未分配：未分配任何补丁组
实例状态	EC2 实例生命周期内的状态。例如：已终止、正在运行、正在停止、已停止、正在关闭、待处理 有关更多信息，请参阅实例生命周期。
维护时段 ID	维护时段标识符
维护窗口状态	可能的值为“启用”或“禁用”。
维护窗口类型	维护窗口类型
维护时段下次执行日期时间	下次预计会执行维护时段。如果为 NULL，则为单窗口执行，即不重复执行
上次执行维护窗口	最近一次执行维护时段的时间

字段名	定义
维护时段持续时间 (小时)	维护时段的持续时间 (以小时为单位)
维护时段覆盖范围	维护时段覆盖范围
补丁基准 ID	当前附加到实例的补丁基准
补丁状态	总体补丁合规性状态。例如：合规、不合规。如果至少缺少一个补丁，则认为实例不合规，否则视为合规。
合规-总计	合规补丁数量 (所有严重性)
不合规-合计	不合规补丁数量 (所有严重性)
合规-关键	严重性为“严重”的兼容补丁数量
合规-高	严重性为“高”的兼容补丁数量
合规-中等	严重性为“中等”的兼容补丁数量
合规-低	严重性为“低”的兼容补丁数量
合规-信息性	严重性为“信息”的兼容补丁数量
合规-未指定	严重性为“未指定”的兼容补丁数量
不合规-严重	严重性为“严重”的不合规补丁数量
不合规-高	严重性为“高”的不合规补丁数量
不合规-中等	严重性为“中等”的不合规补丁数量
不合规-低	严重性为“低”的不合规补丁数量
不合规-信息性	严重性为“信息性”的不合规补丁数量
不合规-未指定	严重性为“未指定”的不合规补丁数量

错过补丁的实例报告

AWS Managed Services (AMS) 错过补丁的实例报告提供了在上次执行维护时段期间错过补丁的实例的详细信息，包括：

- 1. 补丁 ID 级别的缺失补丁数据。
- 2. 有关至少缺少一个补丁的所有实例的数据，以及补丁严重性、未修补天数、补丁范围和发布日期等属性。

字段名	定义
报告日期时间	报告的生成日期和时间。
账户 ID	实例 ID 所属的 AWS 账户 ID
账户名	AWS 账户名称
生产账户	AMS prod、非生产账户的标识符，具体取决于账户名称是否包含值“PROD”、“NONPROD”。
账户状态	AMS 账户状态。例如：活动或非活动
AMS 账户服务等级	高级版或升级版
实例 ID	EC2 实例的 ID
实例平台类型	操作系统 (OS) 类型。例如：Windows
实例状态	EC2 实例生命周期的状态。 例如：已终止、正在运行、正在停止、已停止、已关闭、待处理有关更多信息，请参阅实例生命周期。
补丁 ID	已发布补丁的 ID。例如：KB3172729
补丁严重性	每个发行商的补丁严重程度。例如：严重、重要、中等、低、未指定
补丁分类	每个发行商的补丁分类。例如：关键更新、安全更新、更新汇总、更新、功能包

字段名	定义
补丁发布日期时间 (UTC)	每个发行商的补丁发布日期
补丁安装状态	每个 SSM 在实例上安装补丁状态。例如：已安装、缺失、不适用
未修补的天数	自上次 SSM 扫描以来实例未修补的天数
未修补天数范围	有好几天没有修补。例如：<30 天、30-60 天、60-90 天、90 天以上

修补 SSM 覆盖率报告

AMS Patching SSM 覆盖率报告会告知您账户中的 EC2 实例是否安装了 SSM 代理。

字段名	定义
客户姓名	有多个子客户时的客户名称
资源区域	AWS 资源所在的区域
帐户名称	账户的名称
AWS 账户编号	AWS 账户的 ID
资源 ID	EC2 实例的 ID
资源名称	EC2 实例名称
合规标志	表示资源是否安装了 SSM 代理（“合规”）（“不兼容”）

AMS Backup 报告

可用报告

- [Backup Job 成功/失败报告](#)
- [Backup 摘要报告](#)

- [Backup Summary/Coverage 报告](#)

Backup Job 成功/失败报告

Backup Job Success/Failure 报告提供了有关过去几周内运行的备份的信息。要自定义报告，请指定要检索数据的周数。默认周数为 12。下表列出了报告中包含的数据：

字段名	定义
AWS 账户 ID	资源所属的 AWS 账户 ID
账户名	AWS 账户名称
Backup Job ID	Backup 任务的 ID
资源 ID	备份资源的 ID
资源类型	正在备份的资源类型
资源区域	已备份资源的 AWS 区域
Backup 状态	备份的状态。有关更多信息，请参阅 Backup 作业状态
恢复点 ID	恢复点的唯一标识符
状态消息	备份作业期间发生的错误或警告的描述
Backup 大小	备份的大小（以 GB 为单位）
恢复点 ARN	创建的备份的 ARN
恢复点年限（以天为单位）	自恢复点创建以来已过去的天数
未满 30 天	少于 30 天的备份指示器

Backup 摘要报告

字段名	定义
客户姓名	多个子客户所在情况的客户名称
Backup 月	备份月份
Backup 年份	备份年份
资源类型	正在备份的资源类型
资源数量	已备份的资源数量
恢复点数	不同快照的数量
备份时间不足 30 天	少于 30 天的备份数量
最大恢复点使用年限	以天为单位的最早恢复点年龄
最小恢复点使用年限	最近的恢复点年限 (以天为单位)

Backup Summary/Coverage 报告

Backup Summary/Coverage 报告列出了当前有多少资源未受任何 AWS Backup 计划保护。与您的 CDSM 讨论适当的计划，以尽可能增加覆盖范围并降低数据丢失的风险。

字段名	定义
客户姓名	多个子客户所在情况的客户名称
区域	AWS 资源所在的区域
帐户名称	账户的名称
AWS 账户编号	AWS 账户的 ID
资源类型	资源类型。资源由 AWS Backup (Aurora、D ocu mentDB、DynamoDB、EBS、 、EFS、RD EC2 S 和 S3) 提供支持 FSx

字段名	定义
资源 ARN	资源的 ARN
资源 ID	资源的 ID
覆盖范围	表示资源是否被覆盖（“已覆盖”或“未覆盖”）
资源数量	账户中支持的资源数量
perc_coverage	过去 30 天内执行过备份的受支持资源的百分比。

“已防止的事件和监控热门话题者” 报告

可用报告

- [已阻止的事件报告](#)
- [监控 Top Talkers 报告](#)

已阻止的事件报告

“已阻止的事件” 报告列出了自动补救的 Amazon CloudWatch 警报，以防止可能发生的事件。要了解更多信息，请参阅[自动修复](#)。下表列出了此报告中包含的信息：

字段名	定义
execution_start_time_time_	执行自动化的日期
customer_name	账户客户姓名
account_name	账户的名称
AwsAccountId	AWS 账户的 ID
文档_名称	已执行的 SSM 文档或自动化的名称
持续时间（以分钟为单位）	自动化的时长（以分钟为单位）

字段名	定义
区域	AWS 资源所在的区域
自动化_执行_id	执行的 ID
自动化执行状态	执行的状态

监控 Top Talkers 报告

监控 Top Talkers 报告显示了在特定时间段内生成的 Amazon CloudWatch 警报数量，并提供了生成最多警报数量的资源的可视化效果。此报告可帮助您识别生成警报数量最多的资源。这些资源可能是执行根本原因分析以修复问题或修改警报阈值以防止在没有实际问题时出现不必要的触发的候选资源。下表列出了此报告中包含的信息：

字段名	定义
客户名称	客户姓名
AccountId	AWS 账户的 ID
警报类别	触发的警报类型
说明	警报的描述
资源 ID	触发警报的资源的 ID
资源名称	触发警报的资源的名称
区域	AWS资源所在的区域
事件状态	警报生成的事件的最新状态
第一次出现	警报第一次被触发
最近发生的事件	最近一次触发警报的时间
警报计数	在第一次和最近一次发生之间生成的警报数量

账单费用明细报告

AWS Managed Services (AMS) 账单费用详情报告提供了有关关联账户和相应的 AWS 服务的 AMS 账单费用的详细信息，包括：

- AMS 服务级别费用、提升百分比、账户级 AMS 服务等级和 AMS 费用。
- 关联账户和 AWS 使用费

字段名	定义
账单月份	服务计费的月份和年份
付款人账户 ID	用于识别将负责支付 AMS 费用的账户的 12 位数身份证
关联账户 ID	用于标识使用产生费用的服务的 AMS 账户的 12 位数字 ID
AWS 服务名称	使用的 AWS 服务
AWS 收费	服务名称中列出的 AWS 服务名称的 AWS AWS 费用
定价计划	与关联账户关联的定价计划的名称
上升比例	基于 pricing_plan、SLA 和 AWS 服务的提升百分比 (以十进制 V.WXYZ 表示)
调整后的 AWS 费用	AWS 已针对 AMS 调整使用量
AWS 费用上调	对 AMS 收取的 AWS 费用百分比 ; $adjusted\_aws\_charges * uplift\_percent$
实例 EC2 RDS 支出	在 RDS 实例上 EC2 花钱
AMS 费用	该商品的 AMS 费用总额 ; $uplifted\_aws\_charges + instance\_ec2\_rds\_spend + uplifted\_ris + uplifted\_sp$

字段名	定义
按比例分配的最低费用	我们为满足合同最低要求而收取的金额
最低费用	AMS 最低费用 (如果适用)
关联账户 AMS 费用总额	关联账户的所有费用总和
付款人账户 AMS 费用总额	付款人账户所有费用的总和

可信修正者报告

可用报告

- [可信修正者修正摘要报告](#)
- [可信修正者配置摘要报告](#)
- [Trusted Advisor 查看摘要报告](#)

可信修正者修正摘要报告

“可信修正者修正状态”报告提供有关在先前修正周期中发生的修正的信息。默认周数为 1。要自定义报告，请根据您的补救计划指定周数。

字段名	定义
日期	收集数据的日期。
账户 ID	资源所属的 AWS 账户 ID
账户名	AWS 账户名
检查类别	支 AWS Trusted Advisor 票类别
检查姓名	已修正 Trusted Advisor 的检查的名称
检查 ID	已修正的 checks 的 Trusted Advisor ID
执行模式	为特定 Trusted Advisor 检查配置的执行模式

字段名	定义
OpsItem 身份证	为修复而 OpsItem 创建 Trusted Advisor 的 ID
OpsItem 状态	报告时 OpsItem 创建者的 Trusted Advisor 状态
资源 ID	为修复而创建的资源的 ARN

可信修正者配置摘要报告

“可信修正者配置摘要” 报告提供有关每 Trusted Advisor 项检查的当前可信修正者修正配置的信息。

字段名	定义
日期	收集数据的日期。
账户 ID	配置适用的 AWS 账户 ID
账户名	AWS 账户名
检查类别	支 AWS Trusted Advisor 票类别
检查姓名	配置适用的已修正 Trusted Advisor 检查的名称
检查 ID	配置适用的已修正 Trusted Advisor 检查的 ID
执行模式	为特定 Trusted Advisor 检查配置的执行模式
改写为“自动”	标签模式（如果已配置）将执行模式改为“自动”
改为手动	标签模式（如果已配置）将执行模式改为手动

Trusted Advisor 查看摘要报告

支 Trusted Advisor 票摘要报告提供有关当前 Trusted Advisor 支票的信息。该报告在每个每周补救计划之后收集数据。默认周数为 1。要自定义报告，请根据您的修复周期指定周数。

字段名	定义
日期	收集数据的日期。
账户 ID	配置适用的 AWS 账户 ID
客户姓名	AWS 账户名
检查类别	支 AWS Trusted Advisor 票类别
检查姓名	配置适用的已修正 Trusted Advisor 检查的名称
检查 ID	配置适用的已修正 Trusted Advisor 检查的 ID
状态	支票的警报状态。可能的状态为正常（绿色）、警告（黄色）、错误（红色）或 not_available
已标记的资源	Trusted Advisor 支票标记（列出）的 AWS 资源数量。
资源已忽略	Trusted Advisor 由于您将 AWS 资源标记为已禁止而被忽略的资源数量。
处于危急状态的资源	处于临界状态的资源数量
资源处于警告状态	处于警告状态的资源数量

自助报告

AWS Managed Services (AMS) 自助服务报告 (SSR) 是一项功能，可从各种原生 AWS 服务收集数据，并提供对主要 AMS 产品报告的访问权限。SSR 提供的信息可用于支持运营、配置管理、资产管理、安全管理和合规性。

使用 SSR 从 AMS 控制台访问报告，并通过 Amazon S3 存储桶（每个账户一个存储桶）报告数据集。您可以将数据插入您最喜欢的商业智能 (BI) 工具，以根据您的独特需求自定义报告。AMS <Account_ID>在您的主 AWS 区域创建此 S3 存储桶（S3 存储桶名称:(ams-reporting-data-a)，数据将从 us-east-1 区域托管的 AMS 控制平面共享。

Important

要访问此功能，您必须具有以下角色之一：

- 多账户着陆区：AWSManagedServicesReadOnlyRole
- 单账户登录区：客户__角色 ReadOnly

Important

将自定义密钥与 AWS Glue

要使用客户管理的 KMS 密钥加密您的 AWS Glue 元数据，您必须执行以下额外步骤以允许 AMS 聚合账户中的数据：

1. 在 <https://console.aws.amazon.com/kms> 处打开 AWS Key Management Service 控制台，然后选择客户托管密钥。
2. 选择您计划用于加密 AWS Glue 元数据的密钥 ID。
3. 选择“别名”选项卡，然后选择“创建别名”。
4. 在文本框中输入 AmsReportingFlywheelCustomKey，然后选择创建别名。

主题

- [内部 API 操作](#)
- [补丁报告（每日）](#)
- [Backup 报告（每日）](#)
- [事件报告（每周）](#)
- [账单报告（每月）](#)
- [汇总报告](#)
- [AMS 自助服务报告仪表板](#)
- [数据保留策略](#)
- [从 SSR 中脱颖而出](#)

内部 API 操作

如果您监控 API 操作，则可能会看到对以下仅限内部操作的调用：

- GetDashboardUrl
- ListReportsV2

内部 API 操作：GetDashboardUrl

当 AMS 控制台调用此操作时，此操作会显示在系统日志中。它没有其他用例。它不能直接供您使用。

返回相应报告的嵌入式仪表板 URL。此操作接受 dashboardName 返回的 ListReports。

请求语法

```
HTTP/1.1 200
Content-type: application/json
{
  "dashboardName": "string"
}
```

请求元素

dashboardName：请求网址的 QuickSight 仪表板的名称。在 ListReports V2 中返回仪表板名称。

类型：字符串

响应语法

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。服务以 JSON 格式返回以下数据。

url：返回所请求的 QuickSight 网址 dashboardName。

类型：字符串

错误

有关所有操作中常见的错误的信息，请参阅[常见错误](#)。

BadRequestException:

提交的请求无效。例如，如果输入不完整或不正确。有关详细信息，请参阅随附的错误消息。

HTTP 状态代码：400

NotFoundException:

未找到请求的资源。请确保请求的 URI 正确无误。

HTTP 状态代码：404

TooManyRequestsException:

该请求已达到其限制限制。在指定的时间段后重试。

HTTP 状态代码：429

UnauthorizedException:

请求被拒绝，因为来电者的权限不足。

HTTP 状态代码：401

内部 API 操作：ListReportsV2

当 AMS 控制台调用时，此 API 会出现在系统日志中。它没有其他用例。它不能直接供您使用。

返回指定账户可用的操作报告列表。

请求语法

该请求没有请求正文。

响应语法

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
      "dashboard": "string",
      "lastUpdatedTime": "string",
    }
  ],
}
```

```
"reportsType": "string"
}
```

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。服务以 JSON 格式返回以下数据。

reportsList: 现有行动报告清单。

类型：仪表板对象数组

reportsType：表示报告是否跨多个账户汇总。

类型：字符串

错误

有关所有操作中常见的错误的信息，请参阅[常见错误](#)。

BadRequestException:

提交的请求无效。例如，输入不完整或不正确。有关详细信息，请参阅随附的错误消息。

HTTP 状态代码：400

NotFoundException:

未找到请求的资源。请确保请求的 URI 正确无误。

HTTP 状态代码：404

TooManyRequestsException:

该请求已达到其限制限制。在指定的时间段后重试。

HTTP 状态代码：429

UnauthorizedException:

请求被拒绝，因为来电者的权限不足。

HTTP 状态代码：401

补丁报告（每日）

可用报告

-
- [补丁详情](#)
- [错过补丁的实例](#)

这是一份信息报告，可帮助识别 Patch Orchestrator (PO) 已加载的所有实例、账户状态、实例详细信息、维护时段覆盖范围、维护时段执行时间、堆栈详细信息和平台类型。

该数据集提供：

- 账户的生产和非生产实例的数据。生产和非生产阶段源自账户名，而不是实例标签。
- 按平台类型划分的实例分布数据。当 Sy AWS stems Manager (SSM) 无法获取平台信息时，就会出现“N/A”平台类型。
- 有关实例状态分布、正在运行、停止或终止的实例数量的数据。

控制台字段名称	数据集字段名称	定义
访问限制	访问限制	访问受限的地区
账户编号	aws_account_id	AWS 实例 ID 所属的账户 ID
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
账户名	account_name	AWS 账户名
账户状态	账户状态	AMS 账户状态
	account_sla	AMS 账户服务承诺
Account Type (账户类型)	malz_role	MALZ 角色
自动扩缩组名	instance_asg_name	包含实例的 Auto Scaling 组 (ASG) 的名称
实例 ID	instance_id	EC2 实例的 ID
实例名称	实例名	EC2 实例的名称

控制台字段名称	数据集字段名称	定义
实例补丁组	实例_补丁_组	修补组名称用于将实例分组在一起并应用相同的维护时段
实例补丁组类型	实例_补丁_组_类型	补丁组类型
实例平台类型	实例平台类型	操作系统 (OS) 类型
实例平台名称	实例_平台_名称	操作系统 (OS) 名称
实例状态	实例状态	EC2 实例生命周期内的状态
实例标签	ec2_tags	与亚马逊 EC2 实例 ID 关联的标签
着陆区	malz_flag	举报与 MALZ 相关的账户
维护时段覆盖范围	mw_covered_flag	如果实例至少有一个已启用的维护时段，且执行日期为 future，则该实例被视为已覆盖，否则不包括在内
维护时段执行日期/时间	最早的 window_execution_time	下次预计会执行维护时段
维护时段执行日期/时间	最早的 window_execution_time	下次预计会执行维护时段
生产账户	产品账号	AMS prod、非生产账户的标识符，具体取决于账户名称是否包含值“PROD”、“NONPROD”。
举报日期时间	数据集_日期时间	报告的生成日期和时间。
堆栈名称	实例堆栈名称	包含实例的堆栈名称

控制台字段名称	数据集字段名称	定义
堆栈类型	实例堆栈类型	AMS 堆栈 (客户账户中的 AMS 基础架构) 或客户堆栈 (支持客户应用程序的 AMS 托管基础架构)

补丁详情

该报告提供了各种实例的补丁详细信息和维护时段覆盖范围。

该报告提供：

- 有关补丁组及其类型的数据。
- 有关维护时段、持续时间、截止时间、维护时段执行的未来日期 (计划) 以及每个窗口中受影响的实例的数据。
- 该账户下所有操作系统的数据以及安装该操作系统的实例数量。

字段名	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间。
账户编号	aws_account_id	AWS 实例 ID 所属的账户 ID
账户名	account_name	AWS 账户名
账户状态	账户状态	AMS 账户状态
合规-关键	合规性_关键	严重性为“严重”的兼容补丁数量
合规-高	合规性高	严重性为“高”的兼容补丁数量
合规-中等	合规_中等	严重性为“中等”的兼容补丁数量
合规-低	合规性低	严重性为“低”的兼容补丁数量

字段名	数据集字段名称	定义
合规-信息性	合规_信息	严重性为“信息性”的兼容补丁数量
合规-未指定	合规_未指定	严重性为“未指定”的兼容补丁数量
合规-总计	合规总计	合规补丁数量（所有严重性）
实例 ID	instance_id	EC2 实例的 ID
实例名称	实例名	EC2 实例的名称
	account_sla	AMS 账户服务等级
实例平台类型	实例平台类型	操作系统 (OS) 类型
实例平台名称	实例_平台_名称	操作系统 (OS) 名称
实例补丁组类型	实例_补丁_组_类型	默认：默认补丁组和默认维护时段，由实例上的:True AMSDefault PatchGroup 标签确定 客户：客户创建的补丁组 未分配：未分配补丁组
实例补丁组	实例_补丁_组	修补组名称用于将实例分组在一起并应用相同的维护时段
实例状态	实例状态	EC2 实例生命周期内的状态
实例标签	ec2_tags	与亚马逊 EC2 实例 ID 关联的标签
上次执行维护窗口	上次执行窗口	最近一次执行维护时段的时间
维护时段 ID	window_id	维护时段 ID

字段名	数据集字段名称	定义
维护窗口状态	window_state	维护窗口状态
维护时段类型	窗口类型	维护时段类型
维护时段下次执行日期时间	window_next execution_time	下次预计会执行维护时段
维护时段持续时间 (小时)	窗口持续时间	维护时段的持续时间 (以小时为单位)
维护时段覆盖范围	mw_covered_flag	如果实例至少有一个已启用的维护时段，且执行日期为 future，则该实例被视为已覆盖，否则不包括在内
不合规-严重	不合规_严重	严重性为“严重”的不合规补丁数量
不合规-高	不合规_高	严重性为“高”的不合规补丁数量
不合规-中等	不合规_中等	严重性为“中等”的不合规补丁数量
不合规-低	不合规_低	严重性为“低”的不合规补丁数量
不合规-信息性	不合规 _信息	严重性为“信息性”的不合规补丁数量
不合规-未指定	不合规 _未指定	严重性为“未指定”的不合规补丁数量
不合规-合计	不合规总数	不合规补丁数量 (所有严重性)

字段名	数据集字段名称	定义
补丁基准 ID	patch_baseline_id	当前附加到实例的补丁基准
补丁状态	补丁状态	总体补丁合规性状态。如果至少缺少一个补丁，则认为实例不合规，否则视为合规。
生产账户	产品账号	AMS prod、非生产账户的标识符，具体取决于账户名称是否包含值“PROD”、“NONPROD”。
堆栈类型	实例堆栈类型	AMS 堆栈（客户账户中的 AMS 基础架构）或客户堆栈（支持客户应用程序的 AMS 托管基础架构）
	window_next_exec_yyyy	window_next_execution_time 的年份部分
	window_next_exec_mm	window_next_execution_time 的月份部分
	window_next_exec_D	window_next_execution_time 的当天部分
	window_next_exec_HHMM	小时>window_next_execution_time 的分钟部分

错过补丁的实例

此报告提供了在上次执行维护时段期间错过补丁的实例的详细信息。

该报告提供：

- 补丁 ID 级别的缺失补丁数据。

- 有关至少缺少一个补丁的所有实例以及补丁严重性、未修补天数、补丁范围和补丁发布日期等属性的数据。

字段名	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间
账户编号	aws_account_id	AWS 实例 ID 所属的账户 ID
账户名	account_name	AWS 账户名
客户姓名父公司	客户_姓名_父级	
客户姓名	customer_name	
生产账户	产品账号	AMS 生产账户或非生产账户的标识符，具体取决于账户名称包含值“PROD”还是“NONPROD”。
账户状态	账户状态	AMS 账户状态
Account Type (账户类型)	账户类型	
	account_sla	AMS 账户服务等级
实例 ID	instance_id	您的 EC2 实例的 ID
实例名称	实例名	您的 EC2 实例的名称
实例平台类型	实例平台类型	操作系统 (OS) 类型
实例状态	实例状态	EC2 实例生命周期内的状态
实例标签	ec2_tags	与亚马逊 EC2 实例 ID 关联的标签
补丁编号	补丁_id	已发布补丁的 ID
补丁严重性	patch_sev	每个发行商的补丁严重程度

字段名	数据集字段名称	定义
补丁分类	补丁类	补丁发布者对补丁的分类
补丁发布日期时间 (UTC)	release_dt_utc	每个发行商的补丁发布日期
补丁安装状态	安装状态	每个 SSM 在实例上安装补丁状态
未修补的天数	days_unpatched	自上次 SSM 扫描以来实例未修补的天数
未修补天数范围	days_unpatched_bucke	一大堆未修补的天数

Backup 报告 (每日)

备份报告涵盖主要和次要区域 (如果适用) 。它涵盖了备份的状态 (成功/失败) 以及拍摄的快照的数据。

该报告提供：

- Backup 状态
- 拍摄的快照数量
- 恢复点
- Backup 计划和保管库信息

字段名	数据集字段名称	定义
报告日期时间	数据集_日期时间	报告的生成日期和时间。
账户编号	aws_account_id	实例 ID 所属的 AWS 账户 ID
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
账户名	account_name	AWS 账户名称
账户 SLA	account_sla	AMS 账户服务承诺

字段名	数据集字段名称	定义
	malz_flag	举报与 MALZ 相关的账户
	malz_role	MALZ 角色
	访问限制	访问受限的地区
Backup 快照计划开始日期/时间	start_by_dt_utc	计划开始快照的时间戳
Backup 快照实际开始日期/时间	creation_dt_utc	快照实际开始的时间戳
Backup 快照完成日期/时间	completion_dt_utc	快照完成的时间戳
Backup 快照到期日期/时间	expiration_dt_utc	快照过期的时间戳
Backup Job 状态	备份任务状态	快照的状态
Backup 类型	backup_type	备份类型
Backup Job ID	备份作业 ID	备份任务的唯一标识符
Backup 大小 (字节)	backup_size_in_bytes	以字节为单位的备份大小
Backup Plan ARN	backup_plan_arn	备份计划 ARN
Backup Plan ID	备份计划_ID	Backup 计划唯一标识符
备份计划名称	备份计划名称	Backup 计划名称
Backup 计划版本	备份计划版本	备份计划版本
Backup 规则 ID	backup_rule_id	备份规则 ID
Backup Vault ARN	backup_vault_arn	Backup 保管库 ARN
备份文件库名称	备份保管库名称	备份库名称
IAM 角色 ARN	iam_role_arn	IAM 角色 ARN

字段名	数据集字段名称	定义
实例 ID	instance_id	唯一的实例 ID
实例状态	实例状态	实例状态
实例标签	ec2_tags	与 EC2 实例 ID 关联的标签
资源 ARN	resource_arn	Amazon 资源名称
资源 ID	资源_id	唯一的资源标识符
资源区域	资源_区域	资源的主要（以及次要区域，如果适用）。
资源类型	resource_type	资源的类型
恢复点 ARN	recovery_point_arn	恢复点的 ARN
恢复点 ID	恢复点_id	恢复点的唯一标识符
恢复点状态	恢复点状态	恢复点状态
恢复点数天后删除	恢复点_delete_delete_delete_days	恢复点将在几天后删除
几天后，恢复点会移至冷库	recovery_point_move_to_to_to_cold_storage_days	完成日期之后将备份快照移至冷存储的天数
恢复点加密状态	recovery_point_已加密	恢复点加密状态
恢复点加密密钥 ARN	recovery_point_cryption_key_arn	恢复点加密密钥 ARN
堆栈编号	stack_id	云形成堆栈唯一标识符
堆栈名称	stack_name	堆栈名称
标签：AMS 默认补丁组	tag_ams_default_patch_group	标签值：AMS 默认补丁组
标签：应用程序 ID	tag_app_id	标签值：应用程序 ID

字段名	数据集字段名称	定义
标签：应用程序名称	tag_app_name	标签值：应用程序名称
标签：Backup	标签_备份	标签值：Backup
标签：合规框架	标签合规框架	标签价值：合规框架
标签：成本中心	tag_cost_center	标签价值：成本中心
标签：客户	标签_客户	标签值：客户
标签：数据分类	标签_数据_分类	标签值：数据分类
标签：环境类型	标签_环境_类型	标签值：环境类型
标签：营业时间	标签操作时间	标签值：营业时间
标签：车主团队	tag_owner_team	标签值：所有者团队
标签：车主团队电子邮件	tag_owner_team_email	标签值：所有者团队电子邮件
标签：补丁组	tag_patch_group	标签值：补丁组
标签：Support 优先级	标签_支持_优先级	标签值：Support Priority
音量状态	音量状态	音量状态

事件报告（每周）

该报告提供了事件的汇总列表及其优先级、严重程度和最新状态，包括：

- 被归类为托管账户事件的支持案例数据
- 可视化托管账户的事件指标所需的事件信息
- 有关每起事件的事件类别和补救状态的数据

每周事件报告均提供可视化和数据。

- 可视化可以通过账户中的 AMS 控制台通过“报告”页面进行访问。

- 具有以下架构的数据集可通过托管账户中的 S3 存储桶进行访问。
- 使用提供的日期字段，根据事件创建或解决的月、季度、周、 and/or 日筛选事件。

字段名	数据集字段名称	定义
报告日期时间	数据集_日期时间	报告的生成日期和时间。
账户编号	aws_account_id	AWS 事件所属的账户 ID。
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
账户名	account_name	AWS 账户名。
案例编号	case_id	事件的 ID。
创建月份	创建月份	事件发生的月份。
优先级	priority	事件的优先级。
严重性	severity	事件的严重程度。
状态	状态	事件的状态。
类别	yuma_类别	事件的类别。
创建日	created_day	以 YYYY-MM-DD格式创建事件的那一天。
创建周	created_wk	事件以 YYYY-WW 格式创建的那一周。星期日至星期六算作一周的开始和结束。每周从 01 到 52。第 01 周始终是包含一年中第一天的那一周。例如，2023-12-31和2024-01-01 在2024-01周。

字段名	数据集字段名称	定义
创建季度	created_qtr	以 YYYYYY-Q 格式创建事件的季度。01/01 到 03/31 被定义为第一季度，依此类推。
已解决的日子	resolved_day	以 YYYY-MM-DD格式解决事件的那一天。
已解决周	resolved_wk	以 YYYYYY-WW 格式解决事件的那一周。星期日至星期六算作一周的开始和结束。每周从 01 到 52。第 01 周始终是包含一年中第一天的那一周。例如，2023-12-31和2024-01-01在2024-01周。
已解决月份	已解决_month	事件得到解决的月份，格式为 YYYY-MM。
已解决的季度	resolved_qtr	以 YYYYYY-Q 格式解决事件的季度。01/01 到 03/31 被定义为第一季度，依此类推。
已创建分组规则	分组规则	适用于事件的分组规则。“no_grouping”或“实例分组”。
实例 IDs	实例_id	与事件关联的实例。
警报数量	警报数量	与该事件相关的警报数量。如果您启用了分组，则此数字可以大于 1。如果您未启用分组，则它将始终为 1。
创建于	created_at	事件发生的时间戳。
警报 ARNs	alarm_arns	与您的事件相关的警报的 Amazon 资源名称 (“arn”)。

字段名	数据集字段名称	定义
相关警报	相关警报	与事件相关的所有警报的易读名称。

账单报告（每月）

账单费用详情

该报告详细介绍了关联账户和相应的 AWS 服务的 AMS 账单费用。

该报告提供：

- 有关 AMS 服务级别费用、提升百分比、账户级 AMS 服务等级和 AMS 费用的数据。
- 关联账户和 AWS 使用费用的数据。

 Important

月度账单报告仅在您的管理付款人账户 (MPA) 或您定义的借记账户中可用。这些账户是发送您的 AMS 月度账单的账户。如果您无法找到这些帐户，请联系您的云服务交付经理 (CSDM) 寻求帮助。

字段名	数据集字段名称	定义
账单日期	date	服务计费的月份和年份
付款人账户 ID	payer_account_id	用于识别负责支付 AMS 费用的账户的 12 位数身份证
关联账户 ID	linked_account_id	用于标识 AMS 账户的 12 位数字 ID，该账户使用可生成扩展的服务
AWS 服务名称	product_name	使用的 AWS 服务

字段名	数据集字段名称	定义
AWS 收费	aws_charg	AWS 服务名称中 AWS 服务名称的 AWS 费用
定价计划	定价计划	与关联账户关联的定价计划
AMS 服务组	tier_uplifting_groups	用于确定提升百分比的 AMS 服务组代码
上升比例	上升百分比	基于 pricing_plan、SLA 和服务的提升百分比（以十进制 V.WXYZ 表示）AWS
调整后的 AWS 费用	调整后的 aws_usage	AWS 已针对 AMS 调整使用量
提高冲锋量 AWS	uplifted_aws_charges	AMS 要 AWS 收取的费用百分比；adjusted_aws_charges * uplift_percent
实例 EC2 RDS 支出	instances_ec2_rds_spend	在 RDS 实例上 EC2 花钱
预留实例费用	ris_charges	预留实例费用
上调的预留实例费用	uplifted_ris	向 AMS 收取的预留实例费用的百分比；ris_charges * uplift_percent
Savings Plan 费用	sp_charges	SavingsPlan 使用费
Uplifted Savings Plan 费用	uplifted_sp	向 AMS 收取的储蓄计划费用百分比；sp_charges * uplift_percent
AMS 费用	ams_charges	ams 对该产品的总费用； uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp

字段名	数据集字段名称	定义
按比例分配的最低费用	按比例分配的最小值	我们为履行合同最低要求而收取的金额
关联账户 AMS 费用总额	关联账户总计 ams_charges	关联账户的所有费用总和
付款人账户 AMS 费用总额	付款人账户总计 ams_charges	付款人账户所有费用的总和
最低费用	最低费用	AMS 最低费用 (如果适用)
预留实例和 Savings Plan 折扣	adj_ri_sp_charges	RI/SP discount to be applied against RI/SP费用 (在某些情况下适用)

汇总报告

聚合自助服务报告 (SSR) 为您提供在组织层面、跨账户汇总的现有自助服务报告的视图。这使您可以了解您内部所有账户中由 AMS 管理的所有账户的关键运营指标，例如补丁合规性、备份覆盖范围和事件 AWS Organizations。

所有提供 AWS Managed Services AWS 区域 的商业版均提供聚合 SSR。有关可用区域的完整列表，请参阅[区域表](#)。

启用汇总报告

您必须通过管理[账户 AWS Organizations 管理](#)聚合的 SSR。管理 AWS 账户是您用来创建组织的账户。

要为已登录 AMS 的 AWS Organizations 管理账户启用聚合 SSR，请访问您的 AMS 控制台并导航到报告。选择 top-right-hand角落的组织访问权限以打开 [AWS Managed Services 控制台：组织视图](#) 窗格。在此窗格中，您可以管理聚合 SSR 功能。

AWS Organizations 未加入 AMS 的管理账户无权访问 AMS 控制台。要为未加入 AMS 的 AWS Organizations 管理账户启用聚合 SSR，请先向您的账户进行身份验证 AWS 账户，然后导航到[AWS](#)

[控制台](#)并搜索 Managed Services。这将打开 AMS 营销页面。在此页面上，选择导航栏中的组织访问权限链接，打开 AWS Managed Services 控制台：组织视图，您可以在其中管理聚合 SSR 功能。

首次访问 [AWS Managed Services 控制台：组织视图](#)时，请完成以下步骤：

1. 如果您尚未设置 AWS Organizations，请 AWS Organizations从您的主机中选择“启用”。有关设置的更多信息 AWS Organizations，请参阅《[AWS Organizations 用户指南](#)》。如果您已经在使用，则可以跳过此步骤 AWS Organizations。
2. 要启用聚合自助服务报告服务，请在控制台上选择启用可信访问。
3. （可选）注册授权管理员以获得组织视图的读取权限。

以授权管理员身份查看汇总报告

委托管理员是您选择拥有汇总报告的读取权限的账户。委派的管理员必须是 AMS 已注册的账户，并且是唯一拥有汇总报告读取权限的账户。

要选择委托管理员，请在 AWS Managed Services 控制台：组织视图的步骤 3 中输入账户 ID。您一次只能注册一个委托管理员账户。请注意，委派的管理员账户必须是 AMS 管理的账户。

要更新委托管理员账户，请导航至 [AWS Managed Services 控制台：组织视图](#)，然后选择移除授权管理员。控制台会提示您插入新的账户 ID 以注册为委派管理员。

阅读汇总报告

如果您未注册授权管理员，并且您的 AWS Organizations 管理账户已加入 AMS，则默认情况下，该 AWS Organizations 管理账户将获得对汇总报告的读取权限。如果 AWS Organizations 管理账户不由 AMS 管理，则必须选择授权管理员账户才能读取汇总报告。

在任何时候，只有一个注册到 AMS 的账户拥有对汇总报告的读取权限，无论是 AWS Organizations 管理账户还是注册的委托管理员。您组织内的所有其他成员账户（并已加入 AMS）仍然只能访问每个个人账户的单一账户报告。

启用聚合 SSR 后，导航到您的[报告](#)。此部分列出了您现有的所有自助服务报告，蓝色标签表示这些报告已汇总。请注意，您必须使用您选择的账户访问 AMS 控制台，才能读取汇总报告。这要么是 AWS Organizations 管理账号，要么是委派管理员账号。

启用聚合 SSR 后，可以从下一个报告周期开始使用聚合报告。

禁用聚合报告

要禁用聚合 SSR，请打开 [AWS Managed Services 控制台：组织视图](#)。选择“禁用可信访问”。禁用聚合 SSR 的可信访问权限后，将停止在组织级别跨账户汇总您的 AMS 自助服务报告。另请注意，停用从下一个报告周期开始生效。

禁用“聚合 SSR”后，您需要等待 AMS 控制台中的报告才会显示为单一账户报告。之所以出现这种延迟，是因为该功能的停用从下一个报告周期开始生效。

AMS 自助服务报告仪表板

AMS 自助服务报告提供两个仪表板：[资源标记器控制面板](#)和[安全配置 Rules 控制面板](#)。

资源标记器控制面板

AMS 资源标记器控制面板提供有关资源标记器支持的资源的详细信息，以及资源标记器配置为应用于这些资源的标签的当前状态。

按资源类型划分的资源标记器覆盖率

该数据集由具有资源标记器管理的标签的资源列表组成。

按资源类型划分的资源覆盖率可视化为四个折线图，这些折线图描述了以下指标：

- 资源数量：按资源类型划分的区域中的资源总数。
- 缺少托管标签的资源：按资源类型划分的区域中需要托管标签但未由资源标记器标记的资源总数。
- 非托管资源：按资源类型划分的区域中未使用资源标记器应用托管标签的资源总数。这通常意味着这些资源与任何资源标记器配置都不匹配，或者被明确排除在配置之外。
- 托管资源：对应于非托管资源指标（资源计数-非托管资源）。

下表列出了该报告提供的数据。

字段名称	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间（UTC 时间）
AWS 账户 身份证	aws_account_id	AWS 账户 身份证

字段名称	数据集字段名称	定义
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
区域	区域	AWS 区域
资源类型	resource_type	此字段标识资源的类型。仅包括资源标记器支持的资源类型。
资源计数	资源计数	在该区域部署的（指定资源类型的）资源数量。
ResourcesMissingManagedTags	资源缺失托管标签计数	根据配置配置文件，需要托管标签但尚未由资源标记器标记的资源（指定资源类型）的数量。
UnmanagedResources	unmanaged_resource_count	Resource Tagger 未应用托管标签的资源（指定资源类型）的数量。通常，这些资源与任何 Resource Tagger 配置块都不匹配，或者被明确排除在配置块之外。

资源标记器配置规则合规性

该数据集由按资源类型划分的资源列表组成，这些资源应用了特定的配置文件。AWS 区域它被可视化 为折线图。

下表列出了该报告提供的数据。

字段名称	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间（UTC 时间）

字段名称	数据集字段名称	定义
AWS 账户 身份证	aws_account_id	AWS 账户 身份证
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
区域	区域	AWS 区域
资源类型	resource_type	此字段标识资源的类型。仅包括资源标记器支持的资源类型。
配置配置文件 ID	配置_配置文件_ID	资源标记器配置文件的 ID。配置文件用于定义用于标记资源的策略和规则。
MatchingResourceCount	资源计数	与 Resource Tagger 配置配置文件 ID 相匹配的资源 (指定资源类型) 的数量。要使资源与配置文件匹配，必须启用配置文件并且资源必须与配置文件的规则相匹配。

资源标记器不合规的资源

此数据集由不符合单个资源标记器配置的资源列表组成。这些数据是资源合规性的每日快照，显示了将这些报告交付给客户账户时客户资源的状态 (没有历史视图)。它可视化为一个数据透视表，由不适用于给定配置的资源组成。

下表列出了该报告提供的数据。

字段名称	数据集字段名称	定义
举报日期时间	数据集_日期时间	报告的生成日期和时间 (UTC 时间)
AWS 账户 身份证	aws_account_id	AWS 账户 身份证

字段名称	数据集字段名称	定义
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
区域	区域	AWS 区域
资源类型	resource_type	此字段标识资源的类型。仅包括资源标记器支持的资源类型。
资源 ID	资源_id	资源标记器支持的资源的唯一标识符。
覆盖状态	coverage_state	此字段表示资源是否按资源标记器配置 ID 的配置进行标记。
配置配置文件 ID	配置_配置文件_ID	资源标记器配置文件的 ID。配置文件用于定义用于标记资源的策略和规则。

安全配置 Rules 控制面板

Security Config 规则控制面板可深入了解 AMS 账户的资源 and AWS Config 规则合规性。您可以按规则严重性筛选报告，以确定最关键的发现的优先级。下表列出了该报告提供的数据。

字段名称	数据集字段名称	定义
AWS 账户 身份证	AWS 账户 身份证	与相关资源关联的账户 ID。
管理员账户 ID	aws_admin_account_id	由您启用的可信 AWS Organizations 账户。
报告日期时间	举报日期	报告的生成日期和时间。
customer_name	客户姓名	客户名称。
account_name	账户名	与账户 ID 关联的名称

字段名称	数据集字段名称	定义
资源_id	资源 ID	资源的标识符。
资源_区域	资源区域	资源 AWS 区域 所在的位置。
resource_type	资源类型	AWS 服务 或资源类型。
资源名称	资源名称	资源的名称。
资源_ams_flag	资源 AMS 标志	如果资源由 AMS 拥有，则此标志设置为 TRUE。如果资源归客户所有，则此标志设置为 FALSE。如果所有权未知，则此标志将设置为 UNKNOW WN。
配置规则	Config 规则	配置规则的不可自定义名称。
配置规则_描述	Config 规则描述	配置规则的描述。
源标识符	来源标识符	托管配置规则的唯一标识符，没有自定义配置规则的标识符。
合规标志	合规标志	显示资源是符合还是不符合配置规则。
规则_类型	规则类型	表示规则是预定义的还是定制的。
异常标志	异常标志	资源异常标志显示针对不合规资源的风险接受程度。如果资源的资源异常标志为 TRUE，则该资源将被豁免。如果异常标志为 NULL，则该资源不会被豁免。
cal_dt	日期	规则的评估日期。

字段名称	数据集字段名称	定义
补救说明	补救说明	关于如何修复规则合规性的描述。
severity	严重性	Config 规则严重性表示不合规的影响。
客户行动	客户行动	您需要采取措施来纠正此规则。
建议	建议	对配置规则检查内容的描述。
补救类别	补救类别	当此规则变得不合规时，AMS 采取的默认操作。

数据保留策略

AMS SSR 对每份报告都有数据保留政策，报告期过后，数据将被清除且不再可用。

报告名称	数据保留 SSR 控制台	数据保留 SSR S3 存储桶
实例详细信息摘要（补丁编排器）	2 个月	2 年
补丁详情	2 个月	2 年
在维护时段执行期间错过补丁的实例	2 个月	2 年
AMS 账单费用详情	2 年	2 年
每日备份报告	1 个月	2 年
每周事件报告	2 个月	2 年
安全配置 Config 规则控制面板	3 个月	2 年
资源标记器控制面板	1 年	2 年

从 SSR 中脱颖而出

要退出 SSR 服务，请通过 AMS 控制台创建服务请求 (SR)。提交 SR 后，AMS 运营工程师会帮助您退出 SSR。在 SR 中，提供你想下车的原因。

要退出账户并执行资源清理，请通过 AMS 控制台创建 SR。提交 SR 后，AMS 操作工程师会帮助您删除 SSR 的 Amazon S3 存储桶。

如果您已退出 AMS，则会自动退出 AMS SSR 控制台。AMS 会自动停止向您的账户发送数据。作为离职流程的一部分，AMS 会删除您的 SSR S3 存储桶。

AMS 中的事件报告、服务请求和账单问题

主题

- [事件管理](#)
- [服务请求管理](#)
- [账单问题](#)

借助 AWS Managed Services (AMS)，您可以随时通过 AMS 控制台请求有关操作问题和请求的帮助。AMS 运营工程师可以全天候响应您的事件和服务请求，响应时间服务级别协议 (SLAs) 和服务级别目标 ()，具体取决于您选择的账户服务级别 (Plus、PremiumSLOs)。AMS 运营工程师使用相同的机制主动通知您重要的警报和问题。

事件管理

主题

- [什么是事件管理？](#)
- [事件管理服务承诺](#)
- [事件管理示例](#)

事件是指影响您的托管环境的 AWS 服务 性能问题，由 AWS Managed Services (AMS) 或您决定。AMS 团队识别的事件首先作为“事件”接收：通过监控捕捉到的系统状态变化。如果突破了配置的阈值，则该事件会触发警报，也称为警报。AMS 运营团队确定事件是非影响性事件、事件 (服务中断或降级) 还是问题 (一个或多个已解决事件的根本原因)。

AMS 团队还会通过 支持 中心接收您发现的事件，或者使用带有服务代码sentinel-report-incident的 [AWS Support API](#) 以编程方式接收事件。

AMS 运营团队收到您的事件后，会对其进行审查，以确保该事件不会被更好地归类为服务请求。如果应将其归类为服务请求，则会立即将其重新分类，AMS 服务请求团队接管并通知您。如果接收操作员能够解决事件，则会采取措施立即解决事件。AMS 操作员查阅内部文档以获得解决方案，并在需要时将事件上报给其他支持资源，直到事件得到解决。要随时了解事件解决过程的每个步骤，请务必填写“抄送电子邮件”选项，而且，如果您要通过联盟进行连接，请在点击 AMS 发送的电子邮件中的链接之前登录。问题解决后，AMS 运营团队将记录事件和解决方案，以备将来使用。

如果事件解决方案需要更改基础架构，则可能需要进行安全审查。可能需要安全审查的基础设施变更包括与 IAM、基于资源的策略或风险批准相关的更改。此类事件需要 AMS 运营工程师在进行更改之前创建 RFC，并且需要您批准该 RFC。例如，如果事件解决方案需要更新 IAM 策略，则将进行 AMS 安全审查，然后 AMS 运营工程师将使用管理 | 高级堆栈组件 | 身份和访问管理 (IAM) | 更新实体或策略变更类型 (ct-27tuth19k52b4) 创建 RFC，然后等待您批准 RFC 后再继续操作。

Note

AMS 现在允许在不经过 RFC 批准的额外步骤的情况下进行基础设施变更的事故解决方案。如果解决事件所需的更改不需要安全审查（更改与 IAM、基于资源的策略或风险批准无关），AMS 可以根据您在事件中获得的批准进行更改，而无需在 RFC 中单独获得批准。

有关事件管理术语的定义，请参阅 [AMS 关键术语](#)。

要了解事件的升级路径，请参阅[获取帮助](#)。

有关 AMS 对事件的响应的描述，请参阅 [AMS 事件响应](#)。

什么是事件管理？

事件管理是 AMS 用来记录、采取行动、沟通活动事件进展和提供通知的流程。

事件管理流程的目标是确保尽快恢复托管服务的正常运行，最大限度地减少业务影响，并随时向所有相关方通报情况。

事件的示例包括（但不限于）网络连接中断或降级、进程或 API 无响应或计划任务未执行（例如，备份失败）。

下图描述了您向 AMS 报告的事件的工作流程。

此图描绘了 AMS 向您报告的事件的工作流程。

事件优先级

在 AWS Support 中心、控制台或支持 API (SAPI) 中创建的事件与在 AMS 控制台中创建的事件具有不同的分类。

- 低：您的业务服务或应用程序中与 AWS 或 AMS 资源相关的非关键功能受到影响。

- 中：与 AWS and/or AMS 资源相关的业务服务或应用程序受到中度影响，且运行处于降级状态。
- 高：您的业务受到严重影响。与 AWS and/or AMS 资源相关的应用程序的关键功能不可用。专为影响生产系统的最严重的停机而设计。

 Note

AWS Support 控制台提供五个事件优先级别，我们将其转换为三个 AMS 级别。

问题与事件

当 AMS 认为事件显示出更大的缺陷或配置错误并可能再次发生时，它被视为问题，而不仅仅是事件。在这种情况下，AMS会对问题进行分析并提出解决问题的建议。

事件管理服务承诺

事件管理服务承诺

事件或行动	服务承诺衡量
案例 1：生成了具有已知影响的事件。AMS 打开一个事件并通知你。	事件响应和事件解决的时钟从以下时间开始：
案例 2：AMS 与您联系以确认事件的影响。您确认该事件是事件。	案例 1：AMS 制造了事件。
案例 3：您注意到问题并提交了事件报告。	案例 2：您确认警报是突发事件。
	案例 3：您提交了事件。
	服务承诺取决于所造成事件的优先级。
如果您提交了事件，AMS 会发送回复以进行确认。	事件解决的时钟继续滴答作响。
如果 AMS 代表您创建事件，则不会发送单独的事件响应。	当 AMS 发送事件确认时，事件响应时间的时钟停止。
	 Note 等待您输入所花费的时间不包括在事件解决时间计算中。对于 AMS 创建的事

事件或行动	服务承诺衡量
	件，初始响应时间是向您创建初始事件通知的时间。
对于有问题的资源/服务，AMS 会检查运行状况以验证是否： - AMS 检测到的事件或客户提交的事件符合事件的资格，并且 - 正确确定了事件的优先顺序，并且 如果您提交的事件的优先级不正确，AMS 会重新确定其优先级。如果 AMS 更改了事件优先级，则会向您发送通知以及优先级更改背后的理由。在某些情况下，您提交的问题可能不符合事件的资格，视原因而定。在这种情况下，AMS 会关闭事件并向您发送通知，解释原因。无论事件分类如何，AMS 都会与您合作，根据需要提供帮助。 要了解事件分类规则，请参阅事件优先级。	如果事件优先级发生变化，则适用新优先级的服务承诺；时钟继续滴答作响。如果事件因不符合事件定义而结案，则服务承诺不适用；时钟停止。 在以下情况下，时钟停止： - AMS 已将与该事件相关的所有不可用服务或资源恢复到可用状态，或 - 基础架构恢复已开始。
AMS 正在处理该事件，以便在服务承诺范围内予以解决。在某些情况下，如果 AMS 确定无法及时解决不可用的堆栈或资源，AMS 将提供基础设施恢复作为解决方案选项。除非您另有说明，否则基础设施恢复包括根据受影响堆栈的模板重新部署现有堆栈，并根据上次已知的还原点（EBS/RDS 快照）启动数据恢复。个别 EC2 实例的临时数据将丢失。如果您未按照 AWS 的建议授权基础设施恢复，则将没有资格获得相关事件解决时间服务承诺的服务积分。	

事件或行动	服务承诺衡量
有时，AMS 需要您的澄清或您的活动，以使事件解决工作继续向前推进，除非您有预先定义的、经过批准的行动。因此，AMS 与您之间会进行沟通，以解决突发事件	以下情况下时钟停止：AMS 正在等待您的回复或操作。 当：AMS 收到您的回复或 AMS 要求您执行的操作完成时，时钟将重新启动。

 Note

有关服务承诺的完整列表，请下载 [AMS 服务等级协议](#)。

事件管理示例

事件管理示例。

主题

- [事故测试](#)
- [举报事件](#)
- [监控和更新事件](#)
- [使用 AWS Support API 管理事件](#)
- [响应 AMS 引发的事件](#)

以下示例介绍如何使用 AMS 控制台提交事件。提交后，AMS 团队将与您合作，根据您的服务等级协议 (SLA) 解决事件。

事故测试

在测试AMS事件提交时, 我们要求您在主题文本中包含此标志:AMSTestNoOpsActionRequired. 此标志让 AMS 知道提交的事件仅用于测试。当 AMS 运营工程师看到该标志时，他们不会以任何方式回应提交的事件。

举报事件

使用 AMS 控制台报告事件。为每个新问题或问题创建一个新事件很重要。在打开与旧查询相关的案例时，提供相关的案例编号会很有帮助，这样我们就可以参考以前的信件。

 Note

如果案例信件偏离了原始问题，AMS 操作员可能会要求您举报新的事件。

要使用 AMS 控制台报告事件，请执行以下操作：

1. 从左侧导航栏中选择“事件”

事件列表打开：

如果您的事件列表为空，则清除筛选器选项会将过滤器重置为“任意”状态。

如果您知道要使用电话或聊天，请单击“在支持中心创建事件”，在 Support Center Console 中打开“事件创建”页面，该页面会自动填充 AMS 服务类型。

 Important

- 以开头的电话支持会被录音，以便更好地提高响应能力。如果来电掉线，你必须通过 Support Center 案例回电，AWS 没有回电的机制。
- 电话和聊天支持旨在帮助解决支持案例、事件和服务请求，而不是 RFC 或安全问题。
- 如果 RFC 问题，请使用相关 RFC 详细信息页面上的通信选项联系 AMS 工程师。
- 对于安全问题，请创建高优先级（P1 或 P2）支持案例。实时聊天功能不适用于安全事件。

2. 如果要查找现有事件，请在下拉列表中选择事件状态筛选器。

- 所有尚未解决的事件。
- 尚未分配的新事件。
- 已分配的事件。
- 你重新审理的事件。
- 一个已分配的、复杂的事件。
- 需要您在下一步之前提供反馈的事件。

- 您最近提交信息的事件。
- 一个已经结束的事件。
- 账户中的所有事件。

3. 选择创建。

创建事件页面打开：

4. 选择优先级：

- 低：您的业务服务或应用程序中与 AWS/AMS 资源相关的非关键功能会受到影响。
- 中：与 AWS/AMS 资源相关的业务服务或应用程序受到中度影响，且运行处于降级状态。
- 高：您的业务受到严重影响。您的应用程序中与 AWS/AMS 资源相关的关键功能不可用。专为影响生产系统的最严重的停机而设计。

5. 选择一个类别。

Note

如果您要测试事件功能，请在事件标题中添加不采取行动标志 (AMSTestNoOpsActionRequired)。

6. 输入以下信息：

- 主题：事件报告的描述性标题。
- 抄送电子邮件：一份电子邮件地址列表，供你想向其通报事件报告和解决方案的人使用。
- 详细信息：全面描述事件、受影响的系统以及解决方案的预期结果。回答预设的问题，或者将其删除并输入任何相关信息。

要添加附件，请选择“添加附件”，浏览到所需的附件，然后单击“打开”。要删除附件，请单击“删除”图

标：

7. 选择提交。

将打开一个详细信息页面，其中包含有关事件的信息，例如类型、主题、已创建、ID 和状态，以及一个包含您创建的请求描述的“通信”区域。

单击“回复”以打开通信区域，并提供更多详细信息或状态更新。

事件解决后，单击“关闭案例”。

如果信件数量超过一页所能容纳的信件数量，请单击“加载更多”。

别忘了给沟通打分！

您的事件将显示在“事件”列表页面上。

YouTube 视频：[如何通过 AWS Managed Services 控制台提出事件？](#)

监控和更新事件

您可以使用 AMS 控制台或以编程方式使用支持 API 更新、监控和查看事件报告和服务请求（均为已调用案例）。有关使用支持 API 的信息，请参阅[DescribeCases](#)操作。

要使用 AMS 控制台监控案例、事件或服务请求，请按照以下步骤操作。

1. 在 AMS 控制台的“事件报告”或“服务请求”控制面板中，浏览到案例并选择“主题”，打开包含当前状态和通信内容的详细信息页面。

当 AMS 运营团队更新已报告的事件或服务请求案例时，您会在 AMS 控制台中收到一封电子邮件和事件链接，以便您做出回应。您无法通过回复电子邮件来回复事件通信。

Important

您必须输入电子邮件地址才能接收服务请求或事件案例的状态变更通知。通知仅发送到创建案例时添加到案例中的电子邮件地址。

除非您在 AMS 联合网络上使用电子邮件服务器，否则通知电子邮件中的链接将无法使用。但是，您可以前往 AMS 控制台并使用问题详情页面来回复信件。

2. 如果列表中有许多案例，则可以使用“筛选”选项：
 - 全部打开（默认）：使用此筛选器查看所有尚未解决的案例。
 - 未分配：如果您刚刚提交案例，但未收到任何案例状态已更改的通知，则使用此选项。请注意，根据提交的优先级（事件）或您的服务级别协议（服务请求），处理事件和服务请求案例的及时性会有所不同。

- 打开：如果您收到问题处于“待处理亚马逊”处理状态的通知，则使用；这意味着问题已分配但工作尚未开始。
 - 已@@ 重新打开：如果您收到问题解决后已重新审理的通知，请使用。
 - 处理中：如果您收到操作员已开始处理此案的通知，请使用。
 - 待处理的客户操作：如果您收到了操作员要求您采取行动的请求，则使用。
 - 客户操作已完成：如果您已收到通知，告知您对问题采取的操作已处理，则使用。
 - 已解决：用于查看已知已解决的案例。已解决的案例将在历史记录中保存十二个月。
 - 任何状态：使用此筛选器查看所有案例，无论其状态如何。
3. 要查看最新状态，请刷新页面。
 4. 如果有太多信件以至于没有全部显示在页面上，请选择“加载更多”。
 5. 要更新案例状态，请选择“回复”，输入新的信件，然后选择“提交”。
 6. 要在问题得到令您满意的解决后结案，请选择“关闭案例”。

请务必通过1-5星对服务进行评级，让AMS知道我们的表现如何！

使用 AWS Support API 管理事件

[AWS Support API](#) 使您能够创建事件，并在调查您的问题以及与 AWS Support 员工互动的整个过程中向事件添加信件。AWS Support API 模拟了 [AWS 支持中心](#) 的大部分行为。有关如何使用此 AWS 支持服务的更多详细信息，请参阅[编程 AWS Support 案例](#)。

Note

使用 AWS Support API 或 SAPI 处理 AMS 高级事件时，请使用以下服务代码：sentinel-report-incident。

响应 AMS 引发的事件

AMS 会主动监控您的资源；有关更多信息，请参阅[监控和事件管理](#)。有时，AMS 会识别并创建事件案例，通常是为了将事件通知您。如果您需要采取措施来解决事件，AMS 会向您为该账户提供的联系信息发送通知。你对这起事件的反应方式与对待任何其他事件的方式相同。您通常会通过 AMS 控制台对事件做出回应；在某些情况下，需要通过电子邮件或电话联系。

 Note

AMS 会将通信发送到您的 AWS 账户上的主电子邮件地址；我们建议您添加备用运营联系人电子邮件别名，以简化事件管理流程。AMS 入职流程和相关的入职文档中对此进行了介绍。如果您在入职期间向 AMS 提供了非基于资源的联系人（您已告知您的 CSDM），则会使用这些联系人。例如，您可以提供名为“SecurityContacts”的联系人列表，用于处理 CSDMs/CAs 与安全相关的事件或通知。instances/resources 如果您已同意 CSDM 使用标签信息，则您的联系人标签将用于 AMS 生成的事件。

要了解有关此通知服务的更多信息，请参阅[通知](#)。

服务请求管理

主题

- [何时使用服务请求](#)
- [服务请求管理的工作原理](#)
- [在 AMS 中测试服务请求](#)
- [在 AMS 中创建服务请求](#)
- [在 AMS 中监控和更新服务请求](#)
- [响应 AMS 生成的服务请求](#)

服务请求是指您发送给 AMS 的通信，要求您提供信息或建议。标准服务请求的一个很好的例子是在配置 AMS 服务（例如警报管理器、Patch Orchestrator 等）时寻求指导或帮助。您还可以接收来自 AMS 的服务请求；这些请求称为出站服务请求或服务通知。要查看 AMS 发送给您的服务请求和出站服务请求（服务通知）的列表，请查看 AMS 控制台的服务请求页面。

要了解有关出站服务请求的更多信息，请参阅[响应 AMS 生成的服务请求](#)。

您可以使用 AMS 控制台创建 AWS Managed Services (AMS) 服务请求，或者以编程方式使用 [支持 API](#) 创建 AWS Managed Services (AMS) 服务请求。有关使用 API 的详细信息，请参阅[支持 API](#)。对于 AMS，请选择sentinel-service-request服务代码。

AMS 运营团队收到您的服务请求后，将根据您的服务等级协议对其进行优先排序。要随时了解服务请求解决过程的每个步骤，请务必填写“抄送电子邮件”选项，而且，如果您要通过联盟进行连接，请在点击 AMS 发送的电子邮件中的链接之前登录。

使用 AMS 控制台“创建服务请求”页面执行以下任务：

- 创建和更新服务请求
- 获取有关您当前所有服务请求的列表和详细信息
- 按日期和事件标识符 (包括已解决的请求) 缩小对服务请求的搜索范围
- 在请求中添加通信和文件附件，并为案例通信添加电子邮件收件人
- 解决服务请求
- 对服务请求通信进行评分

何时使用服务请求

以下示例描述了服务请求：

- AMS 或 AWS 一般指导
- 补丁 MW 相关问题
- Backup 计划相关问题
- 有关 AWS 服务功能的问题

以下是不应在服务请求中提出的内容的示例：

- 访问问题
- 补丁失败
- Backup 失败
- RFC 故障或导致业务中断的 RFC (使用意外事件表示业务中断)
- RFC 问题或额外输入或更改 RFC 范围 (使用 RFC 双向对应)

服务请求管理的工作原理

服务请求由待命的 AMS 运营团队处理。

AMS 运营团队收到您的服务请求后，会对其进行审核，以确保该请求不会被更恰当地归类为事件。如果应将其归类为事件，则会立即对其进行重新分类，AMS 事件管理团队接管并通知您。

如果通过提交 RFC 可以解决服务请求，则审核操作员会向您发送一封电子邮件，要求您提交相应的 RFC (已提供详细信息)。

如果 AMS 操作员能够解决服务请求，则会立即采取相应措施。例如，如果服务请求是为了提供架构建议或其他信息，则操作员会将您推荐给相应的资源或直接回答问题。

如果对您的服务请求的分析发现了错误或功能请求，则 AMS 会通过服务请求向您发送通知。由于功能请求或错误修复没有预计到达时间，因此原始服务请求已关闭。有关原始服务请求的后续问题，请联系您的 CSDM。

如果服务请求超出了 AMS 运营的范围，运营商要么将请求发送给您的云服务交付经理，以便他们可以与您沟通，或者发送给相应的 AWS 运营团队，同时向您发送一封电子邮件，告知您正在采取哪些措施。

在您表示对结果感到满意之前，服务请求才会得到解决。

Note

我们建议在任何情况下都提供联系人电子邮件、姓名和电话号码，以便于沟通。

在 AMS 中测试服务请求

在测试 AMS 服务请求时，我们要求您在主题文本中包含以下标志：AMSTestNoOpsActionRequired 让 AMS 知道服务请求仅用于测试。当 AMS 运营工程师看到该标志时，他们不会对服务请求做出回应。

在 AMS 中创建服务请求

要使用 AWS Managed Services (AMS) 控制台创建服务请求，请执行以下操作：

1. 从左侧导航栏中选择“服务请求”。

服务请求列表打开。

如果您的服务请求列表为空，则清除筛选器选项会将筛选器重置为“任意”状态。

如果您知道要使用电话或聊天，请单击 Support Center 中的“创建服务请求”，在 Support Center Console 中打开服务请求创建页面，该页面会自动填充 AMS 服务类型。

 Note

通过支持中心发起的电话会被录音，以更好地提高响应能力。如果来电掉线，你必须通过 Support Center 案例回电，AWS 没有回电的机制。

 Important

电话和聊天支持旨在帮助处理支持案例、事件和服务请求。如果 RFC 问题，请使用相关 RFC 详细信息页面上的通信选项联系 AMS 工程师。

2. 如果要查找现有服务请求，请在下拉列表中选择服务请求状态筛选器。

- 所有尚未解决的服务请求。
- 尚未分配的新服务请求。
- 已分配的服务请求。
- 您重新打开的服务请求。
- 已分配的、复杂的服务请求。
- 需要您在下一步之前提供反馈的服务请求。
- 您最近向其提交信息的服务请求。
- 服务请求已结束。
- 账户中的所有服务请求。

3. 选择创建。

将打开“创建服务请求”页面。

4. 选择一个类别。

 Note

如果您要测试服务请求功能，请在服务请求标题中添加“不采取行动”标志 `AMSTestNoOpsActionRequired`。

5. 输入以下信息：

- 主题：这将在列表页上创建指向服务请求详细信息的链接。
- 抄送电子邮件：除了您的默认电子邮件联系人外，这些电子邮件还会接收信件。
- 详情：请在此处提供尽可能多的信息。

要添加附件，请选择“添加附件”，浏览到所需的附件，然后单击“打开”。要删除附件，请单击“删除”图
标：

6. 选择提交。

将打开一个详细信息页面，其中包含有关服务请求的信息，例如类型、主题、已创建、ID 和状态，以及一个包含您创建的请求描述的通信区域。

此外，您的服务请求会显示在服务请求列表页面上。当您收到警报但尚未收到来自 AMS 的消息时，请使用此选项。

单击“回复”以打开通信区域并提供更多详细信息或状态更新。

服务请求解决后，单击“解决问题”。

单击“加载更多”以查看不适合初始页面的其他信件。

别忘了给沟通打分！

对于与账单相关的查询，请从 Support Center Console 创建服务请求案例。

YouTube 视频：[如何以及何时从 AWS 控制台提出服务请求，其服务级别目标是什么？](#)

在 AMS 中监控和更新服务请求

您可以使用 AMS 控制台或以编程方式使用支持 API 更新、监控和查看事件报告和服务请求（均为已调用案例）。有关使用支持 API 的信息，请参阅[DescribeCases](#)操作。

要使用 AMS 控制台监控案例、事件或服务请求，请按照以下步骤操作。

1. 在 AMS 控制台的“事件报告”或“服务请求”控制面板中，浏览到案例并选择“主题”，打开包含当前状态和通信内容的详细信息页面。

当 AMS 运营团队更新已报告的事件或服务请求案例时，您会在 AMS 控制台中收到一封电子邮件和事件链接，以便您做出回应。您无法通过回复电子邮件来回复事件通信。

 Important

您必须输入电子邮件地址才能接收服务请求或事件案例的状态变更通知。通知仅发送到创建案例时添加到案例中的电子邮件地址。

除非您在 AMS 联合网络上使用电子邮件服务器，否则通知电子邮件中的链接将无法使用。但是，您可以前往 AMS 控制台并使用问题详情页面来回复信件。

2. 如果列表中有许多案例，则可以使用“筛选”选项：

- 全部打开（默认）：使用此筛选器查看所有尚未解决的案例。
- 未分配：如果您刚刚提交案例，但未收到任何案例状态已更改的通知，则使用此选项。请注意，根据提交的优先级（事件）或您的服务级别协议（服务请求），处理事件和服务请求案例的及时性会有所不同。
- 打开：如果您收到问题处于“待处理亚马逊”处理状态的通知，则使用；这意味着问题已分配但工作尚未开始。
- 已@@ 重新打开：如果您收到问题解决后已重新审理的通知，请使用。
- 处理中：如果您收到操作员已开始处理此案的通知，请使用。
- 待处理的客户操作：如果您收到了操作员要求您采取行动的请求，则使用。
- 客户操作已完成：如果您已收到通知，告知您对问题采取的操作已处理，则使用。
- 已解决：用于查看已知已解决的案例。已解决的案例将在历史记录中保存十二个月。
- 任何状态：使用此筛选器查看所有案例，无论其状态如何。

3. 要查看最新状态，请刷新页面。

4. 如果有太多信件以至于没有全部显示在页面上，请选择“加载更多”。

5. 要更新案例状态，请选择“回复”，输入新的信件，然后选择“提交”。

6. 要在问题得到令您满意的解决后将其结案，请选择“关闭案例”。

请务必通过1-5星对服务进行评级，让AMS知道我们的表现如何！

响应 AMS 生成的服务请求

AMS 补丁管理会在您设定的维护时段之前向您发送服务请求（又名服务通知）；有关更多信息，请参阅 [AMS 维护时段](#)。当您的基础设施可能受到某项服务的影响或您的账户中的某个 EC2 实例可能需要重启时，AMS 还会向您发送 AWS 服务通知；有关更多信息，请参阅 [服务通知](#)。

Note

AMS 会将通信发送到您 AWS 账户中您提供的主电子邮件地址；我们建议您添加备用运营联系人电子邮件别名，以简化服务请求或服务通知管理流程。在 AMS 入职流程和相关的入职文档中，将介绍如何添加这些电子邮件。

账单问题

要提交与账单相关的问题，请完成以下步骤：

1. 在家中打开 [AWS 支持 中心](https://console.aws.amazon.com/support/#/) <https://console.aws.amazon.com/support/#/>。
2. 选择“账户和账单”。
3. 选择创建案例。
4. 选择“账户和账单”，然后按照提示提交您的案例。

按需运营

按需运营 (OOD) 是 AWS Managed Services (AMS) 的一项功能，它通过提供 AMS 运营计划当前未提供的运营服务来扩展您的 [AMS 运营计划](#) 的标准范围，或 AWS 者。选定后，目录产品将由自动化和高技能的 AMS 资源组合提供。没有长期承诺或额外合同，允许您根据需要扩展现有的 AMS 以及 AWS 运营和能力。您同意按月购买时段（OOD 区块），每个区块 20 小时。

您可以从标准化产品目录中进行选择，并通过服务请求启动新的 OOD 项目。OOD 产品的示例包括协助维护 Amazon EKS、SAP 集群的 AWS Control Tower 运营和管理。我们会根据需求和我们最常看到的运营用例定期添加新的目录产品。

OOD 可用于 AMS Advanced 和 AMS Accelerate 运营计划，并且适用于所有可用 AMS [AWS 区域](#) 的地方。

AMS 在实施您请求的更改时执行客户安全风险管理体系 (CSRM)。要了解有关 CSRM 流程的更多信息，请参阅 [更改请求安全审查](#)。

按需运营产品目录

按需操作 (OOD) 为您提供下表中所述的服务。



Note

有关术语的定义，请参阅 AWS Managed Services 文档[术语](#)。

运营计划	标题	说明	预期成果
AMS Accelerate	亚马逊 EKS 集群维护	AMS 通过处理您的亚马逊 Elastic Kubernetes Service（亚马逊 EKS）部署的持续维护，让您的容器开发人员腾出时间。AMS 执行更新集群所需的 end-to-end 程序，包括控制平面、插件和节点的组件。AMS 对托管节点类型以及一组精选的 Amazon EKS 和 Kubernetes 插件进行更新。	客户团队协助完成了更新 Amazon EKS 集群的底层运营工作。

AMS Accelerate	AMI 大楼和自动售货机	AMS 为客户提供 AMI 大楼和自动售货机的持续管理。 我们的工程师每月发布订阅版 AMIs，AMIs 针对紧急修补活动按需发布，使用运行手册管理变更，并使用监控监控 AMI 构建。CloudWatch 我们还为指定账户中的所有 AMIs 用户提供故障排除帮助和详细报告。此产品要求通过 EC2 映像生成器部署 AMI 构建管道。AMS 不支持任何其他与 EC2 图像生成器交互的自动化或服务。	客户安全状况得到改善，AMIs 减少了客户在建筑和自动售货上花费的时间。
AMS Accelerate	精心策划的变更执行	与我们熟练的运营工程师合作，将您的业务需求转化为可在您的 AWS 环境中安全执行的经过验证的变更请求。无论是简单的规模变更还是具有下游影响的复杂行动，都可以利用我们独特的自动化方法和最佳运营实践（例如，影响评估、回滚、两人规则）。	帮助客户定义、创建和执行自定义变更请求。更改可以是手动的，也可以是自动的（CloudFormation，SSM）。必要时包括咨询以支持获取配置指导。不适用于更改应用程序代码、应用程序安装/部署、数据迁移或操作系统配置更改。

AMS Accelerate	AWS Network Firewall 操作	AMS 与您合作，为您的防火墙加入并实施和管理持续防火墙操作的策略和规则。为此，我们的工程师利用我们的最佳运营实践和自动化来配置标准化的策略和规则，并启用监控功能以检测自动化流程之外所做的更改。AMS 会迅速通知您不需要的更改，并提供选项，以便在需要时将其包括在内，或者将账户恢复到之前的配置，以确保系统的整体稳定性。	客户团队通过快速检测网络防火墙的意外更改来帮助减少管理开销，从而改善了事件解决方案，缩短了预期和意外问题的根本原因分析时间。
AMS Accelerate	AWS Control Tower 操作	持续运营和管理您的 AWS Control Tower 着陆区，包括T AWS ransit Gateway和 AWS Organizations——提供全面的着陆区解决方案。我们使用我们的自定义控件和护栏库处理账户自动售卖、SCP 和 OU 管理、漂移补救、SSO 用户管理以及 AWS Control Tower 升级。	客户团队协助完成了管理 AWS Control Tower、T AWS ransit Gateway 和 AWS Organizations.
AMS Accelerate	AWS landing zone 加快行动	AMS 提供通过 AWS 着陆区加速器 (LZA) 部署的 AWS 着陆区的持续运营。 我们的工程师负责配置文件更改、AWS Control Tower (CT) 环境管理 (账户售卖、OU 创建、CT 护栏)、服务控制策略 (SCP) 管理、CT 漂移检测和修复、网络配置管理以及 CT 和 LZA 框架的更新。AWS LZA 提供了一种使用最佳运营实践和服务 (例如) 来设置和管理安全的多账户 AWS 环境的方法。 AWS Control Tower	客户团队为 AWS 着陆区加速器解决方案的持续运营和管理提供了协助。

AMS Accelerate	SAP 集群协助	为您的 SAP 集群提供专门的警报、监控、集群修补、备份和事件修复。此目录项允许您从 SAP 运营团队中卸下一些正在进行的运营工作，以便他们可以专注于容量管理和性能调整。	客户或合作伙伴 SAP 团队协助完成了一些底层运营工作。仍然需要客户提供其他 SAP 功能，例如容量管理、性能调整、数据库管理员和 SAP 基础管理。
AMS Accelerate	EC2 操作中的 SQL Server	AMS 与您协作，对部署在 EC2 实例上的 SQL Server 数据库进行登记、实施和管理其持续操作。 我们的工程师利用我们的最佳运营实践和自动化，通过执行备份和修补等任务、将 AMS 运营支持扩展到 SQL Server 补丁以包括集群感知滚动更新、符合我们的勒索软件防御策略的备份和还原服务，以及监控客户提供的备份和补丁控制的遵守情况，从而腾出您的数据库团队。	SQL Server 客户协助卸载修补和备份数据库操作，以提高其工作负载的弹性和安全状况，此外还通过自带许可证 (BYOL) 来优化许可成本。 EC2
AMS 高级版	亚马逊 EKS 集群维护	AMS 通过处理您的亚马逊 Elastic Kubernetes Service (亚马逊 EKS) 部署的持续维护和运行状况来解放您的容器开发人员。AMS 执行更新集群所需的 end-to-end 程序，包括控制平面、插件和节点的组件。AMS 对托管节点类型以及一组精选的 Amazon EKS 和 Kubernetes 插件进行更新。	客户团队协助完成了更新 Amazon EKS 集群的底层运营工作。

AMS 高级版	优先执行 RFC	指定 AMS 运营工程师能力，可优先执行您的变更请求 (RFC)。通过Amazon Chime会议室直接与工程师互动，可以对所有提交的内容进行更高级别的回应，并且可以调整优先顺序。	买家会收到 8 小时的回复 SLO。RFCs
AMS 高级版和 AMS 加速版	旧版操作系统升级	通过将实例升级到支持的操作系统版本来避免实例迁移。我们可以利用软件供应商的自动化和升级功能（例如，从微软 Windows 2008 R2 到微软 Windows 2012 R2）对您选定的实例进行就地升级。这种方法非常适合无法轻易在新实例上重新安装的旧版应用程序，并且在较旧的操作系统版本上提供了额外的保护，使其免受已知和未缓解的安全威胁。 支持以下操作系统进行就地升级： • 微软 Windows 2012 R2 到微软 Windows 2016 及更高版本 • 微软 Windows 2016 到微软 Windows 2022 及更高版本 • 红帽企业 Linux 7 到红帽企业 Linux 8 • 红帽企业 Linux 8 到红帽企业 Linux 9 • 甲骨文 Linux 7 到甲骨文 Linu	此解决方案适用于无法再在新实例上重新安装的应用程序（例如，源代码丢失、I SV 停业等）。您可以将失败的升级恢复到其原始状态。从操作角度来看，回滚是首选，因为它使用最新的安全补丁可以使实例处于更可支持的状态。

主题

- [按需请求 AMS 操作](#)
- [对按需运营产品进行更改](#)

按需请求 AMS 操作

AWS Managed Services (AMS) 按需运营 (OOD) 适用于所有 AWS 账户 已加入 AMS 的用户。要利用按需运营，请向您的云服务交付经理 (CSDM)、解决方案架构师 (SA)、客户经理或云架构师 (CA) 索取更多信息。前面的[按需运营产品目录中列出了可用的 OOD 产品](#)。项目范围界定完成后，向 AMS 运营部门提交服务请求以启动 OOD 项目。

每个 OOD 服务请求都必须包含与项目相关的以下详细信息：

- 所要求的具体 OOD 产品以及每种特定的 OOD 产品：
 - 分配给特定 OOD 产品的区块数量（一个区块等于给定日历月内的 20 小时运营资源时间，按当时 AWS 的标准费率为适用的按需运营产品收费）。
 - 申请特定 OOD 产品的每个 AWS Managed Services 账户的账户 ID。

OOD 服务请求必须由您通过以下任一方式提交：

- 接收适用的按需运营产品的 AWS Managed Services 账户，或
- AWS Man AWS Organizations aged Services 账户，代表其任何成员账户（即 AWS Managed Services 账户）处于所有功能模式的管理账户。

收到 OOD 服务请求后，AMS Operations 会审核并更新账户的批准、部分批准或拒绝。

OOD 提供的服务请求获得批准后，AMS 和您就会协调开始合作。在服务请求获得批准并商定项目开始日期之前，不会启动 OOD 产品。

AMS 使用按月订阅的 OOD 区块分配。我们每月分配批准的区块数量，从参与开始日期开始，直到您通过新的服务请求申请退出。OOD 区块在一个日历月内有效。未使用的区块或区块部分不会结转或结转到未来的月份。

无论实际使用的小时数如何，您每月至少需要支付一个 OOD 区块的费用。任何未使用工时的额外分配的 OOD 区块均不计费。

对按需运营产品进行更改

要申请更改按需运营 (OOD) 产品的持续参与，请提交包含以下信息的服务申请：

- 请求的修改，以及
- 所请求的修改生效日期。

收到 OOD 服务请求后，AMS Operations 会审查该请求并更新其批准情况，或者要求分配的 CSDM 与您合作确定修改的范围和影响。如果确定修改需要与 CSDM 进行范围界定，则您需要在范围界定工作完成后提交第二份 OOD 服务请求以启动修改后的项目。

获得批准后，最近修改的区块分配将变为并继续保持活跃状态，取代之前的任何区块分配，除非您 AWS 和您另行同意。

文档历史记录

下表描述了《AMS 高级用户指南》每个版本中的重要更改。要获得本文档的更新通知，您可以订阅 RSS 源。

- API 版本：2019-05-21
- 新增或更新 CTs 以及演练：[AMS 高级更改类型参考文档历史记录](#)。
- 全新 AMS AMIs:[AMS Amazon 机器映像 \(AMIs\)](#)。

变更	说明	日期
更新了 AMS 高级部分标准控件中的 AWS Identity and Access Management (IAM) 表	更新了表格中有关 IAM 策略和 Amazon S3 存储桶访问权限的信息。	2025年9月25日
更新了账单相关查询的步骤	在 AMS 中创建服务请求部分更新了为账单相关查询创建服务请求的步骤。	2025年9月25日
更新了变更类型的电子邮件通知信息	在配置 RFC 电子邮件通知（控制台）部分更新了为更改类型添加电子邮件通知的信息和示例。	2025年9月25日
更新了更改类型	更新了 AMS 基础设施自动标记部分，其中包含用于标记 AMS 创建的资源的更改类型。	2025年9月25日
Import/Export 在 AWS Managed Services 常见问题中更新了虚拟机	更新了用于请求实例配置文件的 RFC，以允许工具从实例执行命令。	2025年9月24日
更新了启动适用于 SAP Applications 的 SUSE Linux 企业服务器 15 实例的变更请求 (RFC) SP6	更新了如何使用正确的 RFC 启动适用于 SAP Applications 15 的新 SUSE Linux 企业服务器 15 SP6 实例下的步骤 2。	2025年9月22日

更新的变更申请 (RFC)	AWS Elastic Disaster Recovery 在 AWS Managed Services 常见问题解答部分更新了正确的 RFC，以便在您的账户中创建所需的 IAM 角色。	2025年9月22日
新增了 4 项受可信修正者支持 Trusted Advisor 的成本优化检查	添加了以下成本优化检查： • c1z7kmr00n-亚马逊针对实例的成本优化建议 EC2 • c1z7kmr02n-亚马逊 EBS 关于批量的成本优化建议 • c1z7kmr03n-针对数据库实例的 Amazon RDS 成本优化建议 • c1z7kmr05n-函数的成本优化建议 AWS Lambda	2025年9月22日
更新了可用区说明 (AZs)	更新了有关 AMS 中安全组的信息。	2025 年 9 月 5 日
更新了更改类型	FSx 在 AWS Managed Services 常见问题解答部分中更新了亚马逊，更改了将托管 AD 共享到应用程序账户。	2025 年 9 月 5 日
更新了更改类型	在 AWS Managed Services 常见问题解答部分更新了 Amazon DocumentDB，将类型更改为使用删除。APIs	2025 年 9 月 5 日
更新了更改类型	更新了 AWS Managed Services 常见问题解答部分中的 Alexa for Business，将类型更改为两个访问受限的 IAM 用户，用于安装和操作您的 Alexa for Business 网关。	2025 年 9 月 5 日

更新了更改类型	在 AWS Managed Services 常见问题解答部分中更新了 AppStream 2.0，更改了创建和选择将在所有队列流实例上可用的 IAM 角色	2025 年 9 月 5 日
更新了更改类型	EventBridge 在 AWS Managed Services 常见问题解答部分中进行了更新，更改了在使用 EventBridge 触发其他 AWS 资源之前请求 EventBridge 服务角色的类型。	2025 年 9 月 5 日
更新了可信修正者对 Trusted Advisor 安全检查的支持	更新了支票 Hs4ma3G108 支持的预配置参数和约束条件——跟踪 CloudTrail 应与 Amazon Logs 集成 CloudWatch	2025 年 9 月 5 日
更新了可信修正者对 Trusted Advisor 安全检查的支持	更新了 Trusted Advisor 安全检查以添加 Hs4Ma3G184 版本 2-应启用应用程序负载均衡器和经典负载均衡器日志记录	2025 年 9 月 5 日
更新了由“可信修正者”部分支持的卓越 Trusted Advisor 运营检查	更新了 Trusted Remediator 支持的卓越 Trusted Advisor 运营检查部分，添加了新的支持检查 c1fd6b96l4 Amazon S3 访问日志已启用。	2025 年 8 月 28 日
更新了更改类型	更改自定义 IAM 角色的类型。	2025 年 8 月 25 日
在 AMS 部分中使用适用于 .Net 和 SQL Server 的 CloudWatch 应用程序见解进行了更新	修改了更改类型以使用“CloudWatch 应用程序见解”。	2025 年 8 月 25 日
更新的变更申请 (RFC)	请求更改 (RFC) 以向 Amazon S3 存储桶添加更多标签。	2025 年 8 月 25 日

更新的变更申请 (RFC)	变更请求 (RFC)，用于标记 AMS 出于管理目的创建的所有资源。	2025 年 8 月 25 日
更新了 AWS Managed Services 常见问题解答部分中的 Lambda	修改了访问其他 AWS 服务以创建事件源的更改类型。	2025 年 8 月 25 日
更新了 AWS Managed Services 常见问题解答部分中的 Lambda	修改了配置 Lambda 函数的更改类型。	2025 年 8 月 25 日
更新了创建、更改或删除安全组部分	修改了更改类型，以便在堆栈之外创建安全组，以及 VPCs	2025 年 8 月 25 日
更新了“可信修正者”部分，加入了 Compute Optimizer 的新内容	更新了“可信修正者”部分，加入了支持的 AWS Compute Optimizer 建议的新内容。	2025 年 8 月 18 日
已移除 TOC 词汇表链接	AWS 词汇表 。	2025 年 8 月 8 日
精确的更改类型推荐	要将您的客户指标集成到您的应用程序监控系统中，请提交 RFC 并附上部署 监控和通知 SNS 创建 CT (ct-3dfnglm4ombbs)，请求 AMS 为该指标创建 Amazon SNS 主题。	2025 年 8 月 8 日
精确的更改类型推荐	要删除占位符实例卷，请提交管理 高级堆栈组件 EBS 卷 删除更改类型 (ct-3e3h8u0sp5z80)。	2025 年 8 月 8 日
新的监控警报：SecureChannelFailure 以及安全通道中断	AMS 中基线监控产生的警报自动修复警报 。	2025 年 8 月 8 日

新的可信修正者检查	Trusted Advisor 成本优化检查由 Trusted Remediator Hs4ma3G120— AWSManagedServices-TerminateEC 2 InstanceStoppedForPeriodOfTime、Hs4ma3G230—2 和 c18d2gz150—2 和 c18d2gz150—2 支持的受信任修复者 Trusted Advisor 安全检查支持 。AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV AWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime	2025 年 8 月 8 日
在第 3.2 点中更新 IAM 标准	澄清了措辞并删除了对标签的提及。	2025 年 7 月 25 日
更新警报选择退出选项	添加标签允许您选择退出另外两个警报。	2025 年 7 月 25 日
自助服务配置服务已弃用	CloudEndure 自助服务配置服务已被弃用，取而代之 AWS Application Migration Service 的是。	2025 年 7 月 25 日
备份的新功能	使用新标签自定义备份保管库的通知。	2025 年 7 月 25 日
更新了控制表	移除了 AMS-STD-002-AWS Identity and Access Management (IAM) 表格部分中的一些重复控件。	2025 年 6 月 26 日
更新了 SSP 服务先决条件 AWS Transfer Family	在“先决条件”部分中添加了信息。	2025 年 6 月 26 日

更新了 IAM 策略示例	按照建议更新了 IAM 策略示例，增加了更多限制。	2025 年 6 月 26 日
支持更新的 AMI OSes	在 Ubuntu Linux 22.04 下添加了 Ubuntu Linux 24.04，并将所有引用更改为。 SP5 SP6	2025 年 6 月 26 日
自助配置服务，MediaStore 已弃用	添加了的弃用说明。 AWS Elemental MediaStore	2025 年 6 月 26 日
Amazon Inspector Classic 自助配置服务已弃用	为亚马逊 Inspector Classic 添加了弃用说明。	2025 年 6 月 26 日
自助配置服务，Amazon Connect 已弃用	为 Amazon Connect 添加了弃用说明。	2025 年 6 月 26 日
更新了 AMS 中支持的配置部分	更新了 AMS 中支持的操作系统和支持的终止支持 (EOS) 操作系统的支持配置。	2025 年 6 月 25 日
自助配置服务，WorkDocs 已弃用	删除了页面和对已弃 WorkDocs 用的引用。	2025 年 6 月 19 日
补丁管理备用补丁存储库的重要安全说明	在 AMS 中使用备用补丁存储库的重要安全说明和最佳实践。	2025 年 6 月 10 日
支持的操作系统更新	AMS Advanced 支持的操作系统已更新，有些已添加，有些已删除。	2025 年 5 月 22 日
仅限内部 APIs	仅限内部 APIs ，出现在某些 CloudWatch 日志中。	2025 年 5 月 22 日
AMS 可信修正者更新	如何使用新参数在 Trusted preconfigured-parameters Remediator 中自定义 Trusted Advisor 检查。	2025 年 5 月 22 日

SSP Amazon 弹性容器注册表更新	当您加入 Amazon ECR 服务时，系统会自动配置更多角色。	2025 年 5 月 8 日
AMS 高级可信修正器常见问题解答和更新。	对支持的 Trusted Advisor 检查进行了多项更新，Trusted Remediator 常见问题解答 (已添加 “Trusted Remediator 向您的账户部署了哪些资源？”) ，以及更多。另请参阅 可信修正者支持的Trusted Advisor 检查 。	2025 年 5 月 8 日
AMS 高级标准安全控制更新。	添加了 “安全组共享” 控件。	2025 年 5 月 8 日
AMS 高级受保护的命名空间。	AMS 保护了命名空间EPSMarketplaceSubscriptionRole 并EPS已添加。	2025 年 4 月 24 日
AMS 高级日志位置。	添加了其他日志位置。	2025 年 4 月 24 日
适用于 AppStream 2.0 先决条件更新的 AMS 高级自助服务配置模式。	已添加 AppStream 2.0 的先决条件：在提交服务的预配置 RFC 时，必须包含 Amazon S3 存储桶名称。	2025 年 4 月 24 日
AMS 高级全新 Amazon RDS 自动修复警报。	警报 ID：-0224，当请求的分配存储空间达到或超过配置的最大存储阈值时触发。	2025 年 3 月 27 日
AMS Advanc AWS ed 已于 2024 年 7 月 25 CloudSearch 日起关闭新买家访问亚马逊的权限。	现有客户仍然可以使用该服务，但不会有新功能。	2025 年 3 月 27 日

AMS Advanced AWS ed 已从 2024 年 7 月 25 日起关闭新客户访问权限。AWS CodeCommit	现有客户仍然可以使用该服务，但不会有新功能。	2025 年 3 月 27 日
可信修正者现已可用。	Trusted Remediator 是一款可自动修复 AWS Trusted Advisor 支票的 AWS Managed Services 解决方案，现已上市。	2025 年 3 月 19 日
AMS 高级全新自动修复 RDS 警报。	RDS-EVENT-0224 已添加。	2025 年 3 月 17 日
AMS 高级新功能：事件通知。	您可以使用 AppRegistry 创建应用程序并自定义这些应用程序的事件通知。	2025 年 3 月 13 日
AMS 更新到 RDS 警报监控阈值。	RDS 平均 CPU 使用率警报阈值已从 75% 更改为 90%。	2025 年 2 月 20 日
更新了自助服务报告，增加了用于查看汇总报告的新数据选项	为以下自助服务报告添加了数据选项Admin Account ID，以包括新的字段名:aws_admin_account_id、数据集字段名:Trusted AWS Organization account enabled by the customer和定义： - 补丁报告（每日） - Backup 报告（每日） - 事件报告（每周）	2025 年 1 月 28 日

对 AWS Batch SSP 的更新	您可以使用以下 RFC 在您的 AMS 账户 AWS Batch 中进行配置：管理 AWS 服务 自配置服务 添加 (ct-1w8z66n899dct)。	2025 年 1 月 28 日
AMS 新功能：聚合自助服务报告	聚合自助服务报告 (SSR) 为您提供在组织层面、跨账户汇总的现有自助服务报告的视图。	2025 年 1 月 21 日
更新 Forecast SSP 部分	补充说明：AWS 已关闭新买家访问 Amazon Forecast 的权限，自 2024 年 7 月 29 日起生效。Amazon Forecast 现有客户可以继续照常使用该服务。	2025 年 1 月 10 日
更新到 AMS 保护的命名空间部分	在 AMS 保护的命名空间列表中添加了一个缺失的受保护命名空间 (*mc、*MC 和 *Mc)。	2025 年 1 月 9 日
“监控工作原理”部分的更新	添加了有关新功能的信息，即按资源或实例 ID 而不是按事件配置警报通知。	2025 年 1 月 8 日
更新：基于标签的更新内容	修复了 keyname 中的错别字并更正了错误的配置文件路径。	2025 年 1 月 6 日
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	2024 年 11 月 21 日
更新了按需运营产品表	支持以下操作系统进行就地升级： • 微软 Windows 2016 到微软 Windows 2022 及更高版本	2024 年 11 月 11 日

更新了按需运营产品表	支持以下操作系统进行就地升级： • 微软 Windows 2012 R2 到微软 Windows 2016 及更高版本 • 红帽企业 Linux 7 到红帽企业 Linux 8 • 红帽企业 Linux 8 到红帽企业 Linux 9 • 甲骨文 Linux 7 到甲骨文 Linu	2024 年 11 月 1 日
更新了支持的配置	将支持的 Oracle Linux 操作系统更新到 9.0-9.3、8.0-8.9、7.5-7.9。	2024 年 10 月 24 日
更新了 AMS Amazon 机器映像 (AMIs)	更新了基于 Windows 的，删除了 AMIs Windows 2012 和 2012 R2。更新了基于 Linux 的 AMIs 版本，删除了几个不再支持的 AMI，并添加了以下内容： • 亚马逊 Linux (2ARM64) • RHEL 9 • SUSE Linux 企业服务器 15 SP5	2024 年 10 月 24 日
现在，您可以在基于标签的警报中包含多个电子邮件地址。	基于标签的警报现在支持多个电子邮件地址。	2024 年 9 月 20 日
添加了变更请求安全审查部分。	添加了一个新部分，其中提供了有关变更请求安全审查流程的详细信息。	2024 年 9 月 17 日

添加了新章节。	现已推出一个新章节，介绍在 AMS Advanced 中如何进行变更请求安全审查。	2024 年 9 月 12 日
AMS Advanced 支持的新服务。	AWS Resilience Hub 现在由 AMS 高级版支持。	2024 年 8 月 30 日
AMS Advanced 支持的新服务。	AMS Advanced 现在支持五项新服务： • Amazon Bedrock • Amazon Kendra • Amazon Quantum Ledger Database (Amazon QLDB) • AWS Service Catalog AppRegistry • Amazon Managed Service for Prometheus	2024 年 8 月 21 日
新的端点安全网络默认设置现已推出。	更新源现在包含在 EPS 默认网络设置中。	2024 年 8 月 21 日
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	2024 年 7 月 30 日
AMS 现在支持 Amazon Route 53 解析器 DNS 防火墙。	AMS 现在支持 Amazon Route 53 解析器 DNS 防火墙	2024 年 7 月 30 日
AWS DataSync SSP 更新	AWS DataSync 不再需要在 Amazon S3 存储桶名称上加上“数据同步-”前缀。	2024 年 7 月 30 日
安全 Config 规则控制面板	Security Config 规则控制面板现已在自助服务报告中提供。	2024 年 7 月 24 日

AMS 现在支持 Oracle Linux 8.9、RHEL 8.10 和 RHEL 9.4。	AMS 现在支持 Oracle Linux 8.9、RHEL 8.10 和 RHEL 9.4。	2024 年 7 月 5 日
Amazon Bedrock 现已在自助配置模式下推出	现在，您可以在 AMS SSP 模式下申请 Amazon Bedrock。	2024 年 6 月 27 日
安全事件响应中的 Amazon Route 53 Resolver DNS 防火墙事件	AMS 现在可以在安全事件响应中监控 Amazon Route 53 解析器 DNS 防火墙事件	2024 年 6 月 21 日
添加了有关如何启用 AMS 自带 EPS (BYOEPS) 功能的更多信息。	添加了有关如何启用 AMS 自带 EPS (BYOEPS) 功能的更多信息。	2024 年 6 月 5 日
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	2024 年 5 月 23 日
添加了有关 AWS Amplify 在自助服务配置模式下使用自定义角色的信息 (仅限 MALZ 环境)。	添加了有关 MALZ 环境如何在自助配置模式下使用自定义角色 AWS Amplify 的说明。	2024 年 5 月 23 日
Amazon Kendra 现已在自助配置模式下推出。	Amazon Kendra 现已在自助配置模式下推出。	2024 年 5 月 23 日
AMS 高级版支持其他操作系统。	AMS Advanced 支持红帽企业 Linux (RHEL) 9.x 以及 Ubuntu 20.04 和 22.04。	2024 年 4 月 25 日
AMS Advanced 支持亚马逊 Linux 2 的 ARM64 架构。	AMS Advanced 支持亚马逊 Linux 2 的 ARM64 架构。	2024 年 4 月 25 日
从多账号着陆区 (MALZ) 着陆区账户部分更新了 Offboard。	添加了有关如何从多账户 landing zone 中移除应用程序和核心账户的详细信息。	2024 年 4 月 11 日

更新：服务请求管理说明。	更新了服务描述主题中的服务请求管理描述。	2024 年 3 月 21 日
更新：事件管理服务承诺部分。	添加了 AMS 服务等级协议的链接。	2024 年 3 月 21 日
更新：服务请求管理的工作原理部分。	添加了对 AMS 如何处理包含功能请求或错误的服务请求的说明。	2024 年 3 月 21 日
更新：获取支持部分。	更新了“获取支持”部分，加入了新的账单问题部分。	2024 年 3 月 21 日
更新：AMS 自动配置 IAM	使用自定义拒绝列表信息更新了 AMS 自动 IAM 配置	2024 年 3 月 21 日

早期更新

下表描述了 2024 年 3 月之前 AMS 高级指南文档的重要更改。

更改	描述	链接
2024 年 2 月		
更新的支持的操作系统	更新了支持的操作系统以包括 SUSE Linux 企业服务器 15 SP5。	请参阅 支持的配置 。
在 AMS 中为来自基线监控的警报添加了注释。	添加了注释，表示默认情况下，EC2 非根卷使用量警报处于禁用状态。	请参阅 来自 AMS 基线监测的警报 。
在“监控和事件管理”中添加了新的“AMS 事件路由器”部分。	添加了讨论 AMS 高级事件路由器的新章节。	请参阅 在 AMS 中使用亚马逊 EventBridge 托管规则 。
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	见 AMIs。 csv-and-notes.02.2 024

更改	描述	链接
2024 年 2 月		
为 AMS Advanced 的 Amazon EventBridge 规则服务相关角色添加了一个新部分	在“基础设施安全”部分添加了针对 AMS Advanced 的 Amazon EventBridge 规则服务相关角色的新部分。	请参阅 AMS 高级版的 Amazon EventBridge 规则服务相关角色
更新了自助服务配置模式部分	为自助服务配置模式下的新 Amazon Inspector 添加了一个新部分。	参见 亚马逊 Inspector Classic (AMS SSP)
2024 年 1 月		
更新了计划活动管理 (PEM) 部分	在计划活动管理 (PEM) 中添加了更多细节和常见问题。	请参阅 AWS Managed Services 中的计划活动管理 。
为 SSM Agent auto 自动安装添加了新章节	在自动 EC2 实例配置中添加了有关 SSM Agent 自动安装的新部分。	请参阅 SSM 代理自动安装 。
已添加 AWS Resilience Hub (AMS SSP)	添加了一项新的 SSP 服务。	请参阅 使用 AMS SSP AWS Resilience Hub 在您的 AMS 账户中进行预配置 。
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	见 AMIs。 csv-and-notes.01.2024
2023 年 12 月		
更新了 AMS 中的“直接更改”模式	在 AMS 的直接更改模式中添加了新的小节“直接更改模式用例”。	请参阅 AMS 中的直接更改模式 。
已更新 AWS Amplify (AMS SSP)	更新了常见问题解答，以阐明申请 Amplify 需要风险接受才能申请 Amplify。	请参阅 使用 AMS SSP AWS Amplify 在您的 AMS 账户中进行配置 。

更改	描述	链接
全新 AWS Elastic Disaster Recovery (AMS SSP)	添加了新的 SSPS 服务	请参阅 使用 AMS SSP AWS Elastic Disaster Recovery 在您的 AMS 账户中进行配置 。
适用于 Prometheus 的全新亚马逊托管服务 (AMS SSP)	添加了新的 SSPS 服务	请参阅 使用 AMS SSP 在您的 AMS 账户中为 Prometheus 配置亚马逊托管服务 。
更新了连续性管理的工作原理部分。	添加了一个新的小节“AMS 备份监控和报告”。	请参阅 连续性管理的工作原理 。
全新 Amazon DevOps Guru (AMS SSP)	添加了新的 SSPS 服务	请参阅 使用 AMS SSP 在你的 AMS 账户中配置亚马逊 DocumentDB (兼容 MongoDB) 。
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	请参阅 AMIs。 csv-and-notes.12.2023
2023年11月		
更新了 Amazon S CloudWatch Synthetics (AMS SSP)	已更新 FAQs 为使用正确的角色名称。	请参阅 使用 AMS SSP 在你的 AMS 账户中配置 Amazon CloudWatch Synthetics 。
更新了 Amazon API Gateway 自助配置模式	在 API Gatew customer_apigateway_cloudwatch_role ay 部分添加了一个额外的角色。	请参阅 使用 AMS SSP 在你的 AMS 账户中配置 Amazon API Gateway 。
在自助服务配置模式中添加了一项新服务	已 AWS Service Catalog AppRegistry 添加到自助服务配置模式部分	请参阅 使用 AMS SSP AWS Service Catalog AppRegistry 在您的 AMS 账户中进行配置 。

更改	描述	链接
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	请参阅 AMIs。 csv-and-notes.11.2023
2023年9月		
为使用 Patch Orchestrator 添加了注释	在“使用 Patch Orchestrator”部分中添加了以下注释： “不会为操作系统不支持的实例创建补丁失败警报，也不会为在维护时段内停止的实例创建补丁失败警报”	请参阅 AMS 中的补丁管理 。
使用其他服务更新了数据加密	在 AMS 中为数据加密添加了服务。	请参阅 AMS 中的数据保护 。
在 RFC 错误消息中添加了新段落。	添加了一个新段落来添加创建服务请求链接。	请参阅 对 AMS 中的 RFC 错误进行故障排除 。
更正了 IAM 角色名称。	更正了 IAM 角色名 customer_emr_cluster_autoscaling_role。	请参阅 AMS 中的自助服务配置模式 。
更新了基准监控信息	删除了对两个已弃用警报的引用 RDSReadLatencyAlarm 和。 RDSWrite LatencyAlarm	请参阅 来自 AMS 基线监测的警报 。
2023年8月		
新增：AMS 安全事件响应	添加了有关使用 AMS 安全事件响应的文档。	请参阅 AMS 中的安全事件响应 。
2023年7月		
新增：自动化 IAM 预配置	添加了有关使用自动 IAM 配置的文档。	请参阅 自动化 IAM 配置 AMS 。

更改	描述	链接
更新：访问角色表	为 AMS Access 添加了缺少的角色。	请参阅 AMS 客户账户访问权限 IAM 角色 。
2023年6月		
更新：受监控的 RDS 警报列表。	更新了 AMS 基线监控的 RDS 警报列表。添加了 9 种新的 RDS 警报类型，删除了 3 种现有的 RDS 警报类型。	请参阅 来自 AMS 基线监测的警报 。
更新：访问角色表	AMS Security 的新角色。	请参阅 AMS 客户账户访问权限 IAM 角色 。
2023年5月		
更新：服务计费开始日期政策。	更新了账单开始日期的定义。	请参阅 AMS 关键术语 。
2023年4月		
更新：每月账单自助服务报告。	新增说明：月度账单报告仅适用于管理付款人账户（AMS Advanced 多账户登陆区），但适用于所有关联的 AMS Accelerate 管理的账户。	请参阅 账单报告（每月） 。
更新：移除了“标准补丁”内容	AMS 使用补丁协调器。	AMS 中的补丁管理
更新：什么是 AMS？	将之前的一些话题移到了什么是 AMS？成为 AMS 服务说明的一部分。	服务描述
更新：退出多账号着陆区	做了各种澄清。	退出 AMS 多账号 landing zone 账号

更改	描述	链接
更新：AWS Transfer Family (AMS SSP)	添加了转接设置教程的链接。	使用 AMS SSP AWS Transfer Family 在您的 AMS 账户中进行配置
更新内容：自助配置	根据 AWS 法律，将 “” 替换为 “代码服务”。CodeSuite	使用 AMS SSP 在您的 AMS 账户中配置 AMS 代码服务
更新内容：CloudWatch 指标和警报	添加了指向 示例：计算术语出现次数 的链接。	在 AMS 中创建自定义 CloudWatch 指标和警报
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	AMIs。 csv-and-notes.04.2023
2023 年 3 月		
更新内容：从 AMS 下线	澄清了在越过多账户 landing zone 账户时会删除哪些资源	退出 AMS 多账号 landing zone 账号
更新：AMS AMIs	在 “文档历史记录” 部分添加了每个月的 AMI ZIP 文件链接。	文档历史记录
更新：自动修复	移除了对 EC2 音量自动化的 LVM 支持。	AMS 自动修复警报
更新：补丁 RACI	对 RACI 进行了几次更新和澄清，以进行修补。	AMS 责任矩阵 (RACI)
更新内容：自助配置	添加了常见问题解答 bullet。要启动新的 AWS Datasync 代理，不需要 WIGS 提取。	AMS 中的自助服务配置模式
更新内容：自助配置	添加了常见问题解答 bullet。要启动新的 AWS Datasync 代理，不需要 WIGS 提取。	AMS 中的自助服务配置模式

更改	描述	链接
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	AMIs。 csv-and-notes.03.2023
2023年2月		
更新内容：从 AMS 下线	阐明了如何移除多账户 landing zone 环境和 VPCs应用程序账户	离线 AMS 账户
更新内容：寻找 ARNs	添加了用于查找 Dynamo describe-table DB 表 ARN 的 DynamoDB CLI	在 AMS 中查找亚马逊资源名称 (ARNs)
更新内容：自助配置	移除了 AMS CodeSuite “” 选项，因为它不是真正的 SSP。您仍然可以使用管理 AWS 服务 自行配置服务 添加 (需要审阅) (ct-3qe6io8t6jtny) 更改类型并请求三项服务：和。 CodeBuild CodeDeploy CodePipeline然后，AMS 将为您的账户配置以下 IAM 角色：customer_codebuild_service_role customer_codedeploy_service_role 、和aws_code_pipeline_service_role 。在您的账户中配置后，您必须在联合解决方案中加入该角色。	AMS 中的自助服务配置模式
更新内容：Secrets Manager 更新	更正了多账户着陆区 (MALZ) 与单账户着陆区 (SALZ) 所需的角色。	使用 Secrets Manager 共享密钥常见问题解答

更改	描述	链接
更新内容：AMS 自动修复警报	增加了对逻辑卷管理器 (LVM) 卷的支持。	EC2 音量使用补救自动化
更新内容：AMS Amazon 机器映像 (AMIs)	添加了“Offboarding AMS”部分，AMIs 其中包含要 AMIs 从您的账户中删除的示例代码。	AMS Amazon 机器映像 (AMIs)
更新内容：IAM 用户角色	更新了 IAM 政策：AMSBilling 政策。	AMS 中的 IAM 用户角色
新内容：不支持 OSes	添加了有关 AMS 为不支持的操作系统提供哪些服务的信息 (OSes)。	适用于 AMS 中不支持的操作系统的功能
更新内容：按需报告	某些按需报告在 AMS Advanced 中不可用，并且被错误地显示为可用。	应要求报告
更新内容：注销 AMS 账户	澄清了注销 MALZ 应用程序账户的说明。	离线 AMS 应用程序账户
更新内容：Secrets Manager	更正了使用 Secrets Manager 所需的 IAM 角色的名称。	AWS 托管服务中的 Secrets Manager 常见问题解答
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	AMIs。csv-and-notes.02.2023
2023年1月		
新内容：AWS Device Farm (AMS SSP)	添加了一项新的 SSP 服务：Dev AWS ice Farm。	使用 AMS SSP AWS Device Farm 在您的 AMS 账户中进行预配置
更新：支持的 Windows 版本	增加了对 Windows 服务器 2022 的支持。	AMS Amazon 机器映像 (AMIs)、支持的配置 和 带有 SNS 的 AMS AMI 通知

更改	描述	链接
更新：连续性管理	更新了默认 AMS 备份计划中的规则。	默认备份计划，多账户 landing zone
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	AMIs。 csv-and-notes.01.2023
2022年12月		
更新：使用堡垒	修复了错误的链接。	使用堡垒访问实例
更新：资源调度器	进行了多项改进，并添加了指向 AWS 实例调度器的链接以获取更多背景信息。	AWS Managed Services 资源调度器
更新：Windows AMIs 和支持的配置 (适用于新 Windows AMIs)	更新了从 EC2 启动 (Windows Server 2016 及更高版本) 到 EC2 发布 (Windows Server 2016 和 Windows Server 2019) 中添加的 AMS AMI 内容，并添加了 EC2 LaunchV2 (Windows Server 2022 及更高版本)。将基于 Windows 的从 AMIs 微软 Windows 服务器 (2012 年、2012 年 R2、2016 年和 2019 年) 更新为微软 Windows 服务器 (2012、2012 R2、2016、2016、2019 和 2022 年)。	AMS Amazon 机器映像 (AMIs) 和 <u>服务描述</u>
更新：“资源充足的调度器”部分	改进了部署和自定义 AMS 资源调度器的方法。	AWS Managed Services 资源调度器
更新：设置 AMS：私有和公有 DNS	更新了 DNS 架构图。	设置私有和公有 DNS

更改	描述	链接
更新：MALZ 网络架构	更新了图表并添加了加速应用程序账户指南。	MALZ 网络架构
更新：设置：使用标签	新增说明：只有 MALZ 应用程序账户支持自定义标记，核心账户不支持自定义标记。	AMS 基础设施自动标记
更新：访问管理：使用堡垒	更新了简介，加入了 RDP 堡垒。	节省购买单账户着陆区 (SALZ) 堡垒的成本
更新：AMS 默认设置：提醒	在警报表中添加了 EC2 实例：非根卷使用情况。	来自 AMS 基线监测的警报
更新：连续性管理	添加了有关持续备份的指导。	连续性管理的工作原理
更新：自动 EC2 实例配置	增加了对 PowerBroker 身份服务 (PBIS) 和实例代码 (OIC) 的支持。	在 Linux 实例上自动更新 PBIS 和 在 Linux 实例上自动更新代码
更新：Secrets Manager 的自助服务配置	更新了将 Secrets Manager 添加到你的账户的 CT (下方 FAQs)。	使用 AMS SSP AWS Secrets Manager 在您的 AMS 账户中进行配置
更新：日志管理	更新了 EC2 系统级日志列表。	亚马逊弹性计算云 (Amazon EC2)-系统级日志
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	AMIs。csv-and-notes.12.2022
2022年11月		
更新：AMS Amazon 机器映像 (AMIs)	更新了支持的 SUSE Linux 版本。	AMS Amazon 机器映像 (AMIs)
已更新：MALZ 账号	添加了删除客户管理的应用程序账户的指南。	客户托管应用程序账户

更改	描述	链接
更新：设置 AMS	增加了 customer-ams-amazon2-security-enhanced 。	带有 SNS 的 AMS AMI 通知
更新：监控的工作原理	更新了服务通知和事件报告的说明。	监控的工作原理
更新：MALZ 应用程序账户类型	改进了账户类型的解释。	应用程序账户类型
更新：开发者模式	添加了有关开发者模式的警告。	开始使用 AMS 开发者模式之前
更新：计划中的活动管理	添加了“PEM 的类型”部分	AWS Managed Services 中的计划活动管理
更新：Amazon 机器映像 (AMIs)	更新了支持的 SUSE Linux 版本	AMS Amazon 机器映像 (AMIs)
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	AMIs。csv-and-notes.11.2022
2022年10月		
新增：自动实例配置	新增部分描述了自动实例配置流程。	AMS Advanced 中的自动实例配置
新增：某些 SSP 只能使用手动 CT	更新了 50 多个自助服务配置服务 FAQs，使用手动 CT 而不是自动 CT 来添加 SSP。	AMS 中的自助服务配置模式
更新：设置 AMS	在 MALZ 的 EC2 Amazon IAM 实例配置文件中添加了两个策略。	EC2 IAM 实例配置文件

更改	描述	链接
新增：自定义侦探和预防规则库。	根据我们从多个客户那里获得的经验，添加了一组示例服务控制策略 (SCPs) 和预防性 Config 规则控制。	精选规则 SCPs 和 Config 规则
更新：AWS Backup 警告	添加了警告：“请勿编辑 AMS 备份计划，因为您的更改可能会丢失。取而代之的是，使用 ct-2hyozbpa0sx0m 为您的自定义配置创建新的备份计划。”	连续性管理的工作原理
更新：AWS Backup 小心	添加了有关向联合体添加新 IAM 角色的说明。	在 AMS 高级版中部署 IAM 资源
更新：监控管理	警报生成事件报告，而不是服务请求。	监控的工作原理
更新：自备 EPS	适用于 SALZ 和 MALZ。	AMS 自备 EPS
更新：加速应用程序账户	已澄清您的 Accelerate 账户是应用程序账户。	应用程序账户类型
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	AMIs。 csv-and-notes.10.2022
2022年9月		
更新：用于查找资源的 CLI 命令示例	添加了新的示例，可能需要该 --region 选项。	寻找你需要的数据 (SKMS) , AMS
更新：配置 IAM 角色	现在可以使用创建和管理 IAM 角色 AWSManagedServices CloudFormationAdminRole 。	使用“直接更改”模式创建堆栈

更改	描述	链接
更新：AMS 技术标准	AMS-STD-007 日志：(#20) 阐明了转发要求。	安全性和合规性
更新：连续性管理的工作原理	将 Start Backup Job 的措辞修改为“按需”而不是“现有”。	连续性管理的工作原理
更新：安全性与合规性	更新了标准 AMS-STD-007 第 20 号的描述和指南：在账户之间转发日志。	安全性和合规性
更新：变更管理用例	删除了指向旧版《变更管理用户指南》的断开链接。	变更管理用例
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	AMIs。 csv-and-notes.09.2022
2022 年 8 月 11 日		

更改	描述	链接
更新：为了保持一致性和可读性，章节标题已移至更合适的章节	“MALZ 网络架构”和“SALZ 网络架构”现在都是顶层“网络架构”部分（以前是“AMS 网络架构”部分）的子部分 “变更管理模式”是“变更管理”的新标题 “默认设置”现在是“设置 AMS”的一个小节 “AD FS 声明规则和 SAML 设置”（以前是“ActiveDirectory 联合身份验证服务 (ADFS) 声明规则和 SAML 设置”）现在是“设置 AMS”的一个小节 “访问管理”是“AMS 中的访问权限”的新标题，在目录中向上移动 “查找您需要的数据”是“服务知识管理”的新标题 “报告和选项”是“AMS 报告”的新标题，在目录中位于下方 “按需运营”现在是目录中的最后一个主题	什么是 AWS Managed Services ?
更新：查找和 ARN，新增：使用 ARN 查找资源	为了实用起见，这两个程序都完全重写。	在 AMS 中查找亚马逊资源名称 (ARNs) 和 在 AMS 中按照 ARN 查找资源
更新：将你的 CMA 与 Transit Gateway 连接起来	自动化不支持向核心路由域添加路由，也不支持需要更新的程序。	将 CMA 与 Transit Gateway 连接起来

更改	描述	链接
更新：MALZ 基本组件定价	所有价格均以美元为单位，并采用美元符号格式。	AMS 环境基本组件
更新：AMS AMI 注意事项	Zip 文件包括有关最新 AMS Amazon 机器映像 (AMIs) 的注释和最新的 CSV 文件 AMIs。	AMIs。 csv-and-notes.08.2022
2022年7月14日		
更新：自助报告	添加了使用 KMS 密钥加密 AWS Glue 元数据的说明。	自助报告
更新：AMS 基线监测	添加了 DeleteRecoveryPoint 备份警报。	来自 AMS 基线监测的警报
更新：支持的操作系统	增加了亚马逊 Linux 2 的终止支持日期。	支持的配置
更新：自助配置	添加了 AWS 转移 SSP 的先决条件。	使用 AMS SSP AWS Transfer Family 在您的 AMS 账户中进行配置
更新：AMS 报告	添加了有关选择加入区域的注释。	报告和选项
更新：RFC 信函和附件	阐明了允许的文本文件类型；特别是，YAML 文件必须以.yaml (不是.yml) 结尾。	添加 RFC 信件和附件 (控制台)
2022年6月21日		
更新了内容	以前称为“变更管理模式”或“标准 CM 模式”的 AMS 模式现在被称为“RFC 模式”。模式部分已扩展。	模式概述.
新警报	添加了 AWS Backup 警报。	来自 AMS 基线监测的警报

更改	描述	链接
2022年6月16日		
新增内容	事件管理。非安全风险的事件现在可以由 AMS 在事故报告中获得您的批准后解决，无需单独的 RFC 和批准。	事件管理
更新了内容	MALZ：更新了网络架构图。更新：应删除主账户 VPC 到共享服务 vpc 的 VPC 对等连接，因为它不存在。	网络账户架构
	Sagemaker 自助配置服务 (SSP)。已更新，在入职时添加了新的 IAM 角色以供 Sagemaker 使用。	使用 AMS SSP 在你的 AMS 账户中配置 SageMaker Amazon AI
	至 AMIs 支持的 SNS 通知列表：已添加 customer-ams-sles 12、customer-ams-sles 15、customer-ams-amazon 1 安全增强、customer-ams-rhel 8、8、8、2012、2019 和 customer-ams-windows 2019 年 customer-ams-rhel 安全增强。customer-ams-ubuntu customer-ams-windows customer-ams-windows 移除了 customer-ams-rhel 6 和 customer-ams-rhel 6 安全增强版 AMIs。	带有 SNS 的 AMS AMI 通知
	删除了升级电子邮件。	在 AWS Managed Services 中获取帮助

更改	描述	链接
	将主题列表移至开头段落下方。 更新了服务日志，提供了更好的负载均衡日志链接，还重新格式化了。	什么是 AWS Managed Services ? AMS 聚合服务日志
EKS 自助配置服务 (SSP)。添加了有关在集群中启用信封密钥加密的信息。	使用 AMS SSP 在你的 AMS 账户 AWS Fargate 中配置 Amazon EKS	
2022年6月9日		
更新了内容，正在获取帮助	删除了升级路径电子邮件。AMS通过事件报告提供沟通方式, 服务请求, 和 RFCs.	在 AWS Managed Services 中获取帮助
2022年5月12日		
新内容，按需运营 (OOD) 订阅模式	AMS 已将按需运营入职模式从当前的注册和续订模式更改为订阅分配和默认选择加入模式。当您注册 AMS 账户时，您会立即自动注册按需运营。	按需运营
2022年4月14日		
新内容，成本优化	AMS 提供成本优化建议。	AWS Managed Services 中的成本优化
更新了内容，在 MALZ 中加速账号	错误的角色名称 (Customer DefaultAdminRole) 已更新为正确的角色名称 (AccelerateDefaultAdminRole)。	AMS 加速账户 “访问您的加速账户”部分。

更改	描述	链接
更新了内容，AMS 访问了 IAM 角色	添加了用于访问您的账户的其他 AMS IAM 角色。	AMS 访问您的账户的原因和时间 “AMS 客户账户访问 IAM 角色”部分。
更新了内容、AMS 备份计划	添加了 AMS 管理的备份计划。	AMS 备份计划 和 AMS 备份保管库
更新了内容，S AWS secrets Manager	更新了常见问题解答。	使用 AMS SSP AWS Secrets Manager 在您的 AMS 账户中进行配置
更新了内容，直接更改模式 (DCM) 入门	AMS 不支持将 Service Catalog 客户加入 DCM。	直接更改模式入门
更新了内容、服务描述	澄清了“支持的服务”部分： • Fargate 上的亚马逊 EKS-> AWS Fargate 上的亚马逊 Elastic Kubernetes 服务 • 适用于 Fargate 的亚马逊 ECS-> Fargate 上的亚马逊弹性容器服务 AWS • 亚马逊 Kinesis-> 亚马逊 Kinesis Data Streams	支持的 AWS 服务
更新了内容，下线 MALZ 账号	已更新以引用离线应用程序帐户的新变更类型。	离线 AMS 应用程序账户
更新了内容，开发者模式事件管理	已将事件 SLA 描述更新为：AMS SLA 不适用于在 AMS 变更管理（包括开发者模式）之外创建或更新的资源。因此，在开发者模式下更新或创建的资源会自动降级为 P3，并且尽最大努力提供支持。	AMS 开发者模式下的事件管理

更改	描述	链接
更新了内容，DCM 上线	现在，新 DCM 的 RFC 模板包含您的 SAML 提供商 ARN 的字段。	直接更改模式入门
更新了内容，DCM 适用于 CloudFormation	创建和更新 CloudFormation 堆栈的说明现在包含 YAML 示例。	AMS 转型
更新了内容，MALZ Tools 账号	有一个用于迁移的新 IAM 角色：AWSManagedServicesMigrationRole。	AWS 应用程序迁移服务 (AWS MGN) 和 启用对新 AMS Tools 账户的访问权限
新内容，多账号 landing zone 账号	您可以在您的多账号着陆区 AMS 管理账户中创建 Accelerate 账户。	AMS 加速账户
更新了内容，安装了 API/CLI SDK	安装说明列出了错误的 Mac/Linux 安装文件名和错误的命令。此问题已修复。	使用 AMS API 和 CLI
更新了内容，在 MALZ 中加速账号	规则名称 (CustomerDefaultAdminRole) 不正确，它已更新为正确的名称 (AccelerateDefaultAdminRole)。	AMS 加速账户 ，“访问您的加速账户”部分
更新内容，监控	根使用率监控从 85% 修订为 95%。	来自 AMS 基线监测的警报
更新了内容、AMI 通知	您可以为新 AMS 创建多种类型的 SNS 通知 AMIs，我们添加了有关创建各种类型的信息。	带有 SNS 的 AMS AMI 通知
更新了内容，AMS 默认设置	删除了对 Macie Classic 的引用，取而代之的是梅西。	来自 AMS 基线监测的警报

更改	描述	链接
更新了内容，AMS 保留了前缀	按字母顺序排列保留前缀列表。	AMS 保留的前缀
更新了内容、服务描述	有关变更管理和自助服务配置的功能部分已更新，其中包含有关 AMS 模式的更多信息。	AWS Managed Services (AMS) AMS 高级运营计划功能
更新了内容，S AWS secrets Manager	使用 Secrets Manager 共享密钥。	2022 年 2 月 10 日
新内容、自助配置、Amazon Connect	添加了常见问题解答，介绍如何请求添加拨出或呼入电话的国家/地区列表。	2022 年 2 月 10 日
新内容、自助配置、Fargate 上的 Amazon EKS	添加了常见问题解答限制，即 AMS 不支持通过 AWS 云开发套件 (CDK) 或 CloudFormation Ingest 部署 EKS 集群。	2022 年 2 月 10 日
更改了内容，开发者模式	更正，您不使用 RFC 或服务请求将用户分配给您的联合解决方案，而是根据您的解决方案自行完成。	2022 年 2 月 10 日
内容已更改，直接更改模式 (DCM)	请注意，DCM 不支持 IAM。	2022 年 2 月 10 日
	DCM，请注意我们所做的验证。	2022 年 2 月 10 日
	DCM，明确不同角色的限制。	2022 年 2 月 10 日
内容已更改，监控基线警报	Redshift 集群资源警报已更改。	2022 年 2 月 10 日

更改	描述	链接
内容已更改，自助报告	添加了确切的 s3 存储桶名称 (<code>ams-reporting-data-a<Account_ID></code>)，供客户用来获取报告。	2022 年 2 月 10 日
更改了内容，更新了内容以引用自动变更类型而不是手动管理 其他 其他 (MOO)	更新了多账户 landing zone (MALZ) 应用程序账户内容以引用自动更改类型 (三，“将 TGW 附件与路由表关联”、“在 TGW 路由表中创建路由以连接到此 VPC”和“将 VPC 路由表配置为指向 AMS 多账户着陆区交通网关”)。 接收 AMS 生成的警报 基于标签的警报通知	2022 年 2 月 10 日
更改了内容：AMS AMIs。	添加了有关增强安全性的新信息 AMIs。请参阅 支持的配置AMS Amazon 机器映像 (AMIs) 、和 安全性得到增强 AMIs 。	2022 年 1 月 27 日
新内容：自助配置。	添加了适用于 OpenZFS 的 Amazon Fsx。请参阅 使用 AMS SSP 在你的 AMS 账户中 FSx 为亚马逊配置 OpenZFS 。	2022 年 1 月 27 日
更改内容：Code-Deploy 自助配置服务 (SSP)。	其他角色名称和其他限制说明。请参阅 使用 AMS SSP AWS CodeDeploy 在您的 AMS 账户中进行预配置 。	2022 年 1 月 27 日

更改	描述	链接
更改内容：更新了链接。	修复了断开的链接：AMS-AMIs、查找您的设置、查找堆栈 ID、查找 VPC ID ListVpcSummaries、ListStack Summaries、和 GetStack APIs。有关示例，请查看 在 AMS IDs 中查找堆栈 。	2022 年 1 月 13 日
更改了内容：EKS Support for Fargate	增加了以下限制 FAQs：不支持使用 EC2 EKS 创建或管理节点组。请参阅 使用 AMS SSP 在你的 AMS 账户 AWS Fargate 中配置 Amazon EKS 。	2022 年 1 月 13 日
更改内容：CloudFormation，直接更改模式 (DCM)	添加了使用 AmsStackTransform 创建或更新 CF 堆栈的说明。请参阅 使用“直接更改”模式创建堆栈 。	2022 年 1 月 13 日
更改内容：AWS 服务名称的统一性	AMS 参考文献要与官方标 AWS 题或元数据 AWS 服务 完全匹配。以前，有一些细微的变化会使模式匹配变得复杂。有关示例，请查看 使用 AMS SSP 在你的 AMS 账户中配置 Alexa for Business 。	2022 年 1 月 13 日
更改内容：弹性容器注册表 (ECR) 的自助配置	添加了使用 ECR 管理用户权限的常见问题解答项。请参阅 使用 AMS SSP 在您的 AMS 账户中配置 Amazon 弹性容器注册表 。	2022 年 1 月 13 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。