AWS Support

用户指南

API 版本 2013-04-15



AWS Support: 用户指南

Copyright © 2023 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 拥有的其它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

开始使用 AWS Support 1
创建支持案例和案例管理 1
创建支持案例 1
描述您的问题 3
选择严重性 3
示例：创建账户和账单支持工单 4
创建服务限额增加 9
更新、解决和重新打开您的案例 10
更新现有的支持案例 10
解析支持案例 11
重新打开已解决的案例 11
创建相关案例 12
案例历史记录 13
问题排查 13
我想为我的案例重新打开实时聊天 13
我无法连接到实时聊天 14
使用 AWS SDK 14
关于 AWS Support API 15
支持案例管理 15
AWS Trusted Advisor 15
端点 16
在 AWS 开发工具包中支持 16
AWS Support Plans 17
AWS Support 计划的功能 17
更改 AWS Support Plans 18
相关信息 18
AWS Trusted Advisor 19
开始使用 Trusted Advisor 建议 19
登录到 Trusted Advisor 控制台 20
查看检查类别 21
查看特定检查 22
筛选您的检查 23
刷新检查结果 24
下载检查结果 24
组织视图 24
Preferences（首选项） 24
使用 Trusted Advisor 即 Web 服务 25
获取可用 Trusted Advisor 检查的列表 26
刷新可用 Trusted Advisor 检查的列表 26
轮询 Trusted Advisor 检查以了解状态变化 27
请求 Trusted Advisor 检查结果 28
输出 Trusted Advisor 检查的详细信息 28
AWS Trusted Advisor 的组织视图 29
先决条件 29
启用组织视图 29
刷新 Trusted Advisor 检查 30
创建组织视图报告 30
查看报告摘要 33
下载组织视图报告 34
禁用组织视图 38
使用 IAM 策略允许访问组织视图 38
使用其他 AWS 服务查看 Trusted Advisor 报告 40
在 Trusted Advisor 中查看 Security Hub 控件 46
先决条件 47

查看 Security Hub 检查结果 47
刷新 Security Hub 检查结果 48
从 Trusted Advisor 禁用 Security Hub 49
问题排查 49
启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查 51
相关信息 52
AWS Trusted Advisor Priority 入门 52
先决条件 53
启用 Trusted Advisor Priority 53
查看优先建议 53
确认建议 54
忽略建议 55
解决建议 56
重新打开建议 56
下载建议详细信息 57
注册委派管理员 57
注销委派管理员 58
管理 Trusted Advisor Priority 通知 58
禁用 Trusted Advisor Priority 59
开始使用 EngAWS Trusted Advisor age (预览版) 59
先决条件 59
控制面板 60
查看互动类型目录 60
申请订婚 61
提交附件和备注 62
更改参与状态 63
区分推荐的项目和要求的项目 64
搜索参与度 64
Trusted Advisor 检查引用 65
成本优化 66
性能 83
安全性 93
容错能力 108
Service Limits 132
AWS Trusted Advisor 的更改日志 145
新的容错能力和性能检查 145
新的容错能力检查 146
新的容错能力检查 146
亚马逊 ECS 容错检查的区域扩展 146
新的容错能力检查 146
新的容错能力检查 146
更新了与 AWS Security Hub 集成的 Trusted Advisor 147
新的 AWS Resilience Hub 容错能力检查 147
对 Trusted Advisor 控制台的更新 147
Amazon EC2 的新检查 148
已将 Security Hub 检查添加到 Trusted Advisor 148
增加了来自 AWS Compute Optimizer 的检查 148
有关已泄露的访问密钥检查的更新 148
更新了对 AWS Direct Connect 的检查 149
AWS Trusted Advisor 控制台增加了 AWS Security Hub 控件 149
新的 Amazon EC2 和 AWS Well-Architected 检查 149
更新了 Ama OpenSearch y 的检查名称 150
增加了 Amazon Elastic Block Store 卷存储的检查 150
增加了 AWS Lambda 的检查 150
Trusted Advisor 检查删除 151
更新了 Amazon Elastic Block Store 的检查 151
Trusted Advisor 检查删除 151

Trusted Advisor 检查删除 152
Slack 中的 AWS Support App 153
先决条件 153
管理对 AWS Support App 小组件的访问 154
管理对 AWS Support App 的访问 155
授权 Slack 工作区 159
授权多个账户 160
配置 Slack 通道 160
更新 Slack 通道配置 164
在 Slack 中创建支持案例 165
在 Slack 中回复支持案例 170
加入与 AWS Support 的实时聊天会话 172
在 Slack 中搜索支持案例 176
使用您的搜索结果 177
在 Slack 中解决支持案例 179
在 Slack 中重新打开支持案例 180
请求增加服务限额 181
从 AWS Support App 中删除 Slack 通道配置 182
从 AWS Support App 中删除 Slack 工作区配置 183
Slack 中的 AWS Support App 命令 184
Slack 通道命令 184
实时聊天通道命令 184
在 AWS Support Center Console 中查看 AWS Support App 通信信息 185
在 Slack 中为 AWS Support App 创建 AWS CloudFormation 资源 185
AWS Support App 和 AWS CloudFormation 模板 185
为您的组织创建 Slack 配置资源 186
了解有关 CloudFormation 的更多信息 189
使用 Terraform 创建 AWS Support App 资源 189
安全性 190
数据保护 190
支持案例的安全性 191
身份和访问管理 191
受众 192
使用身份进行身份验证 192
使用策略管理访问 193
AWS Support 如何与 IAM 协同工作 194
基于身份的策略示例 196
使用服务相关角色 197
AWS 托管策略 201
管理对 AWS Support 中心的访问 221
管理对 AWS Support 计划的访问权限 224
管理对 AWS Trusted Advisor 的访问 226
问题排查 234
事件响应 235
AWS Support 和 AWS Trusted Advisor 中的日志记录和监控 235
合规性验证 236
故障恢复能力 236
基础设施安全性 236
配置和漏洞分析 237
代码示例 238
操作 243
向案例添加通信 243
向集合添加附件 247
创建案例 250
描述附件 254
描述案例 257
描述通信 261

描述服务 265
描述严重性级别 268
解析案例 271
场景 274
开始使用案例 274
AWS Support 的监控和日志记录 311
使用 EventBridge 监控 AWS Support 案例 311
为 AWS Support 案例创建一个 EventBridge 规则 311
示例 AWS Support 事件 312
另请参阅 314
使用 AWS Support 记录 AWS CloudTrail API 调用 314
AWS Support中的信息 CloudTrail 314
CloudTrail 日志记录中的 AWS Trusted Advisor 信息 315
了解 AWS Support 日志文件条目 315
使用记录AWS Support App API 调用 CloudTrail 316
AWS Support中的应用程序信息 CloudTrail 317
了解 AWS Support App 日志文件条目 317
Support Plans 的监控和日志记录 320
使用 AWS CloudTrail 记录 AWS Support Plans API 调用 320
AWS Support中的计划信息CloudTrail 320
了解 AWS Support Plans 日志文件条目 321
记录更改 AWS Support 计划的控制台操作 324
Trusted Advisor 的监控和日志记录 327
使用 EventBridge 监控 Trusted Advisor 检查结果 327
创建 CloudWatch 警报以监控Trusted Advisor指标 329
先决条件 329
CloudWatch 的指标Trusted Advisor 331
Trusted Advisor 指标和维度 336
使用 AWS CloudTrail 记录 AWS Trusted Advisor 控制台操作 337
Trusted Advisor中的信息 CloudTrail 337
示例：Trusted Advisor 日志文件条目 339
资源问题排查 342
特定于服务的问题排查 342
文档历史记录 345
早期更新 352
AWS 词汇表 355
..... cccIvi

AWS Support 入门

AWS Support 包含一系列计划，这些计划旨在让您能够运用各种工具和专业知识来为成功部署和正常实施 AWS 解决方案提供支持。所有支持计划均提供全天候客户服务、AWS 文档服务、技术论文服务和支持论坛服务。要获取可规划、部署和改善您的 AWS 环境的技术支持服务和更多资源，您可以选择一项适合您的 AWS 使用案例的支持计划。

注意

- 要在 AWS Management Console 中创建支持案例，请参阅 创建支持案例 (p. 1)。
- 有关不同 AWS Support 计划的更多信息，请参阅比较 AWS Support 计划和 更改 AWS Support Plans (p. 18)。
- 支持计划可为您的支持案例提供不同的响应时间。请参阅 选择严重性 (p. 3) 和 响应时间 (p. 4)。

主题

- 创建支持案例和案例管理 (p. 1)
- 创建增加服务限额 (p. 9)
- 更新、解决和重新打开您的案例 (p. 10)
- 问题排查 (p. 13)
- 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)

创建支持案例和案例管理

在 AWS Management Console 中，您可以在 AWS Support 中创建三种类型的客户案例：

- 所有 AWS 客户都可打开账户和账单支持案例。您可以获得账单和账户问题的帮助。
- 提高服务限制请求可供所有 AWS 客户使用。有关默认服务限额（以前称为限制）的信息，请参阅 AWS 一般参考 中的 AWS 服务限额。
- 技术支持案例可为您联系技术支持人员，帮助您解决服务相关的技术问题，有时还有第三方应用程序问题。如果您拥有“基本”支持计划，则无法创建技术支持案例。

  注意

  - 要更改您的支持计划，请参阅 更改 AWS Support Plans (p. 18)。
  - 要关闭账户，请参阅 AWS Billing 用户指南中的关闭账户。
  - 要查找 AWS 服务的常见故障排除主题，请参阅资源问题排查 (p. 342)。
  - 如果您是 AWS Partner Network 中的 AWS Partner 的客户，并且使用分销商支持，请直接与您的 AWS Partner 联系以解决任何与账单相关的问题。AWS Support 无法帮助您解决分销商支持的非技术问题，例如账单和账户管理。有关更多信息，请参阅以下主题：
    - AWS 的合作伙伴如何确定组织中的 AWS Support 计划
    - 由 AWS Partner 主导的支持

创建支持案例

您可以在 AWS Management Console 的支持中心创建支持案例。

注意

- 您可以以 AWS 账户的根用户身份或 AWS Identity and Access Management (IAM) 用户身份登录支持中心。有关更多信息，请参阅管理对 AWS Support 中心的访问 (p. 221)：

- 如果无法登录到支持中心和创建支持案例，则可以使用 Contact Us（联系我们）页面。您可以使用此页面获取有关账单和账户问题的帮助。

创建支持案例

1. 登录到 AWS Support Center Console。

   Tip

   在 AWS Management Console中，您还可以选择问号图标（），然后选择 Support Center（Support 中心）。
2. 选择 Create case（创建案例）。
3. 请选择以下任一选项：

   - Account and billing（账户和账单）
   - Technical（技术）
   - 要提高服务限额，请选择 Looking for service limit increases?（想提高服务限制？），然后按照创建增加服务限额 (p. 9)的说明操作。
4. 选择 Service（服务）、Category（类别）和 Severity（严重性）。

   Tip

   您可以使用针对常见问题提供的建议解决方案。
5. 选择 Next step: Additional information（下一步：其他信息）
6. 在 Additional information（其他信息）页面上，对于 Subject（主题），请为您的问题输入一个标题。
7. 对于 Description（描述），请按照提示操作以描述您的情况，例如：

   - 您收到的错误消息
   - 您遵循的故障排除步骤
   - 您如何访问服务：
     - AWS Management Console
     - AWS Command Line Interface (AWS CLI)
     - API 操作
8. （可选）选择 Attach files（附加文件）以为您的工单添加任何相关文件，例如错误日志或屏幕截图。您最多可以附加三个文件。每个文件最大可为 5 MB。
9. 选择 Next step: Solve now or contact us（下一步：立即解决或联系我们）。
10. 在 Contact us（联系我们）页面上，选择您的首选语言。
11. 选择您的首选联系方式。您可以选择以下选项之一：

    a. Web – 通过 Support 中心接收回复。
    b. Chat（聊天）– 开始与支持座席在线聊天。如果您无法连接到聊天，请参阅 问题排查 (p. 13)。
    c. 电话 – 接收来自客服的电话。如果选择此选项，请输入以下信息：

       - Country or region（国家或地区）
       - Phone number（电话号码）
       - (Optional) Extension [（可选）分机]

       注意

       - 显示的联系选项取决于工单类型和您拥有的支持计划。
       - 您可以选择 Discard draft（丢弃草稿）以清除您的支持工单草稿。

12. （可选）如果您拥有 Business、Enterprise On-Ramp 或 Enterprise Support 计划，则会显示 Additional contacts（其他联系人）选项。您可以输入相关人员的电子邮件地址，以在工单状态发生更改时接收通知。如果您以 IAM 用户身份登录，请包含您的电子邮件地址。如果您使用自己的根账户电子邮件地址和密码登录，则无需填写您的电子邮件地址

    Note

    如果您拥有 Basic Support 计划，则不能使用 Additional contacts（其他联系人）选项。但是，My Account（我的账户）页面的 Alternate Contacts（备用联系人）部分中指定的 Operations（操作）联系人接收案例通信的副本，但仅针对账户和账单以及技术的特定案例类型。

13. 检查工单详细信息，然后选择 Submit（提交）。此时将显示您的案例 ID 号和摘要。

描述您的问题

使您的描述尽可能的详细。包含相关的资源信息，以及可能有助于我们了解您问题的任何其他信息。例如，要排查性能问题，可提供时间戳和日志。对于功能请求或一般指导问题，请提供对您的环境和目的的描述。在所有案例中，都请遵从案例提交表单中的 Description Guidance (描述指导)。

您提供尽可能多的详细信息意味着提升了快速解决案例的可能性。

选择严重性

您可能倾向于始终以您的支持计划允许的最高严重性创建支持案例。但是，我们建议您为无法解决或直接影响生产应用程序的案例选择最高严重性。有关构建服务以避免单个资源的缺失影响到应用程序的信息，请参阅在 AWS 上构建容错的应用程序技术论文。

下表列出了严重性级别、响应时间和问题示例。

注意

- 创建支持案例后，您无法更改支持案例的严重性代码。如果您的情况发生变化，请联系 AWS Support 坐席以处理您的支持案例。
- 有关严重性级别的更多信息，请参阅 AWS Support API 参考。

严重性	严重性级别代码	第一响应时间	说明和支持计划
一般指南	`low`	24 小时	您遇到一般开发问题或想要申请一个功能。（*开发人员、商业、Enterprise On-Ramp 或企业支持计划）
系统受损	`normal`	12 小时	您的应用程序的非关键功能工作异常，或者您存在有时效要求的开发问题。（*开发人员、商业、Enterprise On-Ramp 或企业支持计划）
生产系统受损	`high`	4 小时	您的应用程序的重要功能受到影响或被迫降级。（商业、Enterprise On-Ramp 或企业 Support 计划）
生产系统停机	`urgent`	1 小时	您的业务受到重大影响。您的应用程序的重要功能不可用。（商业、Enterprise On-Ramp 或企业 Support 计划）

严重性	严重性级别代码	第一响应时间	说明和支持计划
业务关键系统停机	`critical`	15 分钟	您的业务面临危险。应用程序的关键功能不可用（企业 Support 计划）。请注意，Enterprise On-Ramp Support 计划的响应时效为 30 分钟。

响应时间

我们会在指示的时间内对您的初次请求尽一切合理努力做出回应。有关每种 AWS Support 计划的支持范围的信息，请参阅 AWS Support 功能。

如果您有商业、Enterprise On-Ramp 或企业支持计划，您可以全天候获得技术支持。*对于开发人员支持，支持案例的响应目标按工作时间计算。工作时间通常是指客户所在国家/地区的上午 8:00 至下午 6:00，节假日和周末除外。对于跨多个时区的国家/地区，工作时间可能不尽相同。客户所在国家/地区信息将显示在 AWS Management Console 中的 My Account（我的账户）页面的 Contact Information（联系人信息）部分。

Note

如果您选择日语作为支持案例的首选联系语言，则可以在以下时间内获得日语支持，如下所示：

- 如果您需要针对非技术支持 案例的客户服务，或者如果您有开发者支持计划并需要技术支持，则可以在 日本的工作时间内的日语支持，工作时间定义为日本标准时间 (GMT+9) 上午 09:00 至下午 06:00，节假日和周末除外。
- 如果您有商业、Enterprise On-Ramp 或企业支持计划，可以全天候获得日语技术支持。

如果您选择中文作为支持案例的首选联系语言，则可以在以下时间内获得中文支持：

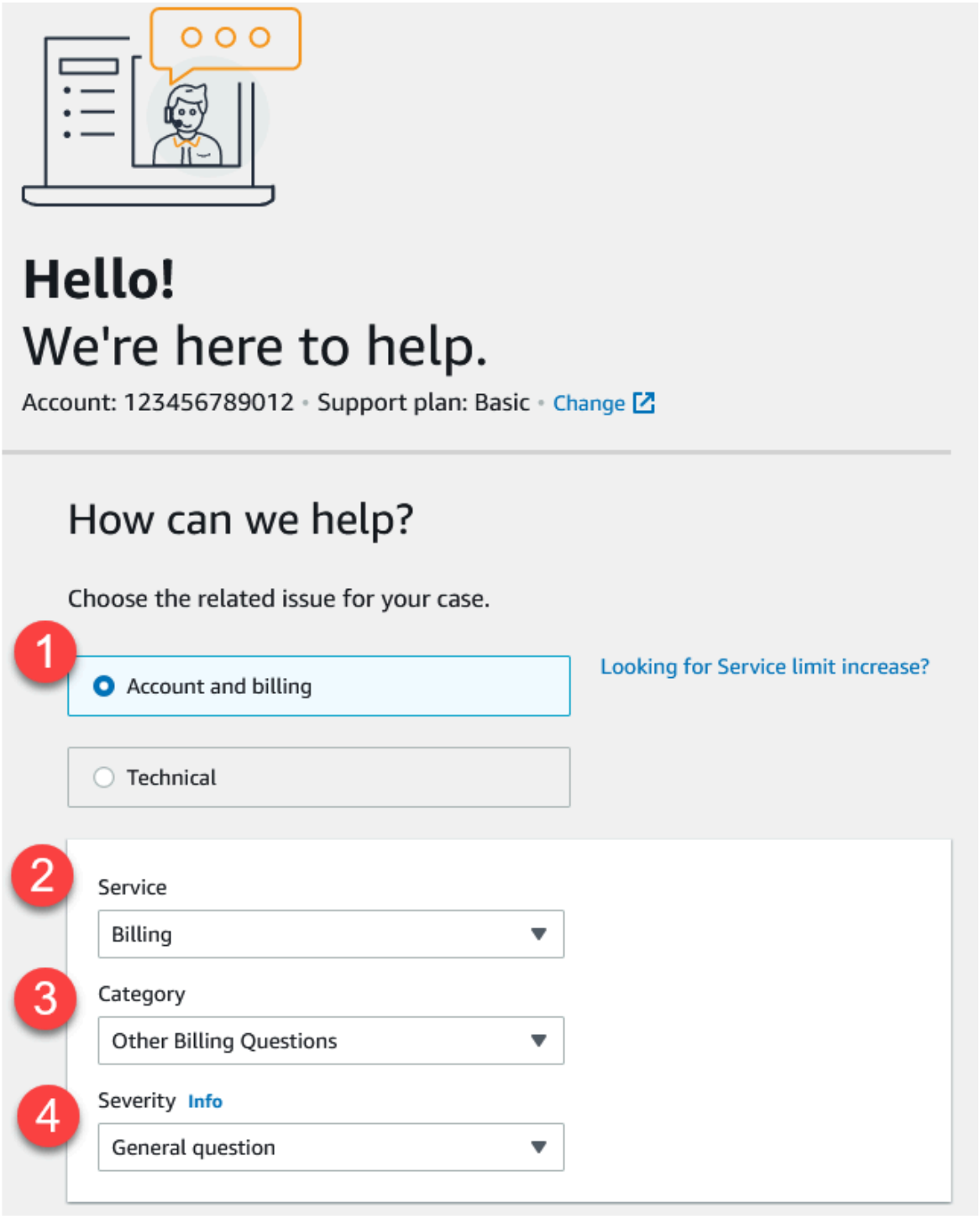
- 如果您需要中文客服协助您处理非技术方面的问题，方可在上午 9:00 至下午 6:00 (GMT+8) 之间的时间段联系客服，不含周末和节假日。
- 如果您有开发者支持 计划，则可以在 “我的账户” 中规定的工作时间（通常定义为您所在国家/地区的上午 8:00 至下午 6:00）的中文技术支持，节假日和周末除外。这些时间可能因具有多个时区的国家/地区而异。
- 如果您有商业、Enterprise On-Ramp 或企业 支持 计划，可以全天候获得中文技术支持。

如果您选择韩语作为支持案例的首选联系语言，则可以在以下时间内获得韩语支持，如下所示：

- 如果您需要针对非技术支持案例的客户服务，则可以在韩国的工作时间（定义为韩国标准时间 (GMT+9) 上午 09:00 至下午 06:00），不包括节假日和周末，提供韩语支持。
- 如果您有开发者支持 计划，则可以在 “我的账户” 中规定的工作时间（通常定义为您所在国家/地区的上午 8:00 至下午 6:00）提供韩语技术支持，节假日和周末除外。这些时间可能因具有多个时区的国家/地区而异。
- 如果您拥有商业、Enterprise On-Ramp 或企业 支持 计划，可以全天候获得韩语技术支持。

示例：创建账户和账单支持工单

以下示例是一个有关账户和账户问题的支持工单。



1. Create case（创建工单）– 选择要创建的工单的类型。在此例中，工单类型为 Account and billing（账户和账单）。

   Note

   如果您拥有“基本”支持计划，则无法创建技术支持案例。

2. 服务 – 如果您的问题涉及到多个服务，请选择最适用的服务。

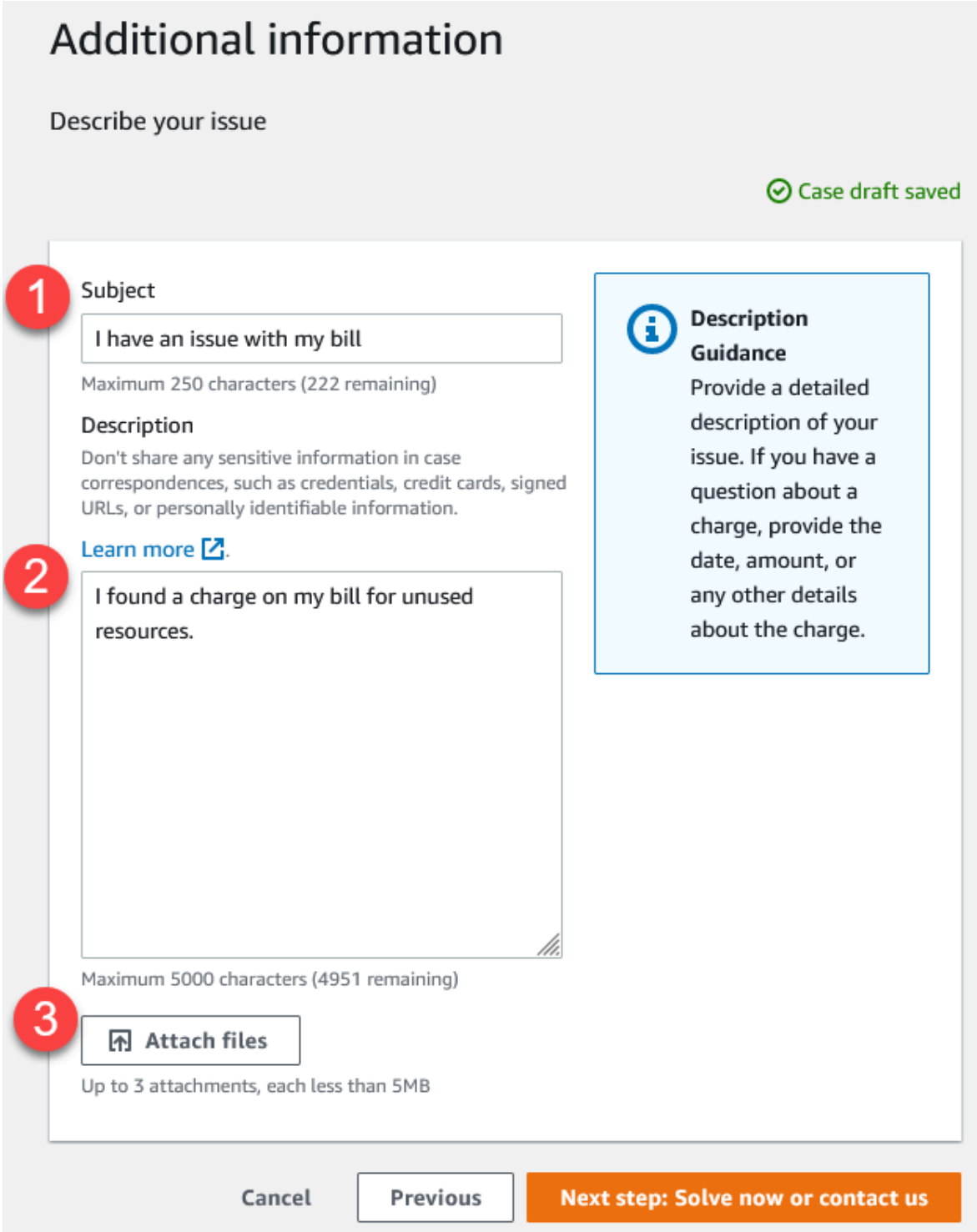
3. 类别 – 请选择最符合您的使用案例的类别。当您选择某个类别时，将会在下方显示可解决问题的信息链接。
4. 严重性 – 已加入付费支持计划的客户可以选择 General guidance（一般指导）（响应时间为 1 天）或 System impaired（系统受影响）（响应时间为 12 小时）这两种严重性级别。已加入业务支持计划的客户还可以选择 Production system impaired（生产系统受损）（响应时间为 4 小时）或 Production system down（生产系统停机）（响应时间为 1 小时）。拥有商业、Enterprise On-Ramp 或企业 Support 计划的客户可以选择 Business-critical system down（业务关键系统停机）（企业 Support 计划的响应时效为 15 分钟，Enterprise On-Ramp 计划的响应时效为 30 分钟）。

   响应时间是指 AWS Support 首次响应的时间。这些响应时间不适用于后续响应。对于第三方问题，响应时间可能较长，具体取决于技术娴熟的人员是否有时间进行处理。有关更多信息，请参阅选择严重性 (p. 3)：

   Note

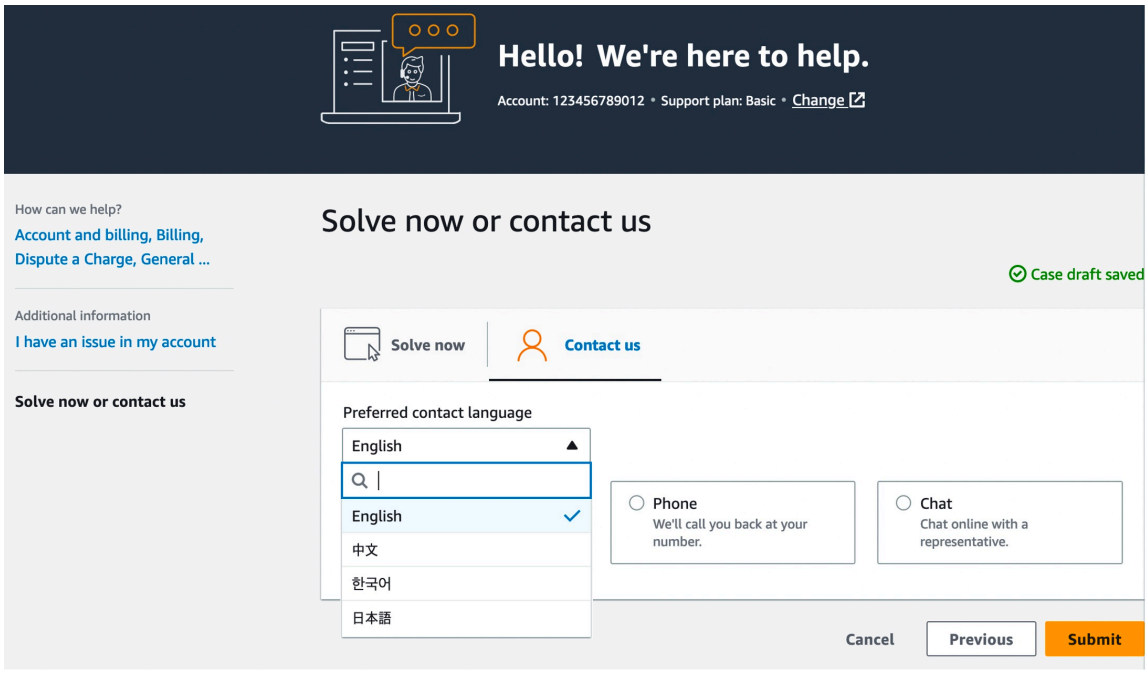
   根据您所选择的类别，系统可能会提示您提供更多信息。

在指定案例类型和分类后，可以指定描述以及希望与您联系的方式。



1. 主题 – 输入用于简要描述问题的标题。
2. Description（描述）– 描述您的支持案例。这是您向 AWS Support 提供的最重要的信息。对于某些服务和类别组合，会有提示指出相关信息。请使用这些链接来帮助解决您的问题。有关更多信息，请参阅描述您的问题 (p. 3)：
3. Attachments（附件）– 附上屏幕截图和其他文件，以帮助支持座席更快地解决您的问题。

在添加工单详细信息后，您可以选择您希望使用的联系方式。



1. 首选联系语言-选择您的首选语言。目前，您可以选择中文、英语、日语或韩语。您的支持计划将显示您首选语言的自定义联系选项。
2. 选择一种联系方式。显示的联系选项取决于工单类型和您拥有的支持计划。
   - 如果您选择 Web，则可以通过支持中心了解案例进展并做出响应。
   - 选择 Chat（聊天）或 Phone（电话）。如果您选择 Phone (电话)，则系统将提示您输入回电号码。
3. 当您的信息填写完毕并且准备好创建案例时，选择 Submit (提交)。

Note

如果您选择日语作为支持案例的首选联系语言，则可以获得日语支持，如下所示：

- 如果您需要针对非技术Support 案例提供客户服务，或者如果您有开发者支持计划并需要技术支持，则在日本的工作时间内（定义为日本标准时间 (GMT+9) 上午 09:00 至下午 06:00，不包括节假日和周末，提供日语支持。
- 如果您有商业、Enterprise On-Ramp 或企业支持计划，可以全天候获得日语技术支持。

如果您选择中文作为支持案例的首选联系语言，则可以获得以下中文支持：

- 如果您需要非技术支持案例的客户服务，则可以在上午 09:00 至下午 06:00 获得中文支持（GMT +8），节假日和周末除外。
- 如果您有开发者Support 计划，则在工作时间内提供中文技术支持，通常定义为您所在国家/地区的上午 8:00 至下午 6:00（节假日和周末除外）。在具有多个时区的国家/地区，这些时间可能会有所不同。
- 如果您有商业、Enterprise On-Ramp 或企业Support 计划，可以全天候获得中文技术支持。

如果您选择韩语作为支持案例的首选联系语言，则可以获得韩语支持，如下所示：

- 如果您需要针对非技术支持案例提供客户服务，则在韩国工作时间内（定义为韩国标准时间 (GMT+9) 上午 09:00 至下午 06:00，不包括节假日和周末，提供韩语支持。
- 如果您有开发者Support 计划，则在工作时间内提供韩语技术支持，工作时间通常定义为您所在国家/地区的上午 8:00 至下午 6:00（节假日和周末除外）。在具有多个时区的国家/地区，这些时间可能会有所不同。
- 如果您有商业、Enterprise On-Ramp 或企业Support 计划，可以全天候获得韩语技术支持。

创建增加服务限额

请求增加服务限额（以前称为限制）以提高服务性能。

Note

您还可以通过服务限额服务直接请求为您的服务增加限额。目前，服务限额不支持所有服务的服务限额。有关更多信息，请参阅《服务限额用户指南》中的什么是服务限额？

创建支持工单以请求增加服务限额

1. 登录到 AWS Support Center Console。

   Tip

   在 AWS Management Console中，您还可以选择问号图标（），然后选择 Support Center（Support 中心）。
2. 选择 Create case（创建案例）。
3. 选择 Looking for service limit increases?（想要提高服务限制？）
4. 要请求提高限额，请按照提示进行操作。可能的选项如下：

   - Limit type（限制类型）
   - 严重性

     Note

     根据您所选择的类别，系统可能会提示您提供更多信息。
5. 对于 Requests（请求），选择 Region（区域）。
6. 对于 Limit（限制），选择该服务限制类型。
7. 对于 New limit value（新限制值），输入所需要的值。
8. （可选）要请求提高其他限额，请选择 Add another request（添加其他请求）。
9. 对于 Case description（工单描述），请描述您的支持工单。
10. 对于 Contact options（联系选项）页面，选择您的首选语言以及希望使用的联系方式。您可以选择以下选项之一：

    - Web – 通过 Support 中心接收回复。
    - Chat（聊天）– 开始与支持座席在线聊天。如果您无法连接到聊天，请参阅 问题排查 (p. 13)。
    - 电话 – 接收来自客服的电话。如果选择此选项，请输入以下信息：
      - Country/Region（国家/地区）
      - Phone number（电话号码）
      - (Optional) Extension [（可选）分机]
11. 选择 Submit（提交）。此时将显示您的案例 ID 号和摘要。

更新、解决和重新打开您的案例

创建支持案例后，您可以在支持中心监控案例的状态。新案例一开始处于 Unassigned（未分配）状态。当客服开始处理一个案例时，状态更改为 Work in Progress（正在处理中）。客服可能会对您的案例作出响应，要求您提供更多信息（Pending Customer Action (等待客户操作)），或者告知您该案例正处于调查中（Pending Amazon Action (等待 Amazon 操作)）。

当您的案例更新后，您会收到电子邮件，其中包含通信信息和指向支持中心中的案例的链接。使用电子邮件消息中的链接导航到支持案例。您无法通过电子邮件来回复案例通信信息。

注意

- 您必须登录提交支持案例的 AWS 账户。如果您以 AWS Identity and Access Management (IAM) 用户身份登录，则必须具有查看支持案例所需的权限。有关更多信息，请参阅管理对 AWS Support 中心的访问 (p. 221)：
- 如果您在几天内未对案例作出回应，AWS Support 会自动解决案例。
- 处于已解决状态超过 14 天的支持案例无法重新打开。如果您遇到与已解决案例相关的类似问题，您可以创建相关案例。有关更多信息，请参阅创建相关案例 (p. 12)：

主题

- 更新现有的支持案例 (p. 10)
- 解决支持案例 (p. 11)
- 重新打开已解决的案例 (p. 11)
- 创建相关案例 (p. 12)
- 案例历史记录 (p. 13)

更新现有的支持案例

您可以更新案例，为支持代理提供更多信息。例如，您可以回复信件、开始另一个实时聊天、添加其他电子邮件收件人等。但是，在创建案例后，您无法更新案例的严重性。有关更多信息，请参阅选择严重性 (p. 3)：

更新现有的支持案例

1. 登录到 AWS Support Center Console。

   Tip

   在 AWS Management Console中，您还可以选择问号图标（），然后选择 Support Center（Support 中心）。
2. 在 Open support cases（打开支持案例）下，选择支持案例的 Subject（主题）。
3. 选择 Reply（回复）。在 Correspondence（通信）部分中，您还可以进行以下任何更改：
   - 提供支持客服请求的信息
   - 上传文件附件
   - 更改您的首选联系方式
   - 添加电子邮件地址以接收案例更新
4. 选择 Submit（提交）。

Tip

如果您已关闭聊天窗口并且希望开始另一个实时聊天，则可以为您的支持案例添加 Reply（回复），然后选择 Chat（聊天），最后选择 Submit（提交）。此时会打开一个新的弹出式聊天窗口。

解决支持案例

当您对支持响应感到满意，或您的问题得到解决时，您可以在支持中心解决案例。

要解决支持案例

1. 登录到 AWS Support Center Console。

   Tip

   在 AWS Management Console中，您也可以选择问号图标（），然后选择 Support Center（Support 中心）。
2. 在 Open support cases（打开支持案例）下，选择您要解决的支持案例的 Subject（主题）。
3. （可选）选择 Reply（回复），并在 Correspondence（通信）部分中，输入解决案例的原因，然后选择 Submit（提交）。例如，如果您需要此信息以供将来参考，您可以输入有关您如何自己解决问题的信息。
4. 选择 Resolve case（解决案例）。
5. 在此对话框中，选择 Ok（确定）以解决案例。

   Note

   如果 AWS Support 为您解决了案例，您可以使用反馈链接提供更多关于您使用 AWS Support 的经验的信息。

Example ：反馈链接

以下屏幕截图显示了支持中心案例通信中的反馈链接。

Please let us know if we helped resolve your issue:

If YES, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-Yes

If NO, click here:
https://console.aws.amazon.com/support/feedback?eventId=1234567890&language=en&questionnaireId=Support-HMD-No

重新打开已解决的案例

如果您再次遇到同一问题，您可以重新打开原始案例。提供有关再次出现问题的详细信息以及您尝试的问题排除步骤。包括任何相关的案例编号，以便客服可以参考以前的通信。

注意

- 从问题得到解决后的 14 天内，您可以重新打开支持案例。但是，您不能重新打开已处于非活动状态超过 14 天的案例。您可以创建新案例或相关案例。有关更多信息，请参阅创建相关案例 (p. 12)：
- 如果您重新打开具有与当前问题不同的信息的现有案例，则客服可能会要求您创建新案例。

要重新打开已解决的案例

1. 登录到 AWS Support Center Console。

   Tip

   在 AWS Management Console中，您也可以选择问号图标（ ），然后选择 Support Center（Support 中心）。
2. 选择 View all cases（查看所有案例），然后选择您想要重新打开的支持案例的 Subject（主题）或 Case ID（案例 ID）。
3. 选择 Reopen case（重新打开案例）。
4. 在 Correspondence（通信）下，对于 Reply（回复），输入案例详细信息。
5. （可选）选择 Choose files（选择文件）以将文件附加到您的案例。您最多可以附加 3 个文件。
6. 对于 Contact methods（联系方式），选择以下选项之一：
   - Web – 通过电子邮件和支持中心获取通知。
   - 聊天 – 与客服在线聊天。
   - 电话 – 接收来自客服的电话。
7. （可选）对于其他联系人，输入您希望接收案例通信的其他人员的电子邮件地址。
8. 查看案例详细信息并选择 Submit（提交）。

创建相关案例

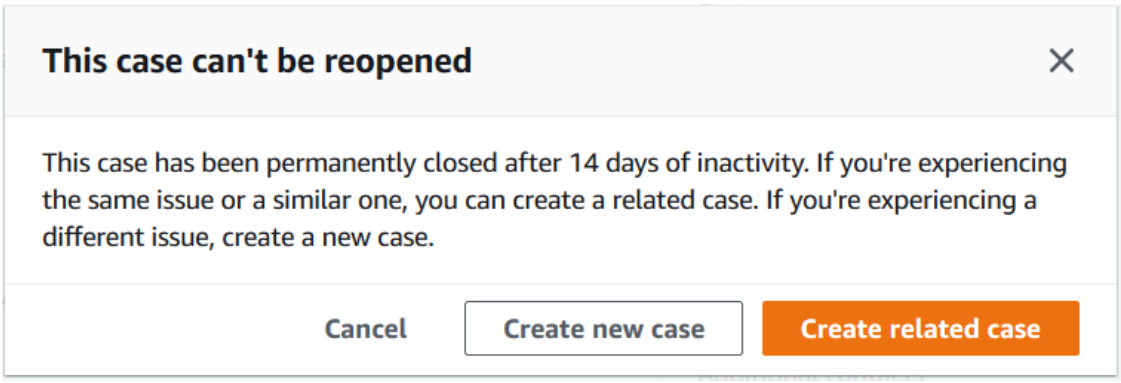
14 天处于不活动状态后，您将无法重新打开已解决的案例。如果您遇到与已解决案例相关的类似问题，您可以创建相关案例。此相关案例将包括指向先前解决的案例的链接，以便客服可以查看之前的案例详细信息和通信。如果您遇到的问题不同，我们建议您创建新案例。

要创建相关案例

1. 登录到 AWS Support Center Console。

   Tip

   在 AWS Management Console中，您也可以选择问号图标（ ），然后选择 Support Center（Support 中心）。
2. 选择 View all cases（查看所有案例），然后选择您想要重新打开的支持案例的 Subject（主题）或 Case ID（案例 ID）。
3. 选择 Reopen case（重新打开案例）。
4. 在此对话框中，选择 Create related case（创建相关案例）。之前的案例信息将自动添加到您的相关问题中。如果您有其他问题，请选择 Create new case（创建新案例）。



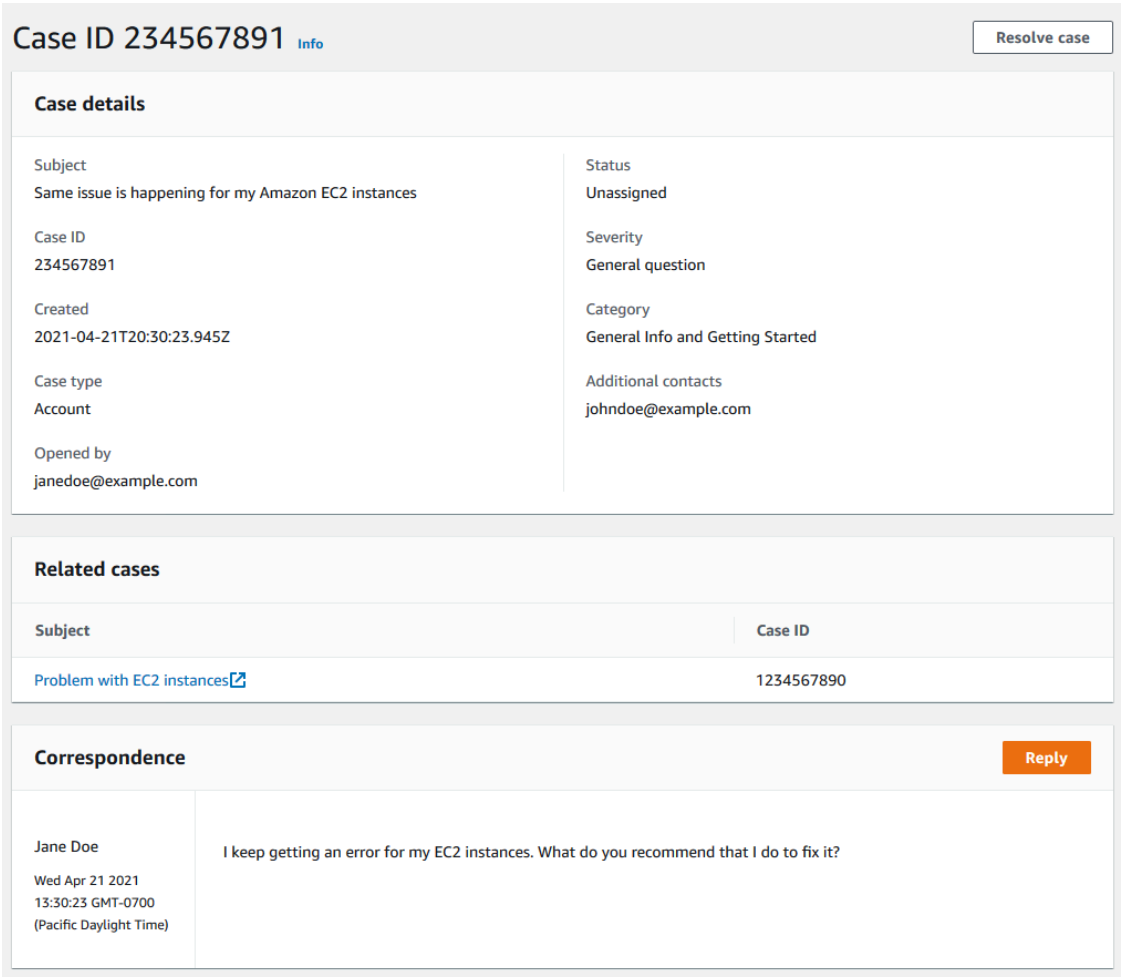
5. 按照同样的步骤创建您的案例。请参阅 创建支持案例 (p. 1)。

   Note

   默认情况下，您的相关案例具有与之前的案例相同的 Type（类型）、Category（类别）和 Severity（严重性）。您可以根据需要更新案例详细信息。

6. 查看案例详细信息并选择 Submit（提交）。

创建案例后，上一个案例将显示在 Related cases（相关案例）部分，例如以下示例中所示。



案例历史记录

您最多可以在创建案例后 24 个月内查看案例历史记录信息。

问题排查

如果您在创建或管理支持案例时遇到问题，请参阅以下问题排查信息。

我想为我的案例重新打开实时聊天

您可以回复现有的支持案例以打开另一个聊天窗口。有关更多信息，请参阅更新现有的支持案例 (p. 10)：

我无法连接到实时聊天

如果您选择了 Chat（聊天）选项，但无法连接到聊天窗口，请先执行以下检查：

- 确保已将浏览器配置为允许支持中心中的弹出窗口。

  Note

  审核浏览器的设置。有关更多信息，请参阅 Chrome 帮助和 Firefox 支持网站。
- 确保您已配置网络，以便可以使用 AWS Support：
  - 您的网络可以访问 `*.connect.us-east-1.amazonaws.com` 端点。

    Note

    对于 AWS GovCloud (US)，端点为 `*.connect-fips.us-east-1.amazonaws.com`。
  - 您的防火墙支持 Web 套接字连接。

如果您仍然无法连接到聊天窗口，请AWS Support使用电子邮件或电话联系方式进行联系。

将 AWS Support 与 AWS 开发工具包配合使用

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

软件开发工具包文档	代码示例
AWS SDK for C++	AWS SDK for C++ 代码示例
AWS SDK for Go	AWS SDK for Go 代码示例
AWS SDK for Java	AWS SDK for Java 代码示例
AWS SDK for JavaScript	AWS SDK for JavaScript 代码示例
AWS SDK for Kotlin	AWS SDK for Kotlin 代码示例
AWS SDK for .NET	AWS SDK for .NET 代码示例
AWS SDK for PHP	AWS SDK for PHP 代码示例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 代码示例
AWS SDK for Ruby	AWS SDK for Ruby 代码示例
AWS SDK for Rust	AWS SDK for Rust 代码示例
AWS SDK for Swift	AWS SDK for Swift 代码示例

可用性示例

找不到所需的内容？ 通过使用此页面底部的 Provide feedback（提供反馈）链接请求代码示例。

关于 AWS Support API

AWS Support API 提供对 AWS 支持中心一些功能的访问。

API 提供两组不同的操作：

- 支持案例管理 (p. 15) 操作用于管理 AWS 支持案例从创建到解决的整个生命周期
- 要访问 AWS Trusted Advisor (p. 19) 检查的 AWS Trusted Advisor (p. 15) 操作

> **Note**
>
> 您必须拥有商业、Enterprise On-Ramp 或企业 Support 计划才能使用 AWS Support API。有关更多信息，请参阅AWS Support：

有关 AWS Support 提供的操作和数据类型的详细信息，请参阅 AWS Support API 参考。

主题

- 支持案例管理 (p. 15)
- AWS Trusted Advisor (p. 15)
- 端点 (p. 16)
- 在 AWS 开发工具包中支持 (p. 16)

支持案例管理

可使用 API 执行以下任务：

- 打开支持案例
- 获取最近的支持案例的列表及相关详细信息
- 通过日期和案例标识符筛选支持案例（包括已经解决的案例）的搜索
- 将通信信息和文件附件添加到您的案例，并添加案例通信的电子邮件收件人
- 解决您的案例

AWS SupportAPI 能够对支持案例管理操作执行 CloudTrail 日志记录。有关更多信息，请参阅使用 AWS Support 记录 AWS CloudTrail API 调用 (p. 314)：

有关演示如何管理支持案例的整个生命周期的代码示例，请参阅为 AWS Support 使用 AWS SDK 的代码示例。

AWS Trusted Advisor

您可以使用 Trusted Advisor 操作执行以下任务：

- 获取 Trusted Advisor 检查的名称和标识符
- 请求针对您的 AWS 账户和资源运行 Trusted Advisor 检查
- 获取 Trusted Advisor 检查结果的摘要和详细信息
- 刷新您的 Trusted Advisor 检查

- 获取每个 Trusted Advisor 检查的状态

该AWS Support API 支持Trusted Advisor操作 CloudTrail 记录。有关更多信息，请参阅 CloudTrail 日志记录中的 AWS Trusted Advisor 信息 (p. 315)：

您可以使用 Amazon Ev CloudWatch ents 监控对您的检查结果的更改Trusted Advisor。有关更多信息，请参阅与亚马逊一起监控AWS Trusted Advisor检查结果EventBridge (p. 327)：

例如，演示如何使用 Trusted Advisor 操作的 Java 代码，请参阅 使用 Trusted Advisor 即 Web 服务 (p. 25)。

端点

AWS Support 是一项全球性服务。这意味着您使用的任何端点都将在支持中心控制台中更新您的支持案例。

例如，如果您使用美国东部（弗吉尼亚州北部）端点创建案例，则可以使用美国西部（俄勒冈州）或欧洲地区（爱尔兰）端点为同一案例添加对应关系。

您可以使用以下端点访问 AWS Support API：

- 美国东部（弗吉尼亚州北部）：https://support.us-east-1.amazonaws.com
- 美国西部（俄勒冈州）：https://support.us-west-2.amazonaws.com
- 欧洲地区（爱尔兰）：https://support.eu-west-1.amazonaws.com

Important

- 如果您调用 Test A CreateCaseIso（测试支持案例），我们建议您包含一个主题行，例如 T EST CASE-Please ignor e。完成测试支持案例后，调用 Also（ResolveCase操作来解决案例）案例。
- 要调用 AWS Support API 中的 AWS Trusted Advisor 操作，必须使用美国东部（弗吉尼亚州北部）端点。目前，美国西部（俄勒冈州）和欧洲地区（爱尔兰）端点不支持这些 Trusted Advisor 操作。

有关 AWS 端点的更多信息，请参阅《Amazon Web Services 一般参考》中的 AWS Support 端点和限额。

在 AWS 开发工具包中支持

AWS Command Line Interface (AWS CLI) 和 AWS 软件开发工具包 (SDK) 包括对 AWS Support API 的支持。

有关支持AWS Support API 的语言列表中，请选择一个操作名称，例如 CreateCase，并在 See Also（另请参阅）部分中，选择您的首选语言。

AWS Support Plans

您可以根据业务需求更改账户的 AWS Support Plans。

主题

- AWS Support 计划的功能 (p. 17)
- 更改 AWS Support Plans (p. 18)

AWS Support 计划的功能

AWS Support 提供五种 Support 计划：

- 基本
- 开发人员
- 业务
- Enterprise On-Ramp
- 企业

基本支持计划提供对账户和账单问题以及提升服务配额的支持。其他计划提供许多带有pay-by-the-month定价且没有长期合同的技术支持案例。

所有 AWS 客户自动获得对以下基本支持计划功能的全天候访问权限：

- O ne-on-one 对账户和账单问题的回复
- 支持论坛
- 服务运行状况检查
- 文档、技术论文和最佳实践指南

“开发人员”支持计划客户可以访问以下额外功能：

- 最佳实践指导
- 客户端诊断工具
- 构建块架构支持：关于 AWS 产品、功能和服务的使用指导
- 支持无限数量的支持案例，这些案例可由一个主要联系人打开，即 AWS 账户根用户。

此外，拥有商业、Enterprise On-Ramp 和企业 Support 计划的客户还可以访问以下功能：

- 使用案例指导 – 使用哪些 AWS 产品、功能和服务最符合您的具体需要。
- AWS Trusted Advisor (p. 19) – 一种 AWS Support 功能，它会检查客户环境，找出可节省开支、弥补安全漏洞并提高系统可靠性和性能的机会。您可以访问所有 Trusted Advisor 检查。
- 与支持中心和 Trusted Advisor 交互的 AWS Support API。您可以使用 AWS Support API 自动执行支持案例管理和 Trusted Advisor 操作。
- 第三方软件支持 – 针对 Amazon Elastic Compute Cloud (Amazon EC2) 实例操作系统和配置提供帮助。此外，还针对 AWS 上常用的第三方软件组件的性能问题提供帮助。对于使用基本或开发人员支持计划的客户，不提供第三方软件支持。
- 支持无限数量的 AWS Identity and Access Management (IAM) 用户，他们可以打开技术支持案例。

此外，拥有 Enterprise On-Ramp 和企业 Support 计划的客户还可以访问以下功能：

- 应用程序架构指导 – 关于如何组合运用各项服务来满足您的特定使用案例、工作负载或应用程序需求的咨询指导。
- 基础设施事件管理 – 使用 AWS Support 短期介入，深入理解您的使用案例。执行分析后，为事件提供架构和扩展方面的指导。
- 技术客户经理 – 针对您的特定使用案例和应用程序，与技术客户经理 (TAM) 合作。
- 案例处理特别通道。
- 管理商业评论。

有关每个支持计划的功能和定价的更多信息，请参阅 AWS Support 和比较 AWS Support 计划。一些功能（如全天候电话和聊天支持）并非以所有语言提供。

更改 AWS Support Plans

您可以使用 AWS Support Plans 控制台更改 AWS 账户 的支持计划。若要更改您的支持计划，您必须具有 AWS Identity and Access Management（IAM）权限或以根用户身份登录您的账户。有关更多信息，请参阅 管理对 AWS Support 计划的访问权限 (p. 224) 和 适用于 AWS Support Plans 的 AWS 托管策略 (p. 220)。

更改您的支持计划

1. 在 https://console.aws.amazon.com/support/plans/home 登录 AWS Support Plans 控制台。
2. （可选）在 AWS Support Plans 页面，比较支持计划。有关定价的更多信息，请参阅定价详细信息页面。
3. （可选）在 AWS Support 定价示例下，选择查看示例，然后选择其中一个支持计划选项以查看预估成本。
4. 您决定计划时，为您需要的计划选择 Review downgrade（查看降级）或 Review upgrade（查看升级）。

   注意

   - 如果您注册了付费支持计划，则需要至少订阅一个月的 AWS Support。有关更多信息，请参阅 AWS Support 常见问题。
   - 如果您拥有 Enterprise On-Ramp 或 Enterprise Support 计划，在 Change plan confirmation（更改计划确认）对话框上，联系 AWS Support 以更改您的支持计划。
5. 在 Change plan confirmation（更改计划确认）对话框中，您可以展开支持项目以查看要在帐户中添加或删除的功能。

   在 Pricing（定价）下，您可以查看新支持计划的预计一次性费用。
6. 选择 Accept and agree（接受并同意）。

相关信息

有关 AWS Support 计划的更多信息，请参阅 AWS Support 常见问题解答。您还可以从 Support Plans 控制台中选择 Contact us（联系我们）。

要关闭账户，请参阅 AWS Billing 用户指南中的关闭账户。

AWS Trusted Advisor

Trusted Advisor 凝聚了从为数十万 AWS 客户提供服务中总结的最佳实践。Trusted Advisor 可检查您的 AWS 环境，然后在有可能节省开支、提高系统可用性和性能或弥补安全漏洞时为您提供建议。

如果您使用的是基本或开发人员支持计划，则可以使用 Trusted Advisor 控制台访问“Service Limits”类别中的所有检查和“安全”类别中的六个检查。

如果您拥有商业、Enterprise On-Ramp 或企业 Support 计划，则可以使用 Trusted Advisor 控制台和 AWS Support API (p. 15) 访问所有的 Trusted Advisor 检查。您也可以使用 Amazon E CloudWatch vents 来监控Trusted Advisor检查的状态。有关更多信息，请参阅与亚马逊一起监控AWS Trusted Advisor检查结果 EventBridge (p. 327)：

您可以在 AWS Management Console 中访问 Trusted Advisor。有关控制对 Trusted Advisor 控制台的访问权限的更多信息，请参阅 管理对 AWS Trusted Advisor 的访问 (p. 226)。

有关更多信息，请参阅 Trusted Advisor。

主题

- 开始使用 Trusted Advisor 建议 (p. 19)
- 使用 Trusted Advisor 即 Web 服务 (p. 25)
- AWS Trusted Advisor 的组织视图 (p. 29)
- 在 AWS Trusted Advisor 中查看 AWS Security Hub 控件 (p. 46)
- 启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查 (p. 51)
- AWS Trusted Advisor Priority 入门 (p. 52)
- 开始使用 EngAWS Trusted Advisor age（预览版） (p. 59)
- AWS Trusted Advisor 检查引用 (p. 65)
- AWS Trusted Advisor 的更改日志 (p. 145)

开始使用 Trusted Advisor 建议

您可以使用 Trusted Advisor 控制台的 Trusted Advisor 建议页面来查看 AWS 账户的检查结果，然后按照建议的步骤修复任何问题。例如，Trusted Advisor 可能会建议您删除未使用的资源以减少您的月费，例如 Amazon Elastic Compute Cloud (Amazon EC2) 实例。

您也可以使用 AWS Support API 来对您的 Trusted Advisor 检查执行操作。有关详细信息，请参阅 AWS Support API 参考。

主题

- 登录到 Trusted Advisor 控制台 (p. 20)
- 查看检查类别 (p. 21)
- 查看特定检查 (p. 22)
- 筛选您的检查 (p. 23)
- 刷新检查结果 (p. 24)
- 下载检查结果 (p. 24)
- 组织视图 (p. 24)
- Preferences（首选项） (p. 24)

登录到 Trusted Advisor 控制台

您可以在 Trusted Advisor 控制台中查看检查和每个检查的状态。

Note

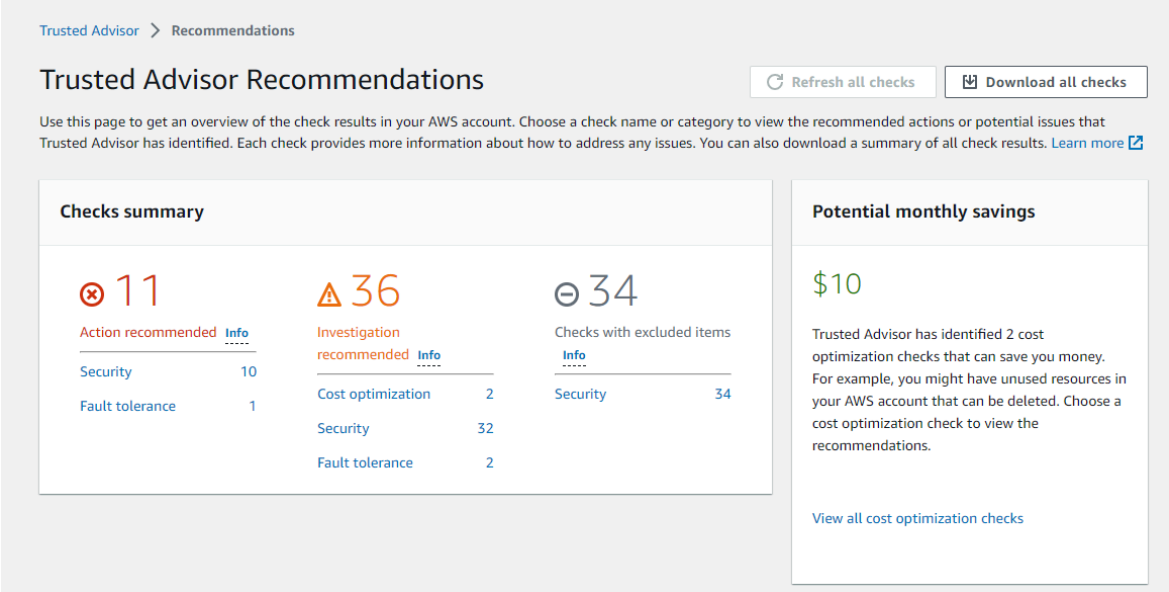
您必须具有 AWS Identity and Access Management (IAM) 权限才能访问 Trusted Advisor 控制台。有关更多信息，请参阅管理对 AWS Trusted Advisor 的访问 (p. 226)：

登录到 Trusted Advisor 控制台

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在 Trusted Advisor 建议页面上，查看每种检查类别的摘要：
   - 建议操作（红色）– Trusted Advisor 建议对检查进行的操作。例如，检测到 IAM 资源安全问题的检查可能会建议紧急步骤。
   - 建议调查（黄泽）– Trusted Advisor检测到检查的可能问题。例如，达到资源配额的检查可能会建议删除未使用的资源的方法。
   - Checks with excluded items (gray) [带排除项目的检查项（灰色）]：带排除项目的检查项数量，例如您希望检查忽略的资源。例如，这可能是您不希望检查评估的 Amazon EC2 实例。
3. 在 Trusted Advisor 建议页面上，您可以执行以下操作：
   - 要刷新您的账户中的所有检查，请选择 Refresh all checks（刷新所有检查）。
   - 要创建包含所有检查结果的 .xls 文件，请选择 Download all checks（下载所有检查）。
   - 在 Checks summary（检查摘要）下，选择一个检查类别，例如 Security（安全性），以查看结果。
   - 在 Potential monthly savings（可能的月节省）下，您可以查看您的账户可能节省的成本以及成本优化检查建议。
   - 在 Recent changes（最近的更改）下，您可以查看最近 30 天内的检查状态更改。选择一个检查名称以查看该检查的最新结果，或者选择箭头图标查看下一页。

Example ：Trusted Advisor 建议

以下示例显示了 AWS 账户 检查结果的摘要。



查看检查类别

您可以查看以下检查类别的检查说明和结果：

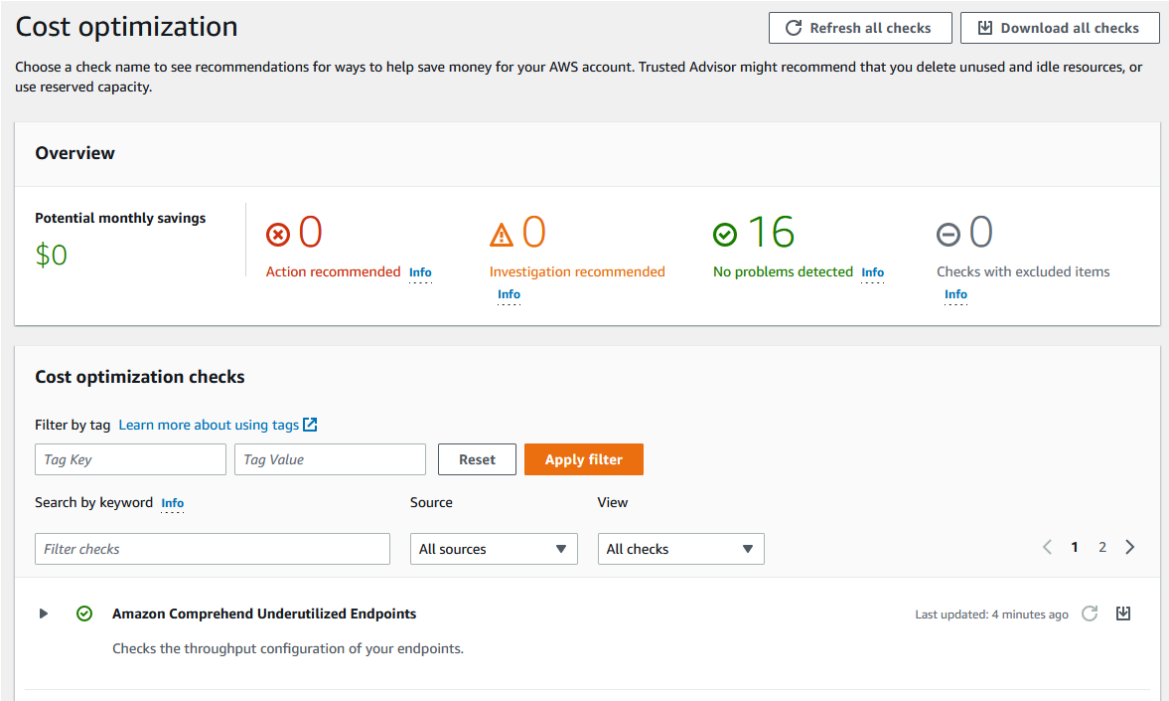
- Cost optimization（成本优化）– 可能会为您节省成本的建议。这些检查突出显示未使用的资源和减少账单的机会。
- 性能 – 可以提高您的应用程序速度和响应能力的建议。
- 安全 – 可以使您的 AWS 解决方案更加安全的安全设置的建议。
- Fault tolerance（容错能力）– 可帮助提高您的AWS解决方案的弹性的建议。这些检查突出显示冗余不足、当前服务限制（也称为配额）和过度使用的资源。
- Service limits（服务限制）– 检查您账户的使用情况以及您的账户是否接近或超过AWS服务和资源的限制（也称为配额）。

要查看检查类别

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在导航窗格中，选择检查类别。
3. 在类别页面上，查看每种检查类别的摘要：
   - 建议操作（红色）– Trusted Advisor 建议对检查进行的操作。
   - 建议调查（黄泽）– Trusted Advisor检测到检查的可能问题。
   - 未检测到问题（绿色）– Trusted Advisor 未检测到检查的问题。
   - 排除的项目（灰色）– 包含排除项目的检查数，例如您希望检查忽略的资源。
4. 对于每次检查，选择刷新图标 ( ) 以刷新此检查。
5. 选择下载图标 ( ) 以创建一个包含此检查结果的 .xls 文件。

Example ：成本优化类别

以下示例显示了 16 个没有任何问题的（绿色）检查。



查看特定检查

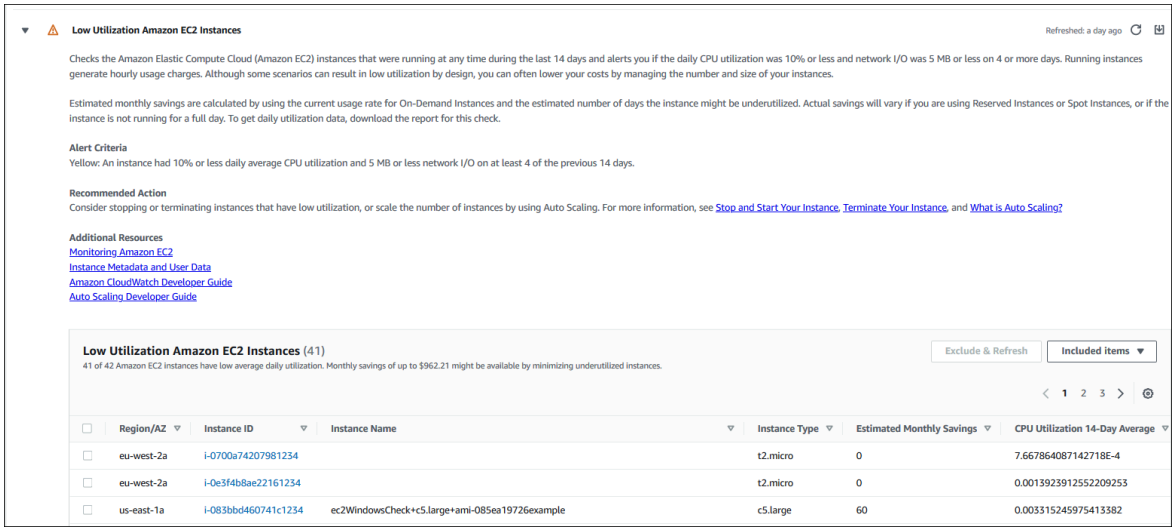
展开检查以查看完整的检查说明、受影响的资源、任何建议的步骤以及指向更多信息的链接。

要查看特定检查

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在导航窗格中，选择检查类别。
3. 选择检查名称以查看说明和以下详细信息：
   - 提示标准 – 描述检查将更改状态的阈值。
   - 建议的操作 – 描述此检查的建议操作。
   - 其他资源 – 列出相关的 AWS 文档。
   - 列出您账户中受影响项目的表。您可以在检查结果中包括或排除这些项目。
4. （可选）要排除项目，以使它们不出现在检查结果中：
   a. 选择一个项目，然后选择 Exclude & Refresh（排除和刷新）。
   b. 要查看所有排除的项目，请选择 Excluded items（排除的项目）。
5. （可选）要包括项目以便检查再次评估它们：
   a. 选择 Excluded items（排除的项目），选择一个项目，然后选择 Include & Refresh（包括和刷新）。
   b. 要查看所有包含的项目，请选择 Included items（包含的项目）。
6. 选择设置图标（ ）。在 Preferences（首选项）对话框中，您可以指定要显示的项目数或属性，然后选择 Confirm（确认）。

Example ：成本优化检查

以下低利用率 Amazon EC2 实例检查会列出账户中受影响的实例。此检查可识别 41 个使用率较低的 Amazon EC2 实例，并建议您停止或终止资源。



筛选您的检查

在检查类别页面上，您可以指定您要查看哪些检查结果。例如，您可以按检测到账户中错误的检查进行筛选，以便首先调查紧急问题。

如果您具有评估账户中的项目的检查，例如 AWS 资源，您可以使用标签筛选条件以仅显示具有指定标签的项目。

要筛选您的检查

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在导航窗格中或 Trusted Advisor 建议页面上，选择检查类别。
3. 对于 Search by keyword（按关键词搜索），请输入检查名称或描述中的关键词以筛选结果。
4. 对于 View（查看）列表，指定要查看哪些检查：
   - All checks（所有检查）：列出此类别的所有检查
   - 建议的操作 – 列出建议您采取操作的检查。这些检查以红色突出显示。
   - 建议的调查 – 列出建议您采取可能的操作的检查。这些检查以黄色突出显示。
   - 未检测到问题 – 列出没有任何问题的检查。这些检查以绿色突出显示。
   - 包含排除项目的检查 – 列出您指定的用于从检查结果中排除项目的检查。
5. 如果您将标签添加到 AWS 资源，例如 Amazon EC2 实例或 AWS CloudTrail 跟踪，您可以筛选结果，以使检查仅显示具有指定标签的项目。

   对于按标签筛选，输入标签键和值，然后选择 Apply filter（应用筛选条件）。
6. 在检查的表中，检查结果仅显示具有指定键和值的项目。
7. 要按标签清除筛选条件，请选择 Reset（重置）。

相关信息

有关 Trusted Advisor 的标签的更多信息，请参阅以下主题：

- AWS Support 启用 Trusted Advisor 的标记功能
- AWS 一般参考 中的添加 AWS 资源

刷新检查结果

您可以刷新检查以获取您账户的最新结果。如果您使用的是开发人员或基本支持计划，则可以登录 Trusted Advisor 控制台刷新检查。如果您拥有商业、Enterprise On-Ramp 和企业 Support 计划，则 Trusted Advisor 会每周自动刷新您账户中的检查。

要刷新 Trusted Advisor 检查

1. 导航到位于 https://console.aws.amazon.com/trustedadvisor 的 AWS Trusted Advisor 控制台。
2. 在 Trusted Advisor 建议或检查类别页面上，选择刷新所有检查。

您也可以通过以下方式刷新特定检查：

- 选择刷新图标 ( ) 进行单独检查。
- 使用 RefreshTrustedAdvisorCheck API 操作。

  注意

  - Trusted Advisor 会每天自动刷新几次某些检查，例如 AWS Well-Architected high risk issues for reliability (可靠性高风险问题) 检查。更改可能需要在几个小时后才会在您的账户中显示。对于这些自动刷新的检查，您无法选择刷新图标 ( ) 来手动刷新结果。
  - 如果您为账户启用了 AWS Security Hub，您将无法使用 Trusted Advisor 控制台来刷新 Security Hub 控件。有关更多信息，请参阅刷新 Security Hub 检查结果 (p. 48)：

下载检查结果

您可以下载检查结果以获取您账户中的 Trusted Advisor 的概述。您可以下载所有检查或指定检查的结果。

从 Trusted Advisor 建议下载检查结果

1. 导航到位于 https://console.aws.amazon.com/trustedadvisor 的 AWS Trusted Advisor 控制台。
   - 要下载所有检查结果，请在 Trusted Advisor 建议或检查类别页面上选择下载所有检查。
   - 要下载指定检查的检查结果，请选择检查名称，然后选择下载图标 ( ) 。
2. 保存或打开 .xls 文件。文件包含来自 Trusted Advisor 控制台的相同摘要信息，例如检查名称、描述、状态、受影响的资源等。

组织视图

您可以设置组织视图功能，以为 AWS 组织中的所有成员账户创建报告。有关更多信息，请参阅AWS Trusted Advisor 的组织视图 (p. 29)：

Preferences (首选项)

在管理Trusted Advisor页面上，您可以禁用 Trusted Advisor (p. 25)。

在 Notifications (通知) 页面上，您可以为检查摘要配置每周电子邮件。请参阅设置通知首选项 (p. 25)。

在您的组织页面上，您可以启用或禁用 AWS Organizations 的可信访问权限。这是AWS Trusted Advisor 的组织视图 (p. 29)功能、“Trusted Advisor优先级 (p. 52)” 和 “Trusted Advisor参与 (p. 59)” 所必需的。

设置通知首选项

指定谁可以接收检查结果和语言的 每周 Trusted Advisor 电子邮件消息。您每周都会收到一封关于 Trusted Advisor 建议检查摘要的电子邮件通知。

Trusted Advisor 建议的电子邮件通知不包含 Trusted Advisor Priority 的结果。有关更多信息，请参阅管理 Trusted Advisor Priority 通知 (p. 58)：

要设置通知首选项

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在导航窗格中的 Preferences（首选项）下，选择 Notifications（通知）。
3. 对于 Recommendations（建议），选择接收检查结果的对象。您可以从 AWS Billing and Cost Management 控制台的 Account Settings（账户设置）页面中添加和删除联系人。
4. 对于 Language（语言），选择电子邮件消息的语言。
5. 选择 Save your preferences（保存首选项）。

设置组织视图

如果您使用 AWS Organizations 设置账户，您可以为组织中的所有成员账户创建报告。有关更多信息，请参阅AWS Trusted Advisor 的组织视图 (p. 29)：

禁用 Trusted Advisor

禁用此服务时，Trusted Advisor 不会对您的账户执行任何检查。尝试访问 Trusted Advisor 控制台或使用 API 操作的任何人都将收到拒绝访问错误消息。

要禁用 Trusted Advisor

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在导航窗格中的首选项下，选择管理 Trusted Advisor。
3. 在 Trusted Advisor 下，关闭 Enabled（已启用）。此操作为您账户中的所有检查禁用 Trusted Advisor。
4. 然后，您可以手动从您的账户中删除该AWSServiceRoleForTrustedAdvisorTrusted Advisor。有关更多信息，请参阅删除 Trusted Advisor 的服务相关角色 (p. 201)：

相关信息

有关 Trusted Advisor 的更多信息，请参阅以下主题：

- 如何开始使用 Trusted Advisor？
- AWS Trusted Advisor 检查引用 (p. 65)

使用 Trusted Advisor 即 Web 服务

借助 AWS Support 服务，您可以编写与 AWS Trusted Advisor 交互的应用程序。此主题演示如何获取 Trusted Advisor 检查的列表、刷新其中一个检查，然后获取检查返回的详细结果。这些任务用 Java 进行演示。有关针对其他语言的支持的信息，请参阅用于 Amazon Web Services 的工具。

主题

- 获取可用 Trusted Advisor 检查的列表 (p. 26)
- 刷新可用 Trusted Advisor 检查的列表 (p. 26)
- 轮询 Trusted Advisor 检查以了解状态变化 (p. 27)
- 请求 Trusted Advisor 检查结果 (p. 28)
- 输出 Trusted Advisor 检查的详细信息 (p. 28)

获取可用 Trusted Advisor 检查的列表

以下 Java 代码段创建一个 AWS Support 客户端实例，您可使用该客户端来调用所有 Trusted Advisor API 操作。接下来，这段代码通过调用 DescribeTrustedAdvisorChecksAPI 操作，获取Trusted Advisor检查的列表及其相应CheckId值。您可以使用此信息来构建用户界面，让用户通过此界面选择他们想运行或刷新的检查。

```
private static AWSSupport createClient()
{
    return AWSSupportClientBuilder.defaultClient();
}
// Get the List of Available Trusted Advisor Checks
public static void getTAChecks() {
    // Possible language parameters: "en" (English), "ja" (Japanese), "fr" (French),
 "zh" (Chinese)
    DescribeTrustedAdvisorChecksRequest request = new
 DescribeTrustedAdvisorChecksRequest().withLanguage("en");
    DescribeTrustedAdvisorChecksResult result =
 createClient().describeTrustedAdvisorChecks(request);
    for (TrustedAdvisorCheckDescription description : result.getChecks()) {
        // Do something with check description.
        System.out.println(description.getId());
        System.out.println(description.getName());
    }
}
```

刷新可用 Trusted Advisor 检查的列表

以下 Java 代码段创建一个 AWS Support 客户端实例，您可使用该客户端来刷新 Trusted Advisor 数据。

```
// Refresh a Trusted Advisor Check
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation.
// Specifying the check ID of a check that is automatically refreshed causes an
 InvalidParameterValue error.
public static void refreshTACheck(final String checkId) {
    RefreshTrustedAdvisorCheckRequest request = new
 RefreshTrustedAdvisorCheckRequest().withCheckId(checkId);
    RefreshTrustedAdvisorCheckResult result =
 createClient().refreshTrustedAdvisorCheck(request);
    System.out.println("CheckId: " + result.getStatus().getCheckId());
    System.out.println("Milliseconds until refreshable: " +
 result.getStatus().getMillisUntilNextRefreshable());
    System.out.println("Refresh Status: " + result.getStatus().getStatus());
}
```

轮询 Trusted Advisor 检查以了解状态变化

在提交运行Trusted Advisor检查以生成最新状态数据的请求之后，请使用 DescribeTrustedAdvisorCheckRefreshStatusesAPI 操作请求检查运行进度以及新数据做好检查准备的时间。

以下 Java 代码段使用 CheckId 变量中的相应值获取在以下部分中请求的检查的状态。此外，此段代码还演示了 Trusted Advisor 服务的其他几种用途：

1. 您可以通过遍历 DescribeTrustedAdvisorCheckRefreshStatusesResult 实例中包含的对象来调用 getMillisUntilNextRefreshable。您可以使用返回的值来测试是否希望代码继续刷新检查。
2. 如果 timeUntilRefreshable 等于零，您可以请求刷新检查。
3. 您可以使用返回的状态继续轮询状态变化，代码段将轮询间隔设置为建议的 10 秒。如果状态为 enqueued 或 in_progress，循环将返回并再次请求状态。如果调用返回 successful，则循环终止。
4. 最后，代码返回一个 DescribeTrustedAdvisorCheckResultResult 数据类型的实例，您可使用该实例遍历检查所生成的信息。

注意：请先使用单个刷新请求，然后再轮询请求的状态。

```
// Retrieves TA refresh statuses. Multiple checkId's can be submitted.
public static List<TrustedAdvisorCheckRefreshStatus> getTARefreshStatus(final String...
 checkIds) {
    DescribeTrustedAdvisorCheckRefreshStatusesRequest request =
            new DescribeTrustedAdvisorCheckRefreshStatusesRequest().withCheckIds(checkIds);
    DescribeTrustedAdvisorCheckRefreshStatusesResult result =
            createClient().describeTrustedAdvisorCheckRefreshStatuses(request);
    return result.getStatuses();
}
// Retrieves a TA check status, and checks to see if it has finished processing.
public static boolean isTACheckStatusInTerminalState(final String checkId) {
    // Since we only submitted one checkId to getTARefreshStatus, just retrieve the only
 element in the list.
    TrustedAdvisorCheckRefreshStatus status = getTARefreshStatus(checkId).get(0);
    // Valid statuses are:
    // 1. "none", the check has never been refreshed before.
    // 2. "enqueued", the check is waiting to be processed.
    // 3. "processing", the check is in the midst of being processed.
    // 4. "success", the check has succeeded and finished processing - refresh data is
 available.
    // 5. "abandoned", the check has failed to process.
    return status.getStatus().equals("abandoned") || status.getStatus().equals("success");
}
// Enqueues a Trusted Advisor check refresh. Periodically polls the check refresh status
 for completion.
public static TrustedAdvisorCheckResult getFreshTACheckResult(final String checkId) throws
 InterruptedException {
    refreshTACheck(checkId);
    while(!isTACheckStatusInTerminalState(checkId)) {
        Thread.sleep(10000);
    }
    return getTACheckResult(checkId);
}
// Retrieves fresh TA check data whenever possible.
// Note: Some checks are refreshed automatically, and they cannot be refreshed by using
 this operation. This method
// is only functional for checks that can be refreshed using the RefreshTrustedAdvisorCheck
 operation.
public static void pollForTACheckResultChanges(final String checkId) throws
 InterruptedException {
    String checkResultStatus = null;
```

```
    do {
        TrustedAdvisorCheckResult result = getFreshTACheckResult(checkId);
        if (checkResultStatus != null && !checkResultStatus.equals(result.getStatus())) {
            break;
        }
        checkResultStatus = result.getStatus();
        // The rule refresh has completed, but due to throttling rules the checks may not
 be refreshed again
        // for a short period of time.
        // Since we only submitted one checkId to getTARefreshStatus, just retrieve the
 only element in the list.
        TrustedAdvisorCheckRefreshStatus refreshStatus =
 getTARefreshStatus(checkId).get(0);
        Thread.sleep(refreshStatus.getMillisUntilNextRefreshable());
    } while(true);
    // Signal that a TA check has changed check result status here.
}
```

请求 Trusted Advisor 检查结果

选择所需的详细结果检查之后，使用 DescribeTrustedAdvisorCheckResultAPI 操作来提交请求。

> Tip
>
> Trusted Advisor 检查的名称和说明可能会发生变化。我们建议您在代码中指定检查 ID 以唯一标识检查。您可以使用 DescribeTrustedAdvisorChecksAPI 操作，以获取检查 ID。

以下 Java 代码段使用 `result` 变量引用的 `DescribeTrustedAdvisorChecksResult` 实例（在之前的代码段中获得）。您提交运行请求之后，该代码段并未通过用户界面以交互方式定义检查，而是通过在每个 `result.getChecks().get(0)` 调用中指定索引值 0 来提交运行列表中第一个检查的请求。接下来，此段代码定义一个 `DescribeTrustedAdvisorCheckResultRequest` 实例，并将该实例传递给名为 `checkResult` 的 `DescribeTrustedAdvisorCheckResultResult` 实例。您可以使用此数据类型的成员结构查看检查结果。

```
// Request a Trusted Advisor Check Result
public static TrustedAdvisorCheckResult getTACheckResult(final String checkId) {
    DescribeTrustedAdvisorCheckResultRequest request = new
 DescribeTrustedAdvisorCheckResultRequest()
            // Possible language parameters: "en" (English), "ja" (Japanese),
 "fr" (French), "zh" (Chinese)
            .withLanguage("en")
            .withCheckId(checkId);
    DescribeTrustedAdvisorCheckResultResult requestResult =
 createClient().describeTrustedAdvisorCheckResult(request);
    return requestResult.getResult();
}
```

注意：请求 Trusted Advisor 检查结果不会生成更新的结果数据。

输出 Trusted Advisor 检查的详细信息

以下 Java 代码段遍历前一节返回的 `DescribeTrustedAdvisorCheckResultResult` 实例，以获取 Trusted Advisor 检查所标记的资源的列表。

```
// Print ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
```

```
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

AWS Trusted Advisor 的组织视图

组织视图允许您查看 AWS Organizations 中所有账户的 Trusted Advisor 检查。启用此功能后，您可以创建报告来聚合组织中所有成员账户的检查结果。该报告包括检查结果的摘要以及每个账户的受影响资源的信息。例如，您可以使用报告通过 IAM 使用检查确定组织中的哪些账户正在使用 AWS Identity and Access Management (IAM)，或者您是否已通过 Amazon S3 存储桶权限检查对 Amazon Simple Storage Service (Amazon S3) 存储桶提出操作建议。

主题

- 先决条件 (p. 29)
- 启用组织视图 (p. 29)
- 刷新 Trusted Advisor 检查 (p. 30)
- 创建组织视图报告 (p. 30)
- 查看报告摘要 (p. 33)
- 下载组织视图报告 (p. 34)
- 禁用组织视图 (p. 38)
- 使用 IAM 策略允许访问组织视图 (p. 38)
- 使用其他 AWS 服务查看 Trusted Advisor 报告 (p. 40)

先决条件

您必须满足以下要求才能启用组织视图：

- 该账户必须是 AWS 组织的成员。
- 您的组织必须已启用 Organizations 的所有功能。有关更多信息，请参阅 AWS Organizations 用户指南中的启用组织中的所有功能。
- 您组织中的管理账户必须拥有商业、Enterprise On-Ramp 和企业 Support 计划。您可以从 AWS Support 中心或从 Support plans（支持计划）页面中查找您的支持计划。请参阅比较 AWS Support 计划。
- 您必须以管理账户中的用户身份（或承担的等效角色）登录。无论您是以 IAM 用户还是 IAM 角色登录，您都必须拥有具有所需权限的策略。请参阅使用 IAM 策略允许访问组织视图 (p. 38)。

启用组织视图

满足上述先决条件之后，请按照以下步骤启用组织视图。启用此功能后，将出现以下情况：

- Trusted Advisor 被启用为组织中的可信服务。有关更多信息，请参阅 AWS Organizations 用户指南中的使用其他 AWS 服务启用可信访问权限。
- `AWSServiceRoleForTrustedAdvisorReporting` service-linked-role是在您组织的管理账户中为您创建的。此角色包括 Trusted Advisor 代表您调用 Organizations 所需的权限。此服务关联角色已锁定，您无法手动删除它。有关更多信息，请参阅将服务相关角色用于 Trusted Advisor (p. 199)：

在 Trusted Advisor 控制台中启用组织视图。

要启用组织视图

1. 以管理员身份登录组织的管理账户，并打开位于 https://console.aws.amazon.com/trustedadvisor 的 AWS Trusted Advisor 控制台。
2. 在导航窗格中的 Preferences（首选项）下，选择 Your organization（您的组织）。
3. 在 “启用可信访问方式” 下AWS Organizations，打开 “启用”。

Note

为管理账户启用组织视图不会为所有成员账户提供相同的检查。例如，如果您的成员账户都具有基本支持，那么这些账户将不会拥有与管理账户相同的检查。AWS Support 计划决定了为账户提供了哪些 Trusted Advisor 检查。

刷新 Trusted Advisor 检查

在您为组织创建报告之前，我们建议您刷新您的 Trusted Advisor 检查的状态。您可以下载报告，而无需刷新 Trusted Advisor 检查，但您的报告可能不包含最新信息。

如果您拥有商业、Enterprise On-Ramp 和企业 Support 计划，则 Trusted Advisor 会每周自动刷新您账户中的检查。

Note

如果您的组织中有具有开发人员或基本支持计划的账户，则这些账户的用户必须登录 Trusted Advisor 控制台刷新检查。您无法刷新组织管理账户中的所有账户的检查。

要刷新 Trusted Advisor 检查

1. 导航到位于 https://console.aws.amazon.com/trustedadvisor 的 AWS Trusted Advisor 控制台。
2. 在 “Trusted Advisor建议” 页面上，选择 “刷新所有支票”。这将刷新您账户中的所有检查。

您也可以通过以下方式刷新特定检查：

- 使用 RefreshTrustedAdvisorCheck API 操作。
- 选择刷新图标 ( ) 进行单独检查。

创建组织视图报告

启用组织视图后，您可以创建报告，以便可以查看组织的 Trusted Advisor 检查结果。

您最多可以创建 50 个报告。如果创建的报告超出此配额，Trusted Advisor 会删除最早的报告。您无法恢复已删除的报告。

要创建组织视图报告

1. 登录组织的管理账户，并打开位于 https://console.aws.amazon.com/trustedadvisor 的 AWS Trusted Advisor 控制台。
2. 在导航窗格中，选择 Organizational View（组织视图）。
3. 选择创建报告。
4. 默认情况下，报告包含所有 AWS 区域、检查类别、检查和资源状态。在 Create report（创建报告）页面上，您可以使用筛选条件选项自定义报告。例如，您可以清除区域的 All（全部）选项，然后指定要包括在报告中的单个区域。

a. 输入报告的 Name（名称）。
b. 对于 Format，选择 JSON 或 CSV。
c. 对于 Region（区域），指定 AWS 区域或选择 All（全部）。
d. 对于 Check category（检查类别），选择检查类别或选择 All（全部）。
e. 对于 Checks（检查），选择该类别的特定检查，或选择 All（全部）。

Note

Check category（检查类别）筛选条件将覆盖 Checks（检查）筛选条件。例如，如果您选择 Security（安全）类别，然后选择特定的检查名称，则您的报告将包含该类别的所有检查结果。若要仅针对特定检查创建报告，请为检查类别保留默认的 All（全部）值，然后选择您的检查名称。

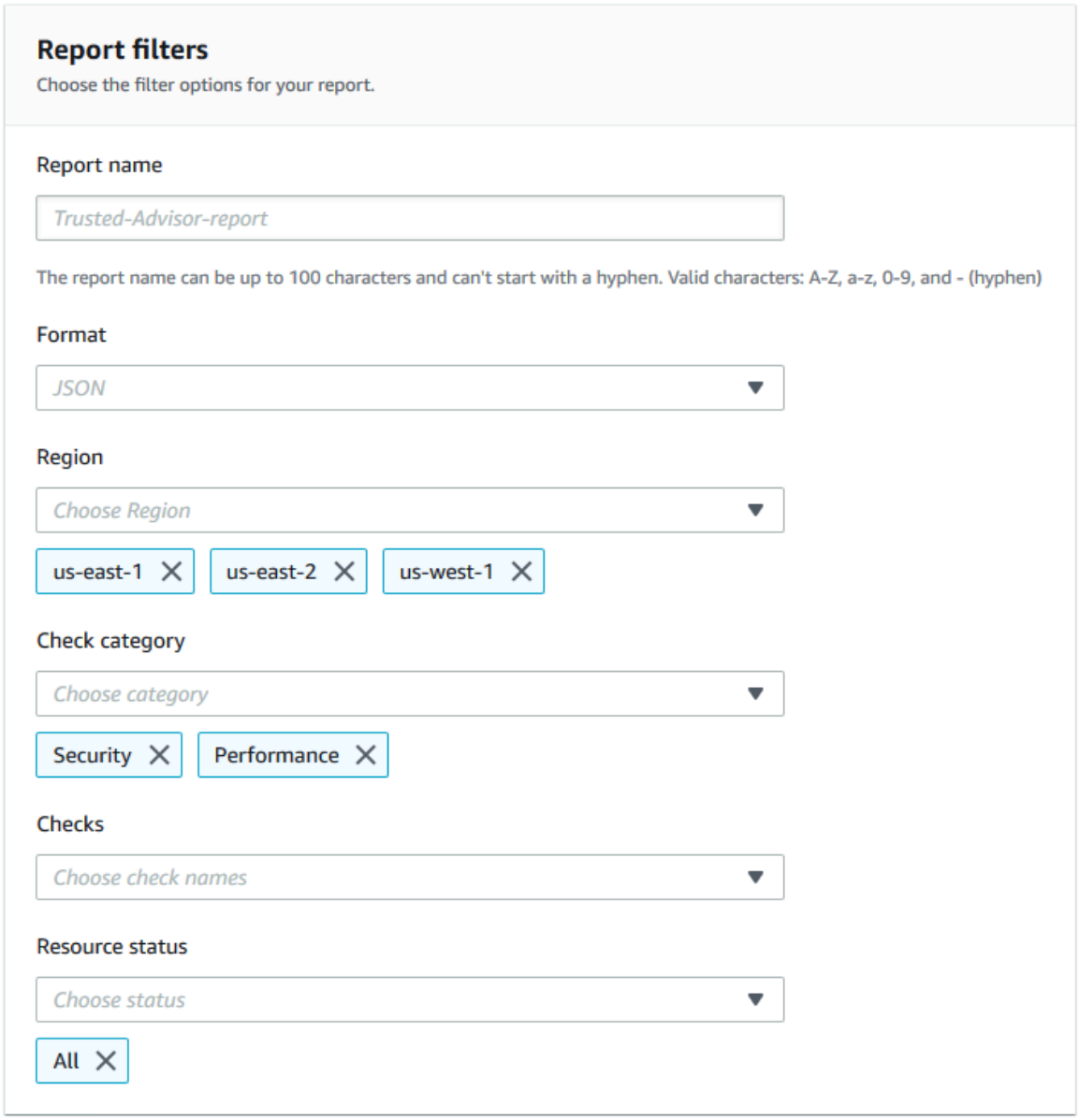
f. 对于 Resource status（资源状态），选择要筛选的状态，如 Warning（警告），或选择 All（全部）。

5. 对于 AWS 组织，选择要包含在您的报告中的组织单位 (OU)。有关 OU 的更多信息，请参阅 AWS Organizations 用户指南中的管理组织单位。
6. 选择创建报告。

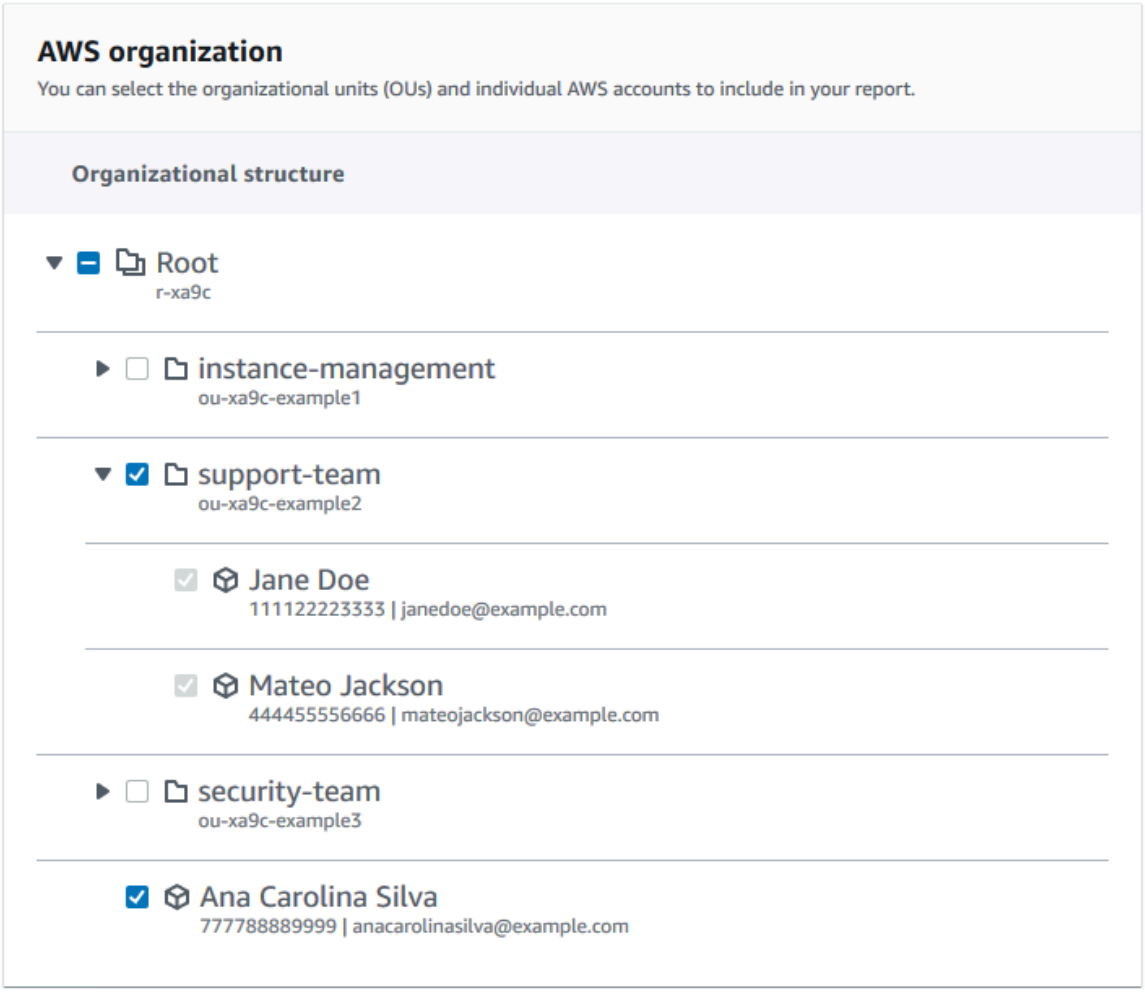
Example ：创建报告筛选条件选项

以下示例为以下选项创建 JSON 报告：

- 三个 AWS 区域
- 所有的安全和性能检查



在以下示例中，报告包含 support-team OU 和属于组织一部分的一个 AWS 账户。



注意

- 创建报告所需的时间量取决于组织中的账户数量以及每个账户中的资源数量。
- 您不能一次创建多个报告，除非当前报告已运行超过 6 个小时。
- 如果您没有看到报告显示在页面上，请刷新页面。

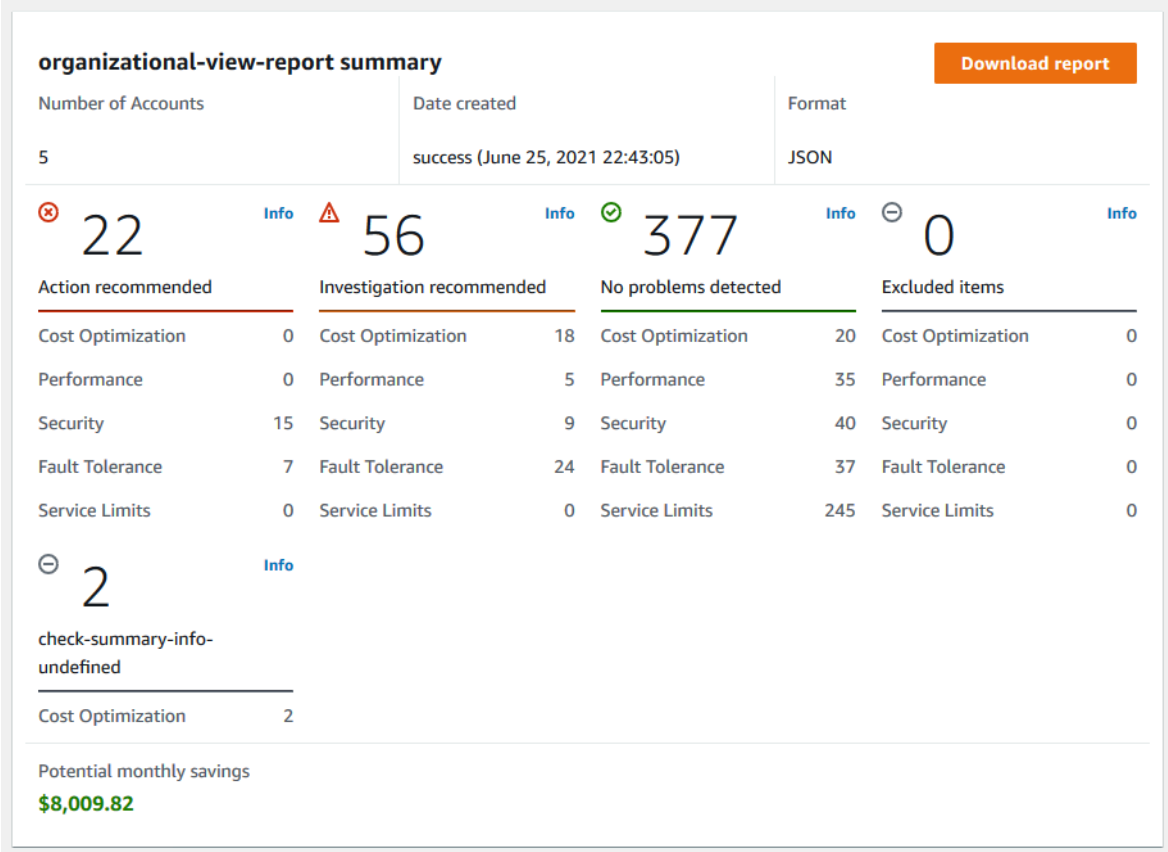
查看报告摘要

报告准备就绪后，您可以从 Trusted Advisor 控制台中查看报告摘要。这样，您就可以快速查看整个组织的检查结果摘要。

要查看报告摘要

1. 登录组织的管理账户，并打开位于 https://console.aws.amazon.com/trustedadvisor 的 AWS Trusted Advisor 控制台。
2. 在导航窗格中，选择 Organizational View（组织视图）。
3. 选择报告名称。
4. 在 Summary（摘要）页面上，查看每种类别的检查状态。您还可以选择 Download report（下载报告）。

Example ：组织的报告摘要



下载组织视图报告

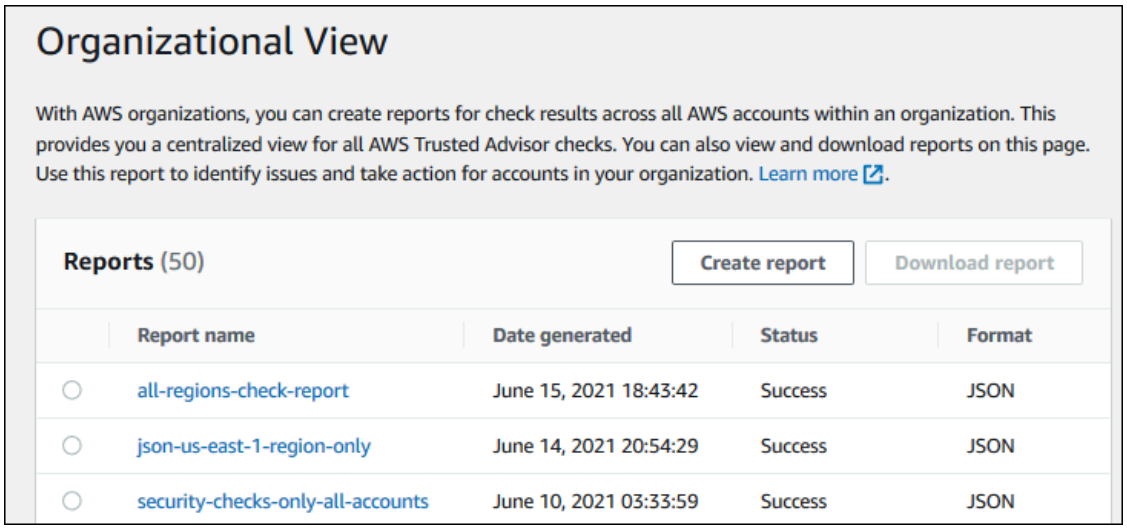
报告准备好后，请从 Trusted Advisor 控制台中下载报告。报告是一个 .zip 文件，其中包含三个文件：

- `summary.json` – 包含每种检查类别的检查结果的摘要。
- `schema.json` – 包含报告中指定检查的 schema。
- 资源文件（.json 或 .csv）– 包含有关组织中资源的检查状态的详细信息。

要下载组织视图报告

1. 登录组织的管理账户，并打开位于 https://console.aws.amazon.com/trustedadvisor 的 AWS Trusted Advisor 控制台。
2. 在导航窗格中，选择 Organizational View（组织视图）。

   Organizational View（组织视图）页面显示可供下载的报告。
3. 选择一个报告，选择 Download report（下载报告），然后保存文件。一次只能下载一个报告。



4. 解压缩该文件。
5. 使用文本编辑器打开 `.json`文件或使用电子表格应用程序打开 `.csv` 文件。

   Note

   如果您的报告为 5MB 或以上，您可能会收到多个文件。

Example ：summary.json 文件

`summary.json` 文件显示组织中的账户数量以及每种类别中的检查的状态。

Trusted Advisor 使用以下颜色代码表示检查结果：

- `Green` – Trusted Advisor 没有检测到检查的问题。
- `Yellow` – Trusted Advisor 检测到检查的可能问题。
- `Red` – Trusted Advisor 检测到错误并建议执行检查操作。
- `Blue` – Trusted Advisor 无法确定检查的状态。

在以下示例中，两个检查为 `Red`，一个为 `Green`，一个为 `Yellow`。

```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
```

```
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
                    "name": "Yellow",
                    "count": 1
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example ：schema.json 文件

schema.json 文件包含报告中的检查的 schema。以下示例包括 IAM 密码策略的 ID 和属性 (Yw2K9puPzl) 和 IAM 密钥轮换 (DqdJqYeRm5) 检查。

```
{
    "Yw2K9puPzl": [
        "Password Policy",
        "Uppercase",
        "Lowercase",
        "Number",
        "Non-alphanumeric",
        "Status",
        "Reason"
    ],
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
```

```
    ],
    ...
}
```

Example ：resources.csv 文件

resources.csv 文件包含组织中资源的相关信息。此示例显示了报告中显示的一些数据列，如下所示：

- 受影响账户的账户 ID
- Trusted Advisor 检查 ID
- 资源 ID
- 报告的时间戳
- Trusted Advisor 检查的完整名称
- Trusted Advisor 检查类别
- 父组织单位 (OU) 或根账户的账户 ID

AccountId	CheckId	ResourceId	TimeStamp	CheckName	Category
1.11122E+11	Qch7DwouX1	LnW14f1M40NMjmMLvY5	1.58983E+12	Low Utilization Amazon EC2 Instances	Cost Optimizing
1.11122E+11	HCP4007jGY	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
1.11122E+11	HCP4007jGY	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Specific Ports Unrestricted	Security
4.44456E+11	1iG5NDGVre	dJrQZXw36ZdswBeo9WUl	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	1iG5NDGVre	1hzakmTbWd5UmAM_a0L	1.58983E+12	Security Groups - Unrestricted Access	Security
4.44456E+11	Pfx0RwqBli	vioZmlba45kf2JWIe_W0j5	1.58983E+12	Amazon S3 Bucket Permissions	Security
4.44456E+11	Pfx0RwqBli	wAvASS3YOwy6WWxlBHf	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	LIc4zRaUSiIGRSlmqaMa5V	1.58983E+12	Amazon S3 Bucket Permissions	Security
1.23457E+11	Pfx0RwqBli	gWB27TMXof2evYzMSYBg	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Pfx0RwqBli	M3LBsF0e15Cl9Mxppapcx	1.58983E+12	Amazon S3 Bucket Permissions	Security
7.77789E+11	Yw2K9puPzl	47DEQpj8HBSa-_TImW-5J	1.58983E+12	IAM Password Policy	Security
7.77789E+11	H7IgTzjTYb	1xHQ5ovV8bS0H1Z-t7Kbib	1.58983E+12	Amazon EBS Snapshots	Fault Tolerance
7.77789E+11	wuy7G1zxql	10F6p6VAF0F-MuL6Dc-dl1	1.58983E+12	Amazon EC2 Availability Zone Balance	Fault Tolerance

仅当存在资源级别检查结果时，资源文件才包含条目。您可能不会在报告中看到检查，原因如下：

- 某些检查，例如根账户上的 MFA，没有资源，也不会显示在报告中。无资源的检查将改为显示在 summary.json 文件中。
- 有些检查仅在它们为 Red 或者 Yellow 时显示资源。如果所有资源都为 Green，则它们可能不会出现在您的报告中。
- 如果没有为需要检查的服务启用账户，则检查可能不会显示在报告中。例如，如果您的组织中没有使用 Amazon Elastic Compute Cloud 预留实例，则 Amazon EC2 Reserved Instance Lease Expiration 检查将不会显示在您的报告中。
- 账户尚未刷新检查结果。当具有基本支持计划或开发人员支持计划的用户首次登录 Trusted Advisor 控制台时可能会发生此情况。如果您拥有商业、Enterprise On-Ramp 和企业 Support 计划，则用户最长可能需要在账户注册后一周才能看到检查结果。有关更多信息，请参阅刷新 Trusted Advisor 检查 (p. 30)：
- 如果只有组织的管理账户启用了检查建议，则报告将不会包括组织中其他账户的资源。

对于资源文件，您可以使用常用软件（如 Microsoft Excel）打开 .csv 文件格式。您可以使用 .csv 文件对组织中所有账户中的所有检查进行一次性分析。如果要将报告与应用程序一起使用，则可以将报告作为 .json 文件下载。

.json 文件格式比 .csv 文件格式提供的灵活度更大，可用于高级使用案例，例如使用多个数据集的聚合和高级分析。例如，您可以将 SQL 界面与 AWS 服务（例如 Amazon Athena）结合使用以对您的报告运行查询。您还可以使用 Amazon QuickSight 创建控制面板并可视化您的数据。有关更多信息，请参阅使用其他 AWS 服务查看 Trusted Advisor 报告 (p. 40)：

禁用组织视图

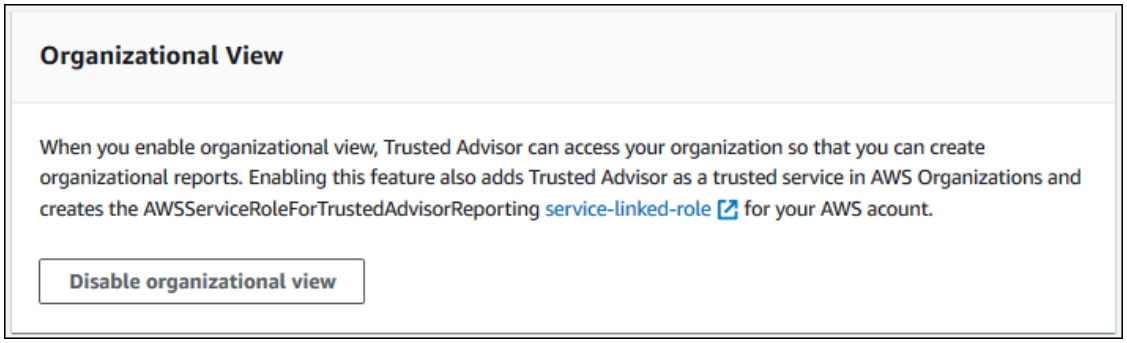
按照此程序来禁用组织视图。您必须登录组织的管理账户，或承担具有禁用此功能所需权限的角色。您无法从组织中的其他账户禁用此功能。

禁用此功能后，将出现以下情况：

- Trusted Advisor 将作为 Organizations 中的可信服务删除。
- `AWSServiceRoleForTrustedAdvisorReporting` 服务关联角色在您组织的管理账户中解锁。这意味着如果需要，您可以手动删除它。
- 您无法为组织创建、查看或下载报告。要访问以前创建的报告，您必须从 Trusted Advisor 控制台中重新启用组织视图。请参阅启用组织视图 (p. 29)。

要禁用 Trusted Advisor 的组织视图

1. 登录组织的管理账户，并打开位于 https://console.aws.amazon.com/trustedadvisor 的 AWS Trusted Advisor 控制台。
2. 在导航窗格中，选择 Preferences。
3. 在 Organizational View（组织视图）下，选择 Disable organizational view（禁用组织视图）。



禁用组织视图后，Trusted Advisor 不再聚合来自组织其他 AWS 账户中的检查。但是，`AWSServiceRoleForTrustedAdvisorReporting` 服务相关角色保留在组织的管理账户上，直到您通过 IAM 控制台、IAM API 或 AWS Command Line Interface (AWS CLI) 将其删除为止。有关更多信息，请参阅 IAM 用户指南中的删除服务相关角色。

> **Note**
>
> 您可以使用其他 AWS 服务查询和可视化组织视图报告的数据。有关更多信息，请参阅以下资源：
>
> - AWS 管理和治理博客中的使用 AWS Organizations 大规模查看 AWS Trusted Advisor 建议
> - 使用其他 AWS 服务查看 Trusted Advisor 报告 (p. 40)

使用 IAM 策略允许访问组织视图

您可以使用以下 AWS Identity and Access Management (IAM) 策略，允许您账户中的用户或角色访问 AWS Trusted Advisor 中的组织视图。

Example ：对组织视图的完全访问权限

以下策略允许完全访问组织视图功能。具备这些权限的用户可以执行以下操作：

- 启用和禁用组织视图

- 创建、查看和下载报告

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:DescribeServiceMetadata",
                "trustedadvisor:DescribeOrganizationAccounts",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateReportStatement",
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:GenerateReport"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ManageOrganizationalViewStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess",
                "trustedadvisor:SetOrganizationAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateServiceLinkedRoleStatement",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting"
        }
    ]
}
```

Example ：对组织视图的读取访问权限

以下策略允许对 Trusted Advisor 的组织视图进行只读访问。具有这些权限的用户只能查看和下载现有报告。

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

```
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
}
```

您还可以创建自己的 IAM 策略。有关更多信息，请参阅 IAM 用户指南 中的创建 IAM 策略。

Note

如果您在账户中启用了 AWS CloudTrail，您的日志条目中可能会显示以下角色：

- `AWSServiceRoleForTrustedAdvisorReporting` –Trusted Advisor 用于访问您组织中的账户的服务关联角色。
- `AWSServiceRoleForTrustedAdvisor` –Trusted Advisor 用于访问您组织中的服务的服务关联角色。

有关服务相关角色的更多信息，请参阅 将服务相关角色用于 Trusted Advisor (p. 199)。

使用其他 AWS 服务查看 Trusted Advisor 报告

遵照本教程通过使用其他 AWS 服务上载和查看您的数据。在本主题中，您将创建 Amazon Simple Storage Service (Amazon S3) 存储桶以存储报告，并创建一个 AWS CloudFormation 模板来在您的账户中创建资源。然后，您可以使用 Amazon Athena 分析或运行针对您的报告的查询，也可以使用 Amazon QuickSight 在控制面板中可视化该数据。

有关可视化报告数据的信息和示例，请参阅 AWS 管理和治理博客中的使用 AWS Organizations 大规模查看 AWS Trusted Advisor 建议

先决条件

开始本教程之前，您必须满足以下要求：

- 以具有管理员权限的 AWS Identity and Access Management (IAM) 用户身份登录。
- 使用美国东部（弗吉尼亚北部）AWS 区域快速设置您的 AWS 服务和资源。
- 创建一个亚马逊 QuickSight 账户。有关更多信息，请参阅《亚马逊 QuickSight 用户指南》中的 “亚马逊 QuickSight数据分析入门”。

将报告上载到 Amazon S3

在您下载 `resources.json` 报告后，将文件上载到 Amazon S3。您必须在美国东部（弗吉尼亚北部）区域中使用存储桶。

要将报告上载到 Amazon S3 存储桶

1. 在 AWS Management Consolehttps://console.aws.amazon.com/ 登录。
2. 使用区域选择器，然后选择美国东部（弗吉尼亚北部）区域。
3. 通过以下网址打开 Simple Storage Service（Amazon S3）控制台：https://console.aws.amazon.com/s3/。
4. 从存储桶列表中，选择 S3 存储桶，然后复制名称。您可以在下一程序中使用该名称。
5. 在 *bucket-name* 页面上，选择 Create folder（创建文件夹），输入名称 **folder1**，然后选择 Save（保存）。
6. 选择 folder1。
7. 在 folder1 中，选择 Upload（上载），然后选择 `resources.json` 文件。
8. 选择 Next（下一步），保留默认选项，然后选择 Upload（上载）。

   Note

   如果您将新报告上载到此存储桶，请在每次上载 `.json` 文件时对其进行重命名，这样就不会覆盖现有报告。例如，您可以将时间戳添加到每个文件，例如 `resources-timestamp.json`、`resources-timestamp2.json`，依此类推。

使用 AWS CloudFormation 创建资源

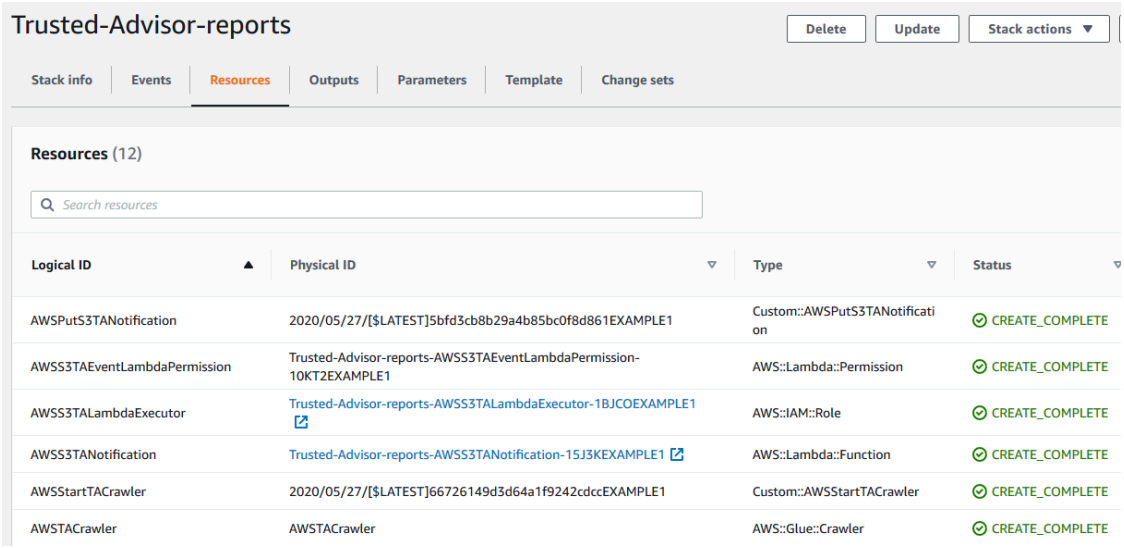
将报告上载到 Amazon S3 后，请将以下 YAML 模板上载到 AWS CloudFormation。此模板将告知 AWS CloudFormation 要为您的账户创建哪些资源，以便其他服务可以使用 S3 存储桶中的报告数据。该模板为 IAM 创建资源 AWS Lambda 和 AWS Glue。

要使用 AWS CloudFormation 创建资源

1. 下载 trusted-advisor-reports-template.zip 文件。
2. 解压缩该文件。
3. 在文本编辑器中打开模板文件。
4. 对于 `BucketName` 和 `FolderName` 参数，请将 *your-bucket-name-here* 和 *folder1* 的值替换为您的账户中的存储桶名称和文件夹名称。
5. 保存该文件。
6. 打开 AWS CloudFormation 控制台，地址：https://console.aws.amazon.com/cloudformation。
7. 如果您尚未设置，请在区域选择器中，选择美国东部（弗吉尼亚北部）区域。
8. 在导航窗格中，选择 Stacks (堆栈)。
9. 选择 Create stack（创建堆栈），然后选择 With new resources (standard)（使用新资源 (标准)）。
10. 在 Create stack（创建堆栈）页面上的 Specify template（指定模板）下，选择 Upload a template file（上载模板文件），然后选择 Choose file（选择文件）。
11. 选择 YAML 文件，然后选择 Next（下一步）。
12. 在 Specify stack details（指定堆栈详细信息）页面上，输入堆栈名称，如 **Organizational-view-Trusted-Advisor-reports**，然后选择 Next（下一步）。
13. 在 Configure stack options（配置堆栈选项）页面上，保留默认设置，然后选择 Next（下一步）。
14. 在审核 **Organizational-view-Trusted-Advisor-reports** 页面上，审核您的选项。在页面底部，选中 I acknowledge that AWS CloudFormation might create IAM resources（我确认 AWS CloudFormation 可能会创建 IAM 资源）的复选框。

15. 选择 Create stack（创建堆栈）。

    创建堆栈约需 5 分钟时间。
16. 堆栈创建成功后，Resources（资源）选项卡的显示类似于以下示例。



查询 Amazon Athena 中的数据

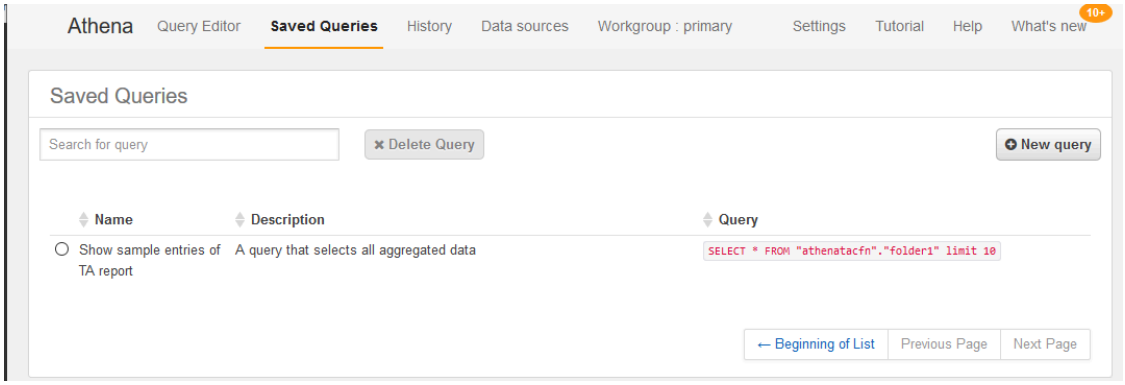
拥有资源后，您可以在 Athena 中查看数据。使用 Athena 创建查询并分析报告的结果，例如查找组织中的账户的特定检查结果。

注意

- 使用美国东部（弗吉尼亚北部）区域。
- 如果您是 Athena 的新手，则必须先指定查询结果位置，然后才能为报告运行查询。我们建议您为此位置指定不同的 S3 存储桶。有关更多信息，请参阅 Amazon Athena 用户指南中的指定查询结果位置。

要在 Athena 中查询数据

1. 从 https://console.aws.amazon.com/athena/ 打开 Athena 控制台。
2. 如果您尚未设置，请在区域选择器中，选择美国东部（弗吉尼亚北部）区域。
3. 选择 Saved Queries（保存的查询）并在搜索字段中，输入 **`Show sample`**。
4. 选择显示的查询，例如 Show sample entries of TA report（显示 TA 报告的示例条目）。



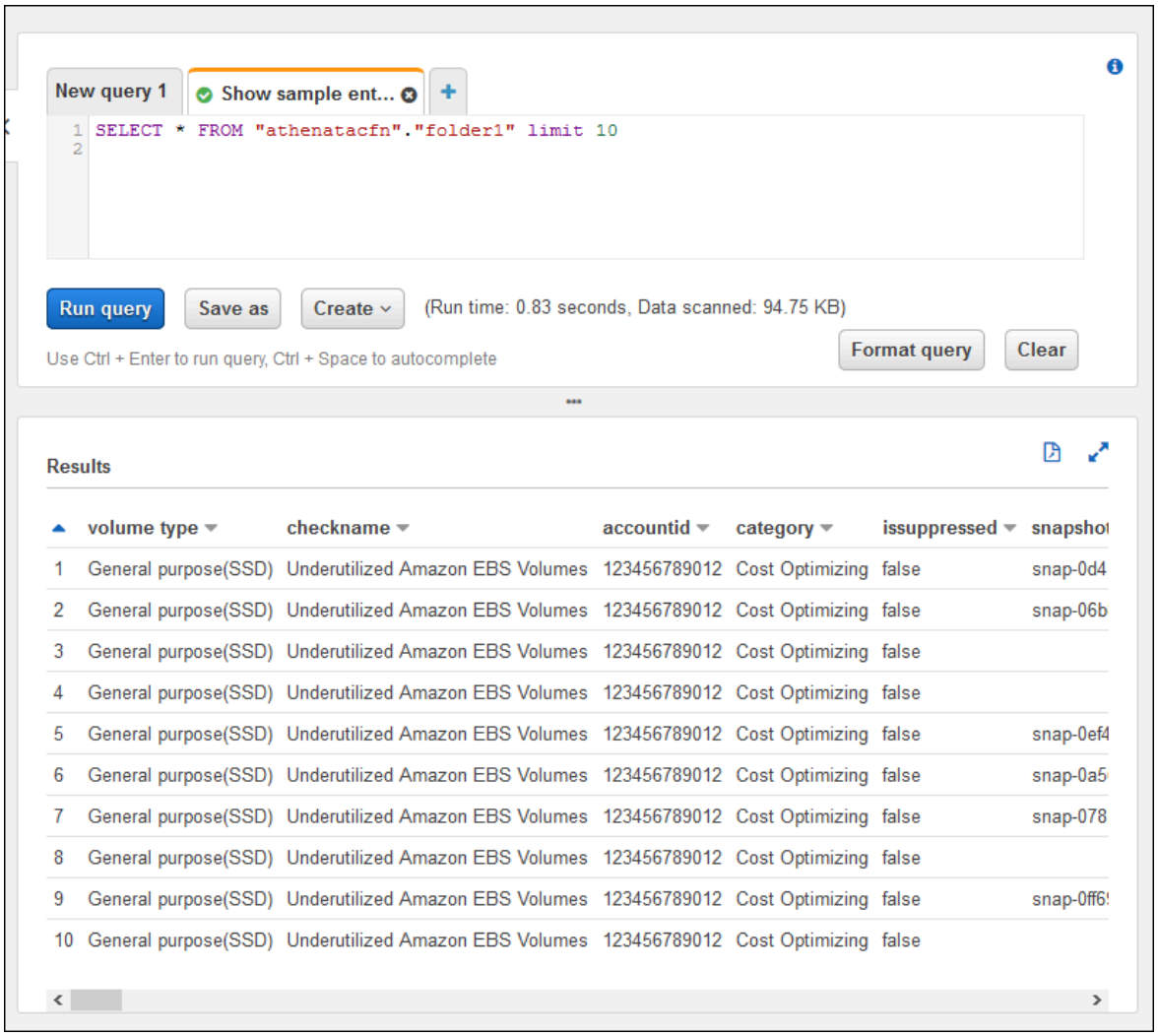
查询应与以下内容类似。

```
SELECT * FROM "athenatacfn"."folder1" limit 10
```

5. 选择 Run query (运行查询)。您的查询结果显示出来。

Example ：Athena 查询

以下示例显示报告中的 10 个示例条目。



有关更多信息，请参阅 Amazon Athena 用户指南中的使用 Amazon Athena 运行 SQL 查询。

在 Amazon 中创建控制面板 QuickSight

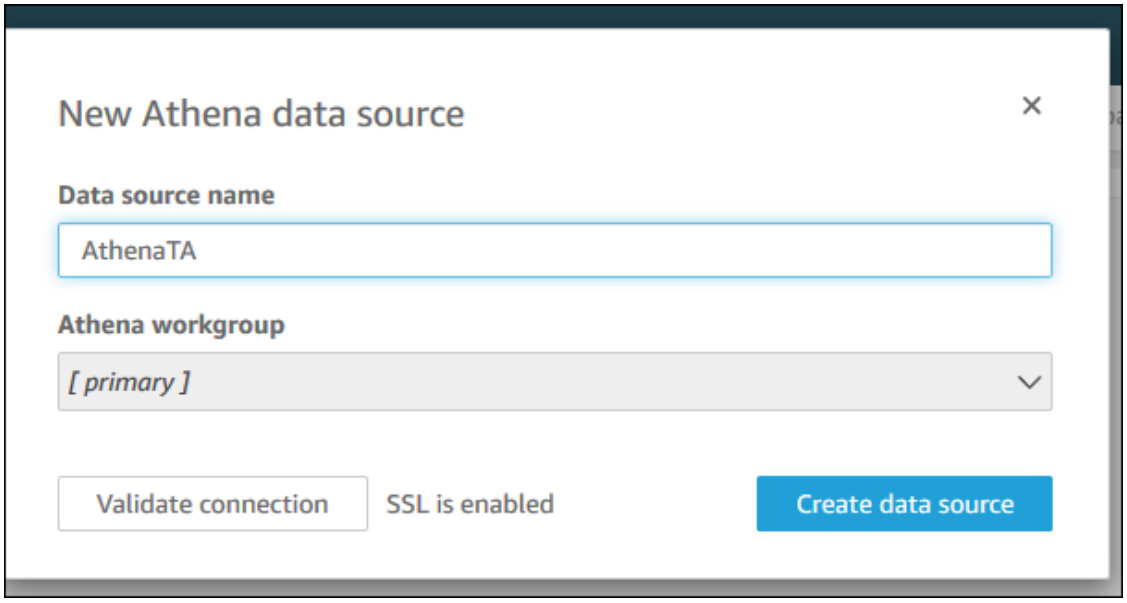
您还可以设置 Amazon， QuickSight 以便在控制面板中查看数据并可视化报告信息。

Note

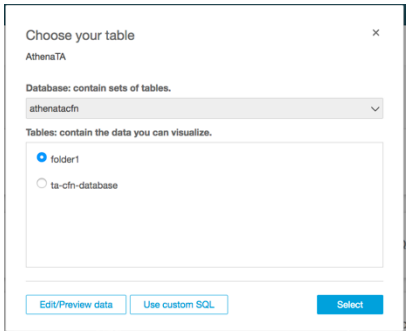
您必须使用美国东部（弗吉尼亚北部）区域。

要在 Amazon 中创建控制面板 QuickSight

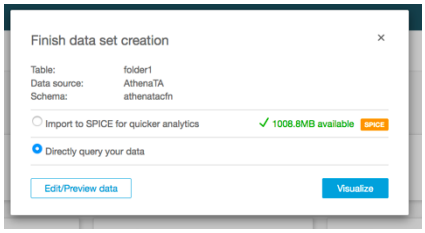
1. 导航到 Amazon QuickSight 控制台并登录您的账户。
2. 选择 New analysis（新的分析）、New dataset（新数据集），然后选择 Athena。
3. 在 New Athena data source（新 Athena 数据源）对话框中，输入数据源名称，例如 AthenaTA，然后选择 Create data source（创建数据源）。



4. 在 Choose your table（选择表）对话框中，选择 athenatacfn 表中，选择 folder1，然后选择 Select（选择）。



5. 在 Finish data set creation（完成数据集创建）对话框中，选择 Directly query your data（直接查询您的数据），然后选择 Visualize（可视化）。

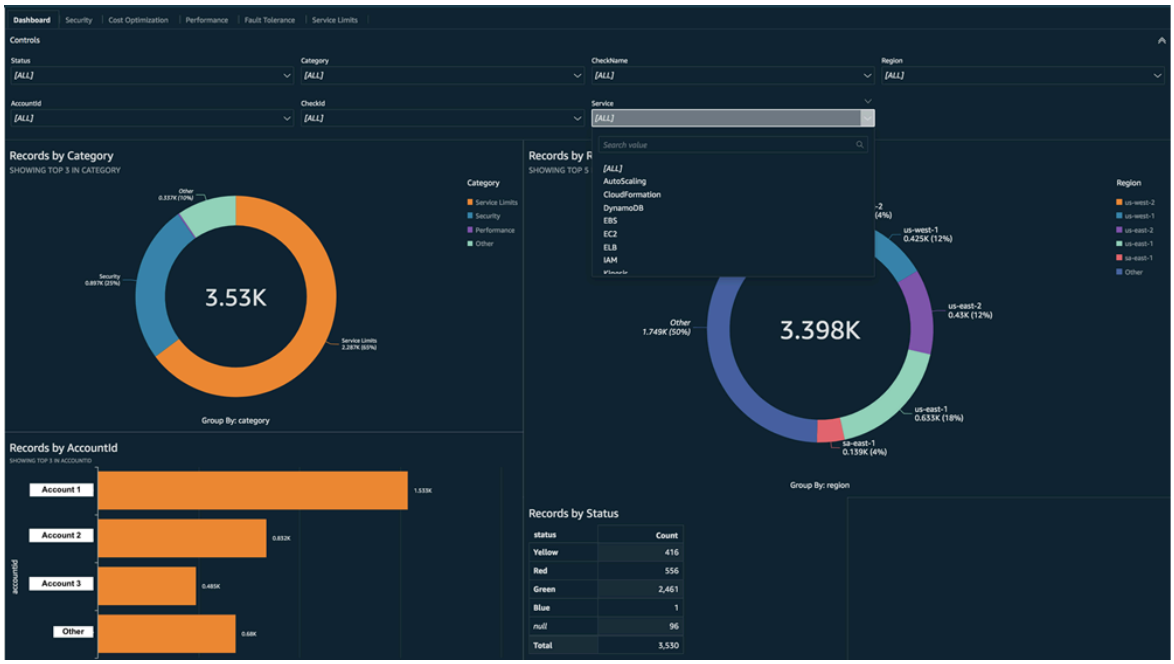


现在，您可以在 Amazon 中创建控制面板 QuickSight。有关更多信息，请参阅《亚马逊 QuickSight 用户指南》中的 “使用控制面板”。

Example : 亚马逊 QuickSight 控制面板

以下示例控制面板显示有关 Trusted Advisor 检查的信息，例如以下内容：

- 受影响的账户 ID
- 按 AWS 区域划分的摘要
- 检查类别
- 检查状态
- 每个账户的报告中的条目数



Note

如果您在创建控制面板时出现权限错误，请确保Amazon QuickSight 可以使用 Athena。有关更多信息，请参阅 Amazon QuickSight 用户指南中的无法Connect 到 Amazon A thena。

有关可视化报告数据的更多信息和示例，请参阅 AWS管理与治理博客中的使用 AWS Organizations 大规模查看 AWS Trusted Advisor 建议。

问题排查

如果您在本教程中遇到问题，请参阅以下故障排除提示。

我没有在我的报告中看到最新数据

创建报告时，组织视图功能不会自动刷新您的组织中的 Trusted Advisor 检查。要获取最新的检查结果，请刷新组织中的管理账户和每个成员账户的检查。有关更多信息，请参阅刷新 Trusted Advisor 检查 (p. 30)：

我的报告中有重复的列

如果您的报告具有重复的列，Athena 控制台可能会在您的表中显示以下错误。

```
HIVE_INVALID_METADATA: Hive metadata for table folder1 is invalid: Table
descriptor contains duplicate columns
```

例如，如果您在报告中添加了已存在的列，则当您尝试在 Athena 控制台中查看报告数据时，这可能会导致问题。您可以按照以下步骤来修复此问题。

查找重复的列

您可以使用 AWS Glue 控制台查看 schema 并快速识别您的报告中是否有重复的列。

要查找重复列

1. 打开 AWS Glue 控制台，地址：https://console.aws.amazon.com/glue/。
2. 如果您尚未设置，请在区域选择器中，选择美国东部（弗吉尼亚北部）区域。
3. 在导航窗格中，选择表。
4. 选择您的文件夹名称，例如 ***folder1***，然后在 Schema 下，查看 Column name（列名称）的值。

   如果您有重复的列，则必须将新报告上载到您的 Amazon S3 存储桶。参阅以下 上载新报告 (p. 46) 部分。

上载新报告

在识别重复列之后，我们建议您使用新报告替换现有报告。这可确保从本教程创建的资源使用组织中的最新报告数据。

要上载新报告

1. 如果您尚未设置，请为组织中的账户刷新您的 Trusted Advisor 检查。请参阅刷新 Trusted Advisor 检查 (p. 30)。
2. 在 Trusted Advisor 控制台中创建并下载另一个 JSON 报告。请参阅创建组织视图报告 (p. 30)。本教程中，您必须使用 JSON 文件。
3. 登录到AWS Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
4. 选择 Amazon S3 存储桶，然后选择 *folder1* 文件夹。
5. 选择上一个 *resources*.json 报告并选择 Delete（删除）。
6. 在 Delete objects（删除对象）页面中的 Permanently delete objects?（永久删除对象？）下输入 **permanently delete**，然后选择 Delete objects（删除对象）。
7. 在 S3 存储桶中，选择 Upload（上载），然后指定新报告。此操作会自动更新您的 Athena 表格和包含最新报告数据的 AWS Glue 爬网程序资源。刷新您的资源可能需要几分钟时间。
8. 在 Athena 控制台中输入新查询。请参阅查询 Amazon Athena 中的数据 (p. 42)。

   Note

   如果您对本教程仍有问题，您可以在 AWS Support 中心创建技术支持案例。

在 AWS Trusted Advisor 中查看 AWS Security Hub 控件

在您的AWS 账户中启用AWS Security Hub之后，您可以在 Trusted Advisor 控制台中查看您的安全控件及其检查结果。您可以按照与使用 Trusted Advisor 检查相同的方式，使用 Security Hub 控件来识别账户中的安全漏洞。您可以查看检查的状态、受影响资源的列表，然后按照 Security Hub 的建议来解决安全问题。借助此功能，您可以一站式获得来自 Trusted Advisor 和 Security Hub 的安全建议。

注意

- 您可以通过 Trusted Advisor 查看所有 AWS 基础安全最佳实践安全标准中的控件，但 Category: Recover > Resilience（类别：恢复 > 弹性）的控件除外。有关受支持控件的列表，请参阅《AWS Security Hub 用户指南》中的 AWS基础安全最佳实践控件。

  有关 Security Hub 类别的更多信息，请参阅控件类别。
- 目前，当 Security Hub 向 AWS 基础安全最佳实践安全标准添加新的控件时，可能需要等待两到四周后才能在 Trusted Advisor 中查看这些控件。此时间范围是尽力而为，不能保证。

主题

- 先决条件 (p. 47)
- 查看 Security Hub 检查结果 (p. 47)
- 刷新 Security Hub 检查结果 (p. 48)
- 从 Trusted Advisor 禁用 Security Hub (p. 49)
- 问题排查 (p. 49)

先决条件

您必须满足以下要求才能启用 Security Hub 与 Trusted Advisor 的集成：

- 您必须拥有商业、Enterprise On-Ramp 或企业 Support 计划才能使用此功能。您可以从 AWS Support 中心或从 Support plans（支持计划）页面中查找您的支持计划。有关更多信息，请参阅比较 AWS Support 计划。
- 您必须在您需要使用 Security Hub 控件的 AWS 区域 的 AWS Config 中启用资源记录。有关更多信息，请参阅启用和配置 AWS Config。
- 您必须启用 Security Hub 并选择 AWS Foundational Security Best Practices v1.0.0（基础安全最佳实践 v1.0.0）安全标准。如果您尚未执行此操作，请参阅《AWS Security Hub 用户指南》中的设置 AWS Security Hub。

Note

如果您已经满足了这些先决条件，则可以跳到 查看 Security Hub 检查结果 (p. 47)。

关于 AWS Organizations 账户

如果您已经满足管理账户的先决条件，则系统会自动为组织中的所有成员账户启用此集成。会员账户无需单独联系 AWS Support 以启用此功能。但组织中的成员账户必须启用 Security Hub 后才能在 Trusted Advisor 查看器检查结果。

如果要为特定的成员账户禁用此集成，请参阅为 AWS Organizations 账户禁用此功能 (p. 49)。

查看 Security Hub 检查结果

为您的账户启用 Security Hub 后，最长需要 24 个小时才会在 Trusted Advisor 控制台的 Security（安全）页面显示 Security Hub 检查结果。

在 Trusted Advisor 查看 Security Hub 检查结果

1. 导航到 Trusted Advisor 控制台，然后选择 Security（安全）类别。

2. 在 Search by keyword（按关键词搜索）字段中，输入控件的名称或描述。

   Tip

   对于 Source（源），您可以选择 AWS Security Hub 以筛选 Security Hub 控件。

3. 选择 Security Hub 控件名称以查看以下信息：

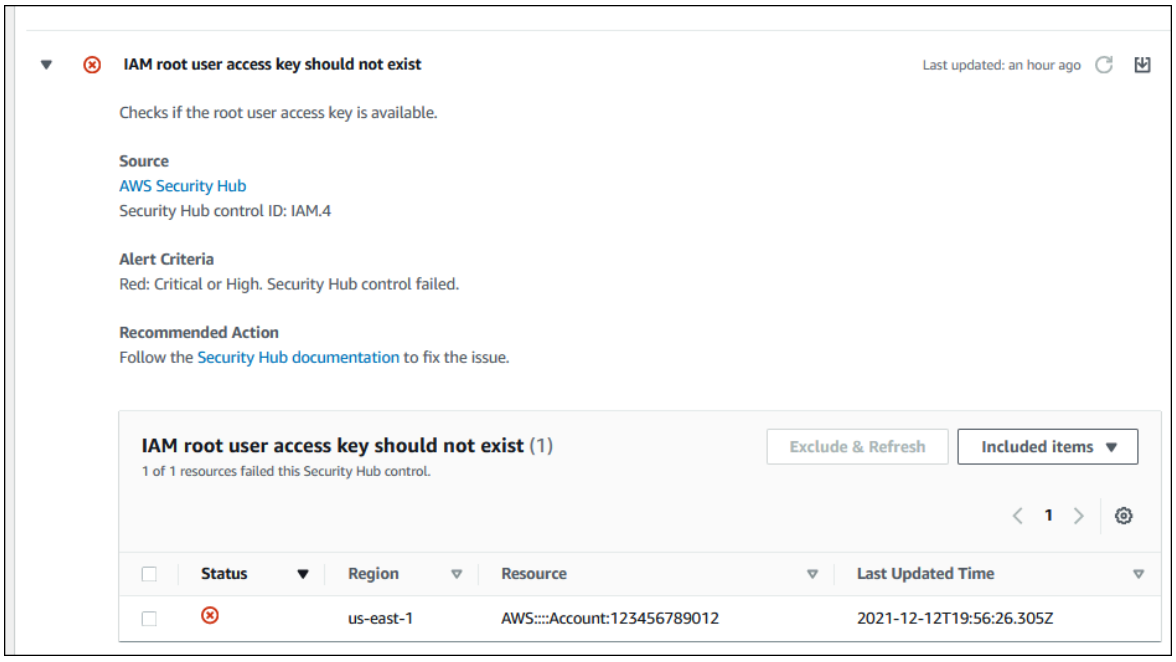
   - Description（描述）– 描述此控件将如何检查您的账户是否存在安全漏洞。
   - Source（源）– 检查是来自 AWS Trusted Advisor 还是 AWS Security Hub。对于 Security Hub 控件，您可以找到控件 ID。
   - Alert Criteria（提示标准）– 控件的状态。例如，假设 Security Hub 检测到重要问题，则状态可能为 Red: Critical or High（红色：严重或高）。
   - Recommended Action（建议的操作）– 使用 Security Hub 文档链接查找修复问题的建议步骤。
   - Security Hub resources（Security Hub 资源）– 您可以查找 Security Hub 在您账户中检测到问题的资源。

   注意

   - 您必须使用 Security Hub 才能将资源从检查结果中排除。目前不支持使用 Trusted Advisor 控制台从 Security Hub 控件中排除项目。有关更多信息，请参阅 设置检查结果的工作流状态。
   - 组织视图功能支持与 Security Hub 集成。您可以查看整个组织的 Security Hub 控件检查结果，然后创建和下载报告。有关更多信息，请参阅 AWS Trusted Advisor 的组织视图 (p. 29)。

Example 例如：IAM 用户访问密钥的 Security Hub 控件不应存在

以下是 Trusted Advisor 控制台中的 Security Hub 控件检查结果示例。



刷新 Security Hub 检查结果

启用某个安全标准后，Security Hub 最长可能需要两个小时才能获得有关您资源的检查结果。然后最长可能需要 24 小时才会在 Trusted Advisor 控制台中显示该数据。如果您最近启用了 AWS Foundational Security Best Practices v1.0.0（基础安全最佳实践 v1.0.0）安全标准，请稍后再重新检查 Trusted Advisor 控制台。

Note

- 每个 Security Hub 控件的刷新计划可以是定期触发，也可以是在发生更改时触发。目前，您无法使用 Trusted Advisor 控制台或 AWS Support API 来刷新 Security Hub 控件。有关更多信息，请参阅运行安全检查的计划。
- 如果想要将资源从检查结果中排除，您必须使用 Security Hub。目前不支持使用 Trusted Advisor 控制台从 Security Hub 控件中排除项目。有关更多信息，请参阅 设置检查结果的工作流状态。

从 Trusted Advisor 禁用 Security Hub

如果您不希望在 Trusted Advisor 控制台中显示 Security Hub 信息，则执行以下步骤。此操作步骤仅禁用 Security Hub 与 Trusted Advisor 的集成，不会影响您的 Security Hub 配置。您可以继续使用 Security Hub 控制台查看安全控件、资源和建议。

禁用 Security Hub 集成

1. 联系 AWS Support 并请求禁用 Security Hub 与 Trusted Advisor 的集成。

   AWS Support 禁用此功能后，Security Hub 不再将数据发送到 Trusted Advisor。您的 Security Hub 数据将从 Trusted Advisor 中删除。
2. 要重新启用此集成，请联系 AWS Support。

为 AWS Organizations 账户禁用此功能

如果您已经为管理账户完成了前述步骤，则系统会自动从组织中的所有成员账户中删除 Security Hub 集成。组织中的具体成员账户无需单独联系 AWS Support。

如果您是某个组织的成员账户，则可以联系 AWS Support 以便仅为您的账户中删除此功能。

问题排查

如果您遇到与此集成有关的问题，请参阅以下问题排查信息。

目录

- 我没有在 Trusted Advisor 控制台中看到看到 Security Hub 检查结果 (p. 49)
- 我正确配置了 Security Hub 和 AWS Config，但仍没有看到结果 (p. 50)
- 我想禁用特定的 Security Hub 控件 (p. 50)
- 我想查找已被排除的 Security Hub 资源 (p. 50)
- 我想为属于某个 AWS 组织的成员账户启用或禁用此功能 (p. 50)
- 我看到针对 Security Hub 检查的相同受影响资源有多个 AWS 区域 (p. 50)
- 我关闭了 Security Hub 或 AWS Config 在一个区域 (p. 51)
- 我的控件已归档在 Security Hub 中，但 Trusted Advisor 中仍显示检查结果。 (p. 51)
- 我仍然无法查看我的 Security Hub 检查结果 (p. 51)

我没有在 Trusted Advisor 控制台中看到看到 Security Hub 检查结果

确认您是否已完成以下步骤：

- 您拥有商业、Enterprise On-Ramp 或企业 Support 计划。

- 您已在与 Security Hub 相同的区域的 AWS Config 中启用了资源录制。
- 您已启用了 Security Hub 并选择了 AWS Foundational Security Best Practices v1.0.0（ 基础安全最佳实践 v1.0.0）安全标准。
- 来自 Security Hub 的新控件将在两到四周内添加为 Trusted Advisor 中的检查。请参阅说明 (p. 47)。

有关更多信息，请参阅 先决条件 (p. 47)。

我正确配置了 Security Hub 和 AWS Config，但仍没有看到结果

Security Hub 最长可能需要两个小时才能获得有关您资源的检查结果。然后最长可能需要 24 小时才会在 Trusted Advisor 控制台中显示该数据。请稍后重新检查 Trusted Advisor 控制台。

注意

- 在 Trusted Advisor 中将仅显示 AWS 基础安全最佳实践安全标准中控件的检查结果，但 Category: Recover > Resilience（类别：恢复 > 弹性）的控件除外。
- 如果 Security Hub 存在服务问题或者 Security Hub 服务不可用，最长可能需要 24 小时才会在 Trusted Advisor 中显示您的检查结果。请稍后重新检查 Trusted Advisor 控制台。

我想禁用特定的 Security Hub 控件

Security Hub 会自动将数据发送到 Trusted Advisor。如果您禁用了某个 Security Hub 控件或者不再拥有该控件的资源，则将不会在 Trusted Advisor 中显示检查结果。

您可以登录到 Security Hub 控制台并确认控件已启用还是已禁用。

如果您禁用 Security Hub 控件或禁用 AWS 基础安全最佳实践安全标准的所有控件，您的结果将在接下来的五天内归档。这五天的归档期仅为近似值且仅尽力而为，并不能保证。当您的结果归档后，它们将从 Trusted Advisor 中删除。

有关更多信息，请参阅以下主题：

- 禁用和启用各个控件
- 禁用或启用安全标准

我想查找已被排除的 Security Hub 资源

您可以在 Trusted Advisor 控制台中选中 Security Hub 控件的名称，然后选择 Excluded items（排除的项目）选项。此选项将会显示 Security Hub 中隐藏的所有资源。

如果某个资源的工作流状态设置为 SUPPRESSED，则该资源就是在 Trusted Advisor 中被排除的项目。您不能通过 Trusted Advisor 控制台隐藏 Security Hub 资源。要隐藏资源，您需要使用 Security Hub 控制台。有关更多信息，请参阅 设置检查结果的工作流状态。

我想为属于某个 AWS 组织的成员账户启用或禁用此功能

预设情况下，成员账户会从 AWS Organizations 的管理账户继承此功能。如果管理账户启用了此功能，则该组织中的所有账户也将具有此功能。如果您拥有的是成员账户并希望对您的账户进行特定的更改，则必须联系 AWS Support。

我看到针对 Security Hub 检查的相同受影响资源有多个 AWS 区域

AWS 服务有些是全球性的，并非特定于某个区域，例如 IAM 和 Amazon CloudFront。默认情况下，Amazon S3 存储桶之类的全球资源将出现在美国东部（弗吉尼亚州北部）区域中。

针对用于评估全球服务资源的 Security Hub 检查，您可能会看到受影响资源的多个项目。例如，如果 `Hardware MFA should be enabled for the root user` 检查发现您的账户尚未激活此功能，则您将在表中看到对于同一资源有多个区域。

您可以配置 Security Hub 和 AWS Config，以便不会为同一资源显示多个区域。有关更多信息，请参阅您可能希望禁用的 AWS 基础最佳实践控件。

我关闭了 Security Hub 或 AWS Config 在一个区域

如果您使用 AWS Config 停止资源记录或者在 AWS 区域中禁用 Security Hub，Trusted Advisor 不再接收该区域中任何控件的数据。Trusted Advisor 会在 7 至 9 天内删除您的 Security Hub 检查结果。此时间范围是尽力而为，不能保证。有关更多信息，请参阅禁用 Security Hub。

要为您的账户禁用此功能，请参阅 从 Trusted Advisor 禁用 Security Hub (p. 49)。

我的控件已归档在 Security Hub 中，但 Trusted Advisor 中仍显示检查结果。

当检查结果的 `RecordState` 状态更改为 `ARCHIVED` 时，Trusted Advisor 将从您的账户中删除该 Security Hub 控件的检查结果。检查结果可能仍会在 Trusted Advisor 中显示，最多需要 7-9 天才会被删除。此时间范围是尽力而为，不能保证。

我仍然无法查看我的 Security Hub 检查结果

如果您仍然遇到与此功能有关的问题，可以在 AWS Support 中心创建技术支持案例。

启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查

Compute Optimizer 服务可以分析 AWS 资源的配置和利用率指标。此服务会报告从效率和可靠性的角度看，您的资源是否已正确配置。它还会提供有关如何实施改进以提高工作负载性能的建议。借助 Compute Optimizer，您可以查看 Trusted Advisor 检查中的相同建议。

您可以仅为您的 AWS 账户启用此服务，也可以为属于 AWS Organizations 中组织一部分的所有成员账户启用。有关更多信息，请参阅《AWS Compute Optimizer 用户指南》中的入门。

启用 Compute Optimizer 后，以下检查将接收来自您的 Lambda 函数和 Amazon EBS 卷的数据。系统最长可能需要在 12 小时后才会生成检查结果和优化建议。而要在 Trusted Advisor 中查看下列检查的结果，您最长可能需要再等待 48 小时：

成本优化 (p. 66)

- Amazon EBS 过度预调配卷
- 相比内存大小过度预调配的 AWS Lambda 函数

性能 (p. 83)

- Amazon EBS 预调配不足的卷
- 相比内存大小而言预调配不足的 AWS Lambda 函数

注意

- 这些检查的结果会每天自动刷新几次。不允许刷新请求。更改可能需要几个小时才能显示。您目前无法从这些检查中排除资源。

- Trusted Advisor 已经有利用率不足 Amazon EBS 卷和利用率过高 Amazon EBS 磁性卷检查。

  如果您启用了 Compute Optimizer，我们建议您使用新的 Amazon EBS 过度预调配卷和 Amazon EBS 预调配不足卷检查。

相关信息

有关更多信息，请参阅以下主题：

- 《AWS Compute Optimizer 用户指南》中的查看 Amazon EBS 卷建议
- 《AWS Compute Optimizer 用户指南》中的查看 Lambda 函数建议
- 《AWS Lambda 用户指南》中的配置 Lambda 函数内存
- 《适用于 Linux 实例的 Amazon EC2 用户指南》中的请求对 Amazon EBS 卷进行修改

AWS Trusted Advisor Priority 入门

Trusted Advisor Priority 可帮助您保护和优化 AWS 账户，以遵循 AWS 最佳实践。借助 Trusted Advisor Priority，您的 AWS 账户 团队可以主动监控您的账户，并在发现适合您的机会时创建优先建议。

例如，您的客户团队可以识别您的根账户是否缺少多重身份验证（MFA）。您的客户团队可以创建一条建议，以使您能够立即采取措施进行检查，例如 `MFA on Root Account`。该建议在 Trusted Advisor 控制台的 Trusted Advisor Priority 页面显示为活动的优先建议。然后您可以按照建议解决。

Trusted Advisor Priority 建议可以来自以下两个来源之一：

- AWS 服务 – 服务(Trusted Advisor、AWS Security Hub 和 AWS Well-Architected）会自动创建建议。您的客户团队会与您分享这些建议，以便它们显示在 Trusted Advisor Priority 中。
- 您的客户团队 – 您的客户团队可以手动创建建议。

Trusted Advisor Priority 可帮助您专注于最重要的建议。从您的客户团队分享建议开始，直到您确认、解决或忽略此建议，您和您的客户团队可以监控整个建议生命周期。您可以使用 Trusted Advisor Priority 为您的组织中的所有成员账户查找建议。

主题

- 先决条件 (p. 53)
- 启用 Trusted Advisor Priority (p. 53)
- 查看优先建议 (p. 53)
- 确认建议 (p. 54)
- 忽略建议 (p. 55)
- 解决建议 (p. 56)
- 重新打开建议 (p. 56)
- 下载建议详细信息 (p. 57)
- 注册委派管理员 (p. 57)
- 注销委派管理员 (p. 58)
- 管理 Trusted Advisor Priority 通知 (p. 58)
- 禁用 Trusted Advisor Priority (p. 59)

先决条件

要使用 PTrusted Advisor riority，您必须采取必要的措施来满足以下要求：

- 您必须拥有企业级控制Support 块。
- 您的账户必须是中所有功能已启用中的所有功能的组织的一部分AWS Organizations。有关更多信息，请参阅 AWS Organizations 用户指南中的启用组织中的所有功能。
- 您的组织必须已启用的可信访问权Trusted Advisor。您可以通过以管理帐户身份登录并在Trusted Advisor控制台中转到您的组织 (p. 24)页面来启用可信访问。
- 您必须登录到组织的管理账户或委托管理员账户。有关注册委托管理员账户的说明，请参阅注册委派管理员 (p. 57)。
- 您必须具有 AWS Identity and Access Management（IAM）权限才能访问 Trusted Advisor Priority。有关如何控制对 Trusted Advisor Priority 的访问的信息，请参阅 管理对 AWS Trusted Advisor 的访问 (p. 226) 和 AWS适用于 AWS Trusted Advisor 的托管策略 (p. 213)。

启用 Trusted Advisor Priority

请联系您的客户团队并让他们为您启用此功能。您必须拥有企业支持计划并成为组织的管理账户所有者。如果控制台中的 Trusted Advisor Priority 页面显示您需要 AWS Organizations 的可信访问权限，则您可以选择启用 AWS Organizations 的可信访问权限。有关更多信息，请参阅之前的 先决条件 (p. 53) 部分。

查看优先建议

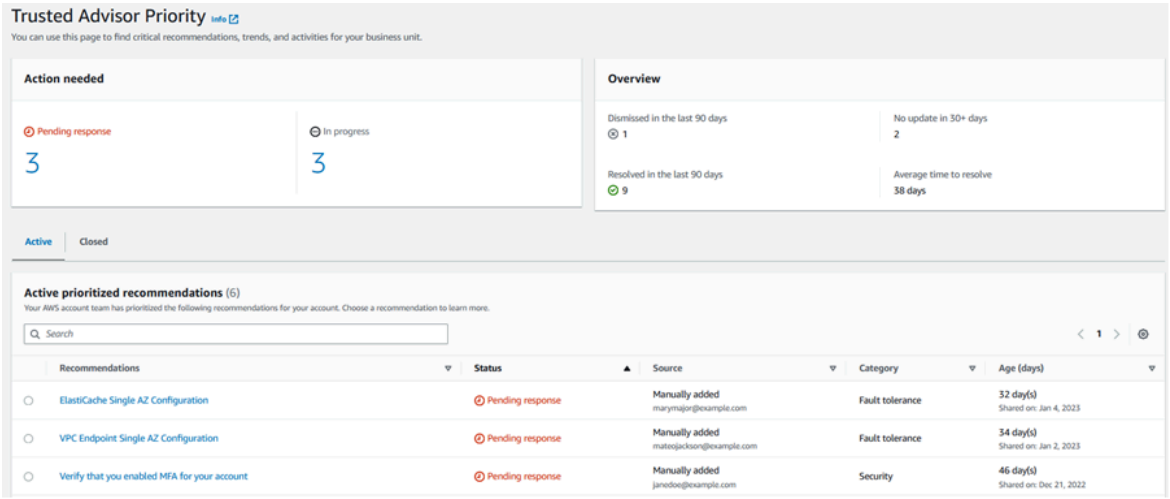
在您的客户团队为您启用 Trusted Advisor Priority 后，您可以查看贵组织的最新建议。

查看优先建议

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在 Trusted Advisor Priority 页面上，您可以查看以下内容：
   - 所需操作 – 正在等待响应或正在处理的建议的数量。
   - Overview（概述）– 以下信息：
     - 过去 90 天内被忽略的建议
     - 过去 90 天内已解决的建议
     - 超过 30 天没有更新的建议
     - 解决建议的平均时间
3. 在 Active（活动）选项卡下，Active prioritized recommendations（活动优先建议）显示您的客户团队为您优先考虑的建议。已关闭选项卡显示已解决或已忽略的建议。
   - 要筛选您的结果，请使用以下选项：
     - Recommendation（建议）– 输入关键字以按名称进行搜索。关键字可以是检查名称，也可以是客户团队创建的自定义名称。
     - 状态 – 建议正在等待响应、正在进行、已被忽略还是已解决。
     - Source（来源）– 优先建议的源。建议可能来自 AWS 服务、您的 AWS 账户 团队或计划的服务事件。
     - Category（类别）– 建议类别，例如安全或成本优化。
     - Age（期限）– 当您的客户团队与您分享建议时。
4. 请选择建议以详细了解其详细信息、受其影响的资源和账户以及应采取的建议操作。然后，您可以确认 (p. 54)或忽略 (p. 55)相应的建议。

Example ：Trusted Advisor Priority 建议

以下示例显示了三条正在等待响应的建议以及需要操作部分下正在进行的三条建议。下图显示了活动优先建议选项卡中正在等待响应的其中三条建议。



确认建议

在活动选项卡下，您可以了解有关相应建议的更多信息，然后再决定是否要确认。

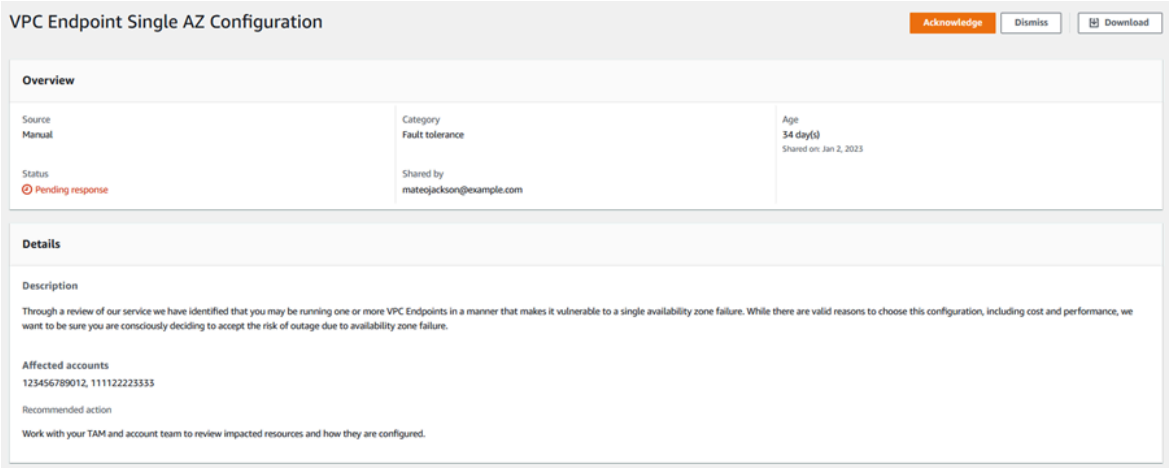
确认建议的方法

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在 Trusted Advisor Priority 页面中的 Active（活动）选项卡下，选择一个建议名称。
3. 在详细信息部分，您可以查看有关建议的以下信息：
   - 您组织中账户的受影响资源
   - 相关支持案例的链接
   - 建议完成的操作
4. 选择确认。
5. 在确认建议对话框中，选择确认。

   建议状态将变为 In progress（正在进行）。正在处理的或正在等待响应的建议显示在 Trusted Advisor Priority 页面的 Active（活动）选项卡中。
6. 按照建议的操作解决建议。有关更多信息，请参阅解决建议 (p. 56)：

Example ：来自 Trusted Advisor Priority 的手动建议

下图显示了正在等待响应的 VPC 端点单可用区配置建议。



忽略建议

您还可以忽略建议。也就是说，您会确认建议，但不会处理该建议。如果建议与您的账户无关，您可以忽略该建议。例如，如果您有计划删除的测试 AWS 账户，则无需执行建议的操作。

忽略建议的方法

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在 Trusted Advisor Priority 页面中的 Active（活动）选项卡下，选择一个建议名称。
3. 在建议详细信息页面上，查看有关组织内受影响的资源和账户的信息。
4. 如果此建议不适用于您的账户，请选择忽略。
5. 在忽略建议对话框中，选择您不处理该建议的原因。
6. （可选）输入备注，说明您忽略相关建议的原因。如果您选择其他，则必须在备注部分输入说明。
7. 选择忽略。建议状态将变为已忽略并出现在 Trusted Advisor Priority 页面的已关闭选项卡中。

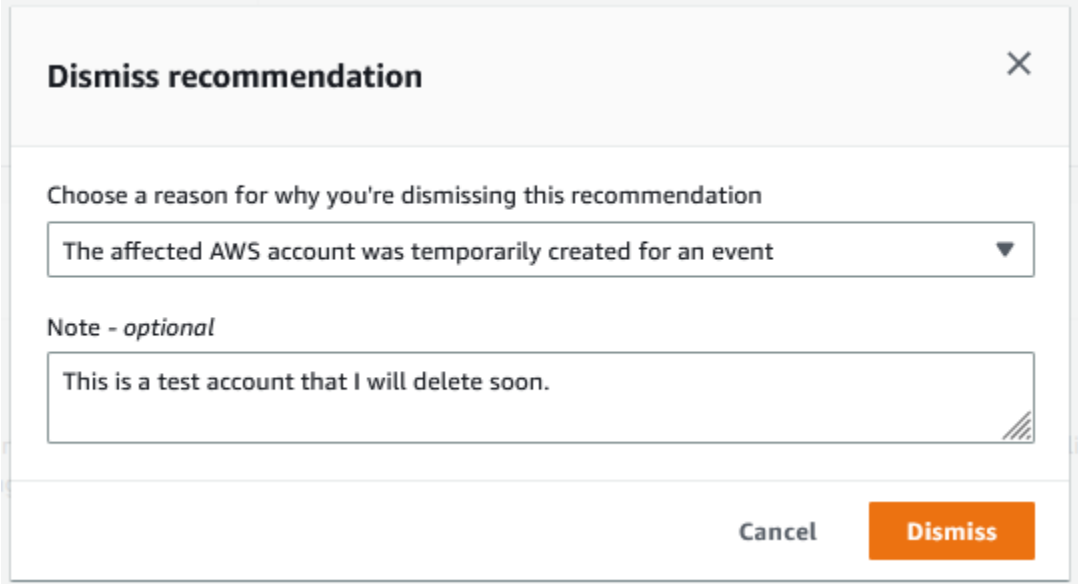
   Tip

   您可以选择建议名称，然后选择查看备注找出忽略的原因。如果您的客户团队为您忽略了建议，则他们的电子邮件地址将显示在备注旁。

   Trusted Advisor Priority 还会通知您的客户团队您已忽略建议。

Example ：忽略来自 Trusted Advisor Priority 的建议

以下示例说明了如何忽略建议。



解决建议

确认建议并完成建议的操作后，您可以解决该建议。

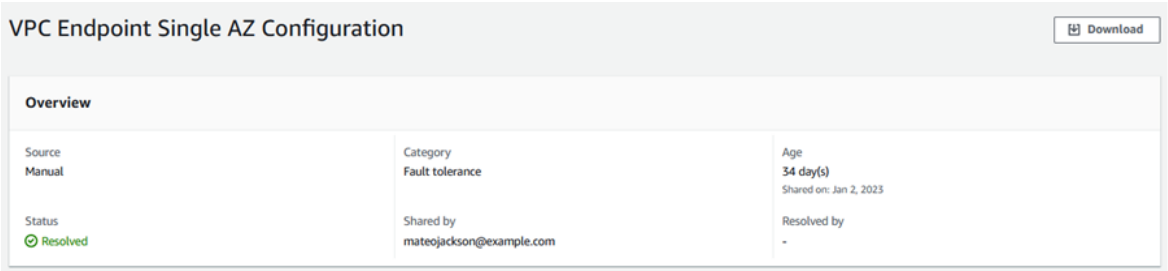
> Tip
>
> 解决建议后，您将无法重新打开该建议。如果您想稍后再次查看该建议，请参阅“忽略建议 (p. 55)”。

解决建议

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在 Trusted Advisor Priority 页面上，选择建议，然后选择 Resolve（解决）。
3. 在解决建议对话框中，选择解决。已解决的建议显示在 Trusted Advisor Priority 页面中的 Closed（已关闭）选项卡下。Trusted AdvisorPriority 会通知您的客户团队您已解决该建议。

Example ：来自 Trusted Advisor Priority 的手动建议

以下示例显示了已解决的 VPC 端点单可用区配置建议。



重新打开建议

您忽略建议后，您或您的客户团队可以重新打开该建议。

重新打开建议

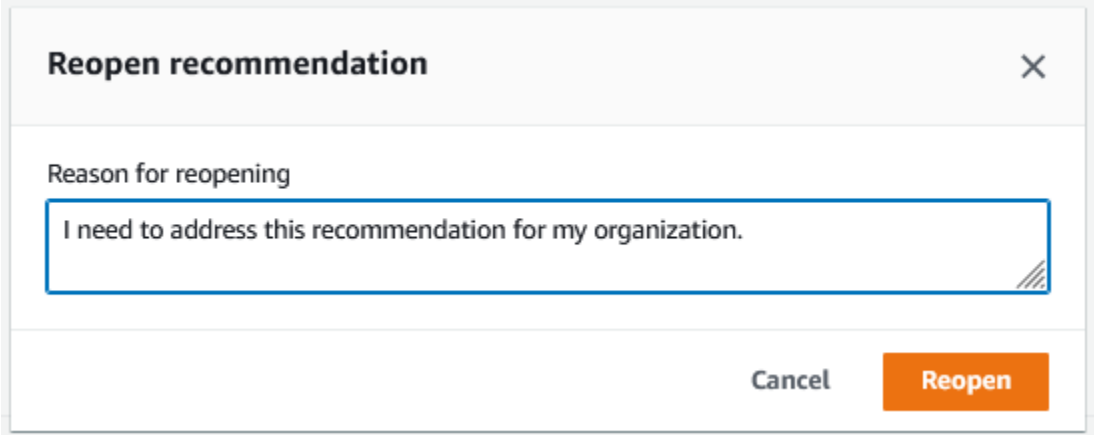
1. 在 Trusted Advisor Priority 页面，选择 Closed（已关闭）选项卡。
2. 在关闭的建议下，选择已忽略的建议，然后选择重新打开。
3. 在重新打开建议对话框中，说明重新打开建议的原因。
4. 选择 Reopen（重新打开）。建议状态将变为 In progress（正在进行）并出现在 Active（活动）选项卡下。

   Tip

   您可以选择建议名称，然后选择查看备注找出重新打开的原因。如果您的客户团队为您重新打开了建议，他们的名字会出现在备注旁。
5. 按照建议详细信息中的步骤操作。

Example ：从 Trusted Advisor Priority 中重新打开建议

以下示例显示了您想要重新打开的建议。



下载建议详细信息

您也可以从 Trusted Advisor Priority 下载优先建议的结果。

Note

目前，您一次只能下载一个建议。

下载建议

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在 Trusted Advisor Priority 页面上，选择建议，然后选择 Download（下载）。
3. 打开文件查看建议详细信息。

注册委派管理员

您可以将属于您组织的成员账户添加为委派管理员。委派管理员账户可以在 Trusted Advisor Priority 中查看、确认、解决、忽略和重新打开建议。

注册账户后，您必须授予委派管理员访问 Trusted Advisor Priority 所需的 IAM 权限。有关更多信息，请参阅 管理对 AWS Trusted Advisor 的访问 (p. 226) 和 AWS适用于 AWS Trusted Advisor 的托管策略 (p. 213)。

您最多可以注册五个成员账户。只有管理账户才能为组织添加委派管理员。

注册委派管理员

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在导航窗格中的 Preferences（首选项）下，选择 Your organization（您的组织）。
3. 在 Delegated administrator（委派管理员）下，选择 Register new account（注册新账户）。
4. 在对话框中，输入成员账户 ID，然后选择 Register（注册）。
5. （可选）要注销账户，请选择一个账户并选择 Deregister（注销）。在此对话框中，再次选择 Deregister（注销）。

注销委派管理员

在您注销成员账户后，该账户将不再具有和管理账户相同的 Trusted Advisor Priority 访问权限。已不再是委派管理员身份的账户将不会收到来自 Trusted Advisor Priority 的电子邮件通知。

注销委派管理员

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在导航窗格中的 Preferences（首选项）下，选择 Your organization（您的组织）。
3. 在 Delegated administrators（委派管理员）下，选择账户，然后选择 Deregister（注销）。
4. 在此对话框中，选择 Deregister（注销）。

管理 Trusted Advisor Priority 通知

Trusted Advisor Priority 通过电子邮件发送通知。此电子邮件通知包括您的客户团队为您优先考虑的建议的摘要。您可以指定从 Trusted Advisor Priority 接收更新的频率。

如果您将成员账户注册为委派管理员，成员账户的使用者也可以将账户设置为接收 Trusted Advisor Priority 电子邮件通知。

Trusted Advisor Priority 电子邮件通知不包括单个账户的检查结果，与 Trusted Advisor 建议的每周通知是相互独立的。有关更多信息，请参阅设置通知首选项 (p. 25)：

管理您的 Trusted Advisor Priority 通知

1. 登录到位于 https://console.aws.amazon.com/trustedadvisor/home 的 Trusted Advisor 控制台。
2. 在导航窗格中的 Preferences（首选项）下，选择 Notifications（通知）。
3. 在 Priority 下，您可以选择以下选项。
   a. Daily（每天）– 每天接收一封电子邮件通知。
   b. Weekly（每周）– 每周接收一封电子邮件通知。
   c. 选择要接收的通知：
      - 优先建议摘要
      - 解决日期
4. 在 Recipients（收件人）选项中，选择其他联系人以接收电子邮件通知。您可以从 AWS Billing and Cost Management 控制台的 Account Settings（账户设置）页面中添加和删除联系人。
5. 在 Language（语言）选项中，选择电子邮件通知使用的语言。
6. 选择 Save your preferences（保存首选项）。

Note

Trusted Advisor Priority 使用 noreply@notifications.trustedadvisor.us-west-2.amazonaws.com 地址发送电子邮件通知。您可能需要确认您的电子邮件客户端有没有将这些电子邮件识别为垃圾邮件。

禁用 Trusted Advisor Priority

请联系您的客户团队并让他们为您禁用此功能。您的 Trusted Advisor 控制台将不再显示优先建议。

如果禁用 Trusted Advisor Priority，然后稍后再次启用它，您仍然可以查看客户团队在您禁用 Trusted Advisor Priority 之前发送的建议。

开始使用 EngAWS Trusted Advisor age（预览版）

Note

AWS Trusted AdvisorEngaum 为预览版，可能会发生变化。你可以在这里查看预览服务条款 https://aws.amazon.com/service-terms/。

您可以使用 Engage 轻松查看、请求和跟踪所有主动AWS Trusted Advisor参与活动，并与AWS 账户团队就持续的互动进行沟通，从而最大限度地利用您的AWS Support计划。

例如，您可以进入AWS Trusted Advisor控制台中的 Eng ag e 页面，向您的AWS 账户团队申请 “管理业务审查”。然后，将指派AWS专家处理您的请求，并跟踪整个项目。

主题

- 先决条件 (p. 59)
- 控制面板 (p. 60)
- 查看互动类型目录 (p. 60)
- 申请订婚 (p. 61)
- 提交附件和备注 (p. 62)
- 更改参与状态 (p. 63)
- 区分推荐的项目和要求的项目 (p. 64)
- 搜索参与度 (p. 64)

先决条件

要使用 EngTrusted Advisor age，您必须采取必要的措施来满足以下要求：

- 您必须具有企业级控制Support 板。
- 您的账户必须是中的所有功能的组织的一部分AWS Organizations。有关更多信息，请参阅 AWS Organizations 用户指南中的启用组织中的所有功能。
- 您的组织必须已启用Trusted Advisor。您可以通过以管理帐户身份登录并在Trusted Advisor控制台中转到您的组织 (p. 24)页面来启用可信访问。
- 您必须登录到组织的管理账户或委托管理员账户。有关注册委托管理员账户的说明，请参阅注册委派管理员 (p. 57)。
- 您必须具有AWS Identity and Access Management（IAM）权限才能访问 EtockTrusted Advisor um。有关如何控制 EngTrusted Advisor age 访问权限的信息，请参阅管理对 AWS Trusted Advisor 的访问 (p. 226)。

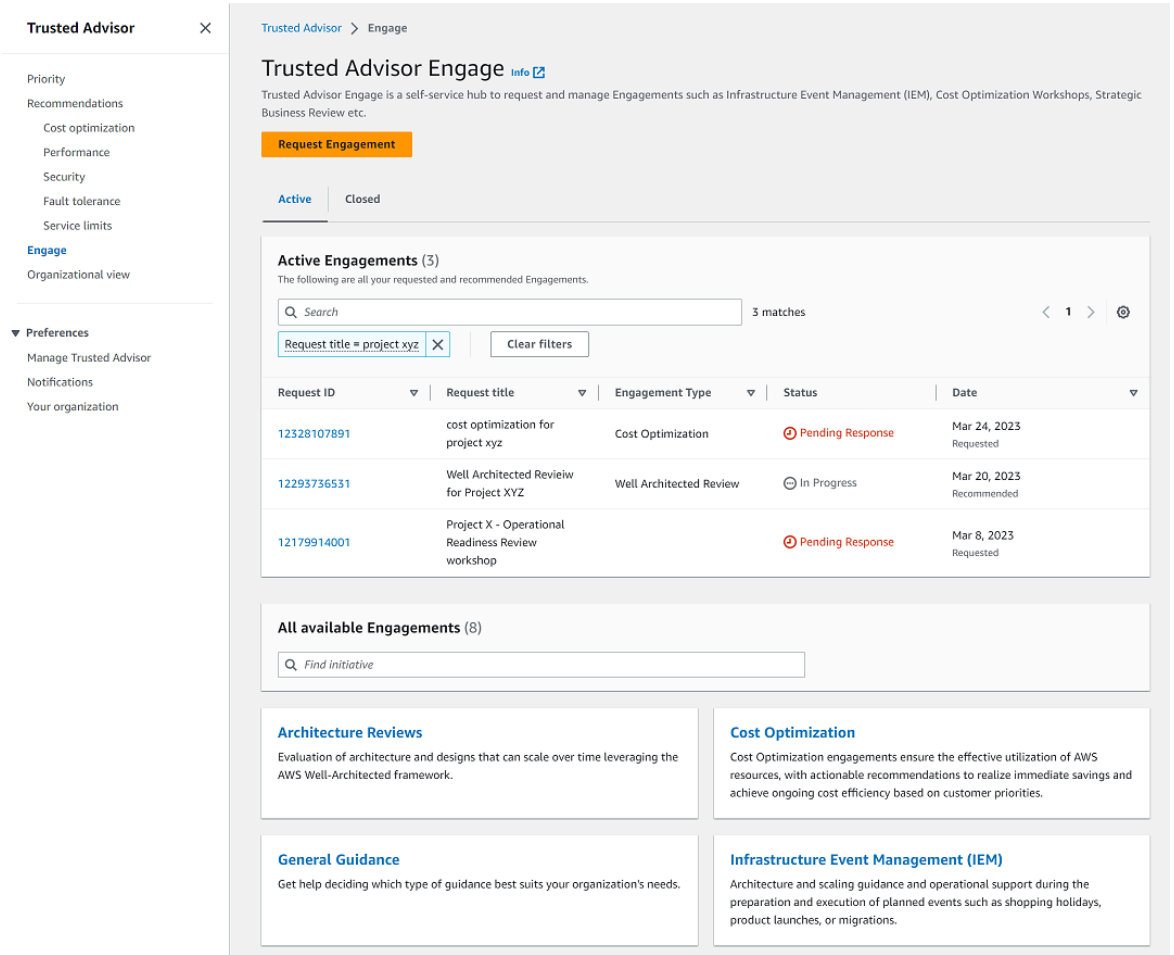
控制面板

获得访问权限后，您可以访问控制台中的 EngTrusted Advisor age 页面以查看Trusted Advisor控制面板，在其中可以管理与AWS 账户团队的互动。

要管理您的互动，请执行以下操作：

1. 通过 https://console.aws.amazon.com/trustedadvisor/home 登录主Trusted Advisor机。
2. 在 En Trusted Advisorg age 页面上，您可以查看：
   - 申请参与按钮
   - 活跃参与度表
   - 封闭参与度表
   - 所有可用的项目目录

Example：控制面板



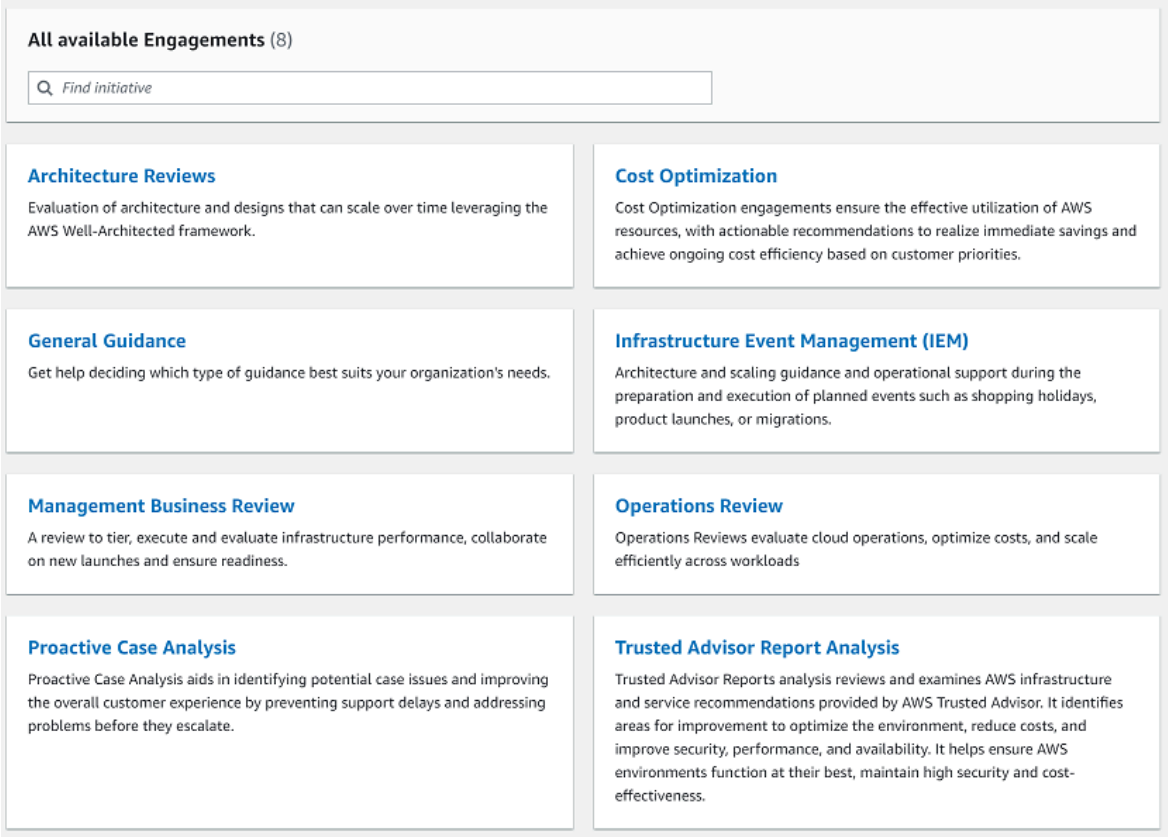
查看互动类型目录

您可以查看互动类型目录，以查找可以向AWS 账户团队请求的最新参与类型。

要查看互动类型目录，请执行以下操作：

1. 通过 https://console.aws.amazon.com/trustedadvisor/home 登录主Trusted Advisor机。
2. 在Trusted Advisor互动页面上，您可以找到互动类型的目录。

Example：参与类型目录



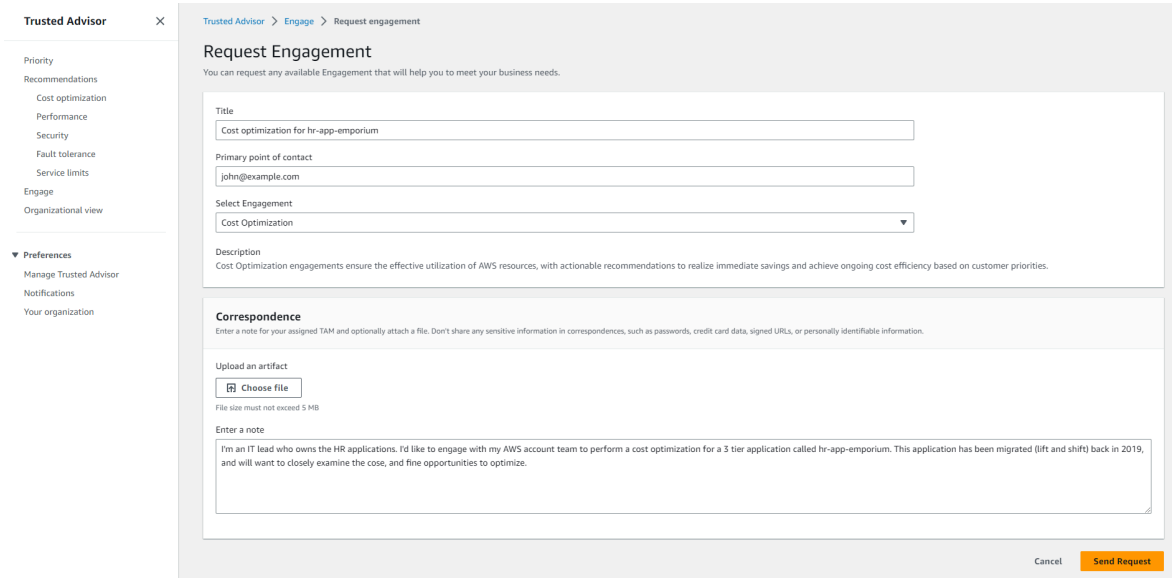
申请订婚

您可以根据Support 计划中包含的参与类型向您的AWS 账户AWS团队请求互动。

要申请参与，请执行以下操作：

1. 通过 https://console.aws.amazon.com/trustedadvisor/home 登录主Trusted Advisor机。
2. 在 “Trusted Advisor参与” 页面上，选择 “请求互动”。
3. 以下字段
   - 职务
   - 主要联系人：AWS将用作本次项目主要合同点的电子邮件地址。
   - 选择参与度：您要请求的参与类型。
   - 信函：一份备注和一份可选文件附件，供您提供有关本次活动的详细信息。
4. 选择 “发送请求”。

Example：申请参与



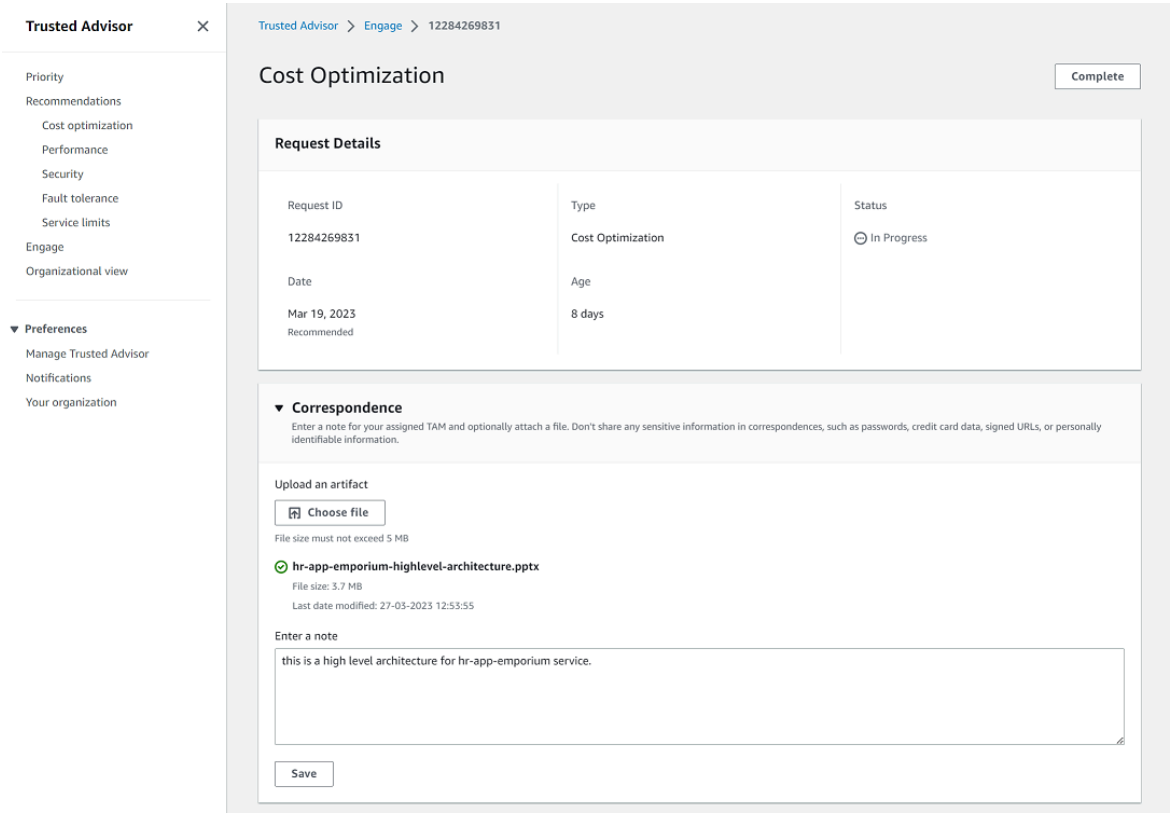
提交附件和备注

您可以通过发送备注和文件附件来支持您的参与请求，就个人活动与您的AWS 账户团队进行沟通。您可以为每封通信添加单个附件和备注，只能将文件附加到与请求参与的项目相同的AWS 账户项目，并且在发送通信后无法删除附件或备注。

要在 “活跃互动” 请求中附加文件或添加备注，请执行以下操作：

1. 通过 https://console.aws.amazon.com/trustedadvisor/home 登录主Trusted Advisor机。
2. 在 E Trusted Advisorn gage 页面上，选择您要向其附加文件或添加备注的活跃互动的 ID。
3. 选择 “信函” 以展开表单。
4. 为分配的 TAM 输入备注，并可选择附加文件。不要在通信中分享任何敏感信息，例如密码、信用卡数据、签名网址或个人身份信息。
5. 选择保存。

Example : 向项目添加备注和附加文件



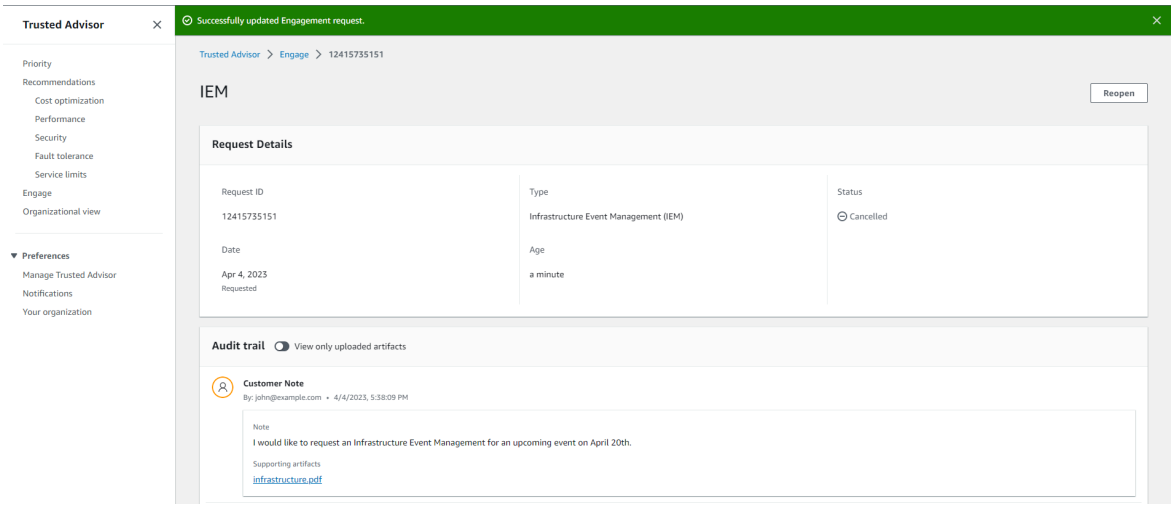
更改参与状态

您可以将互动状态更改为取消待回复的互动、完成正在进行的互动以及重新打开已标记为已取消或已关闭的互动。

要订到组织的状态：

1. 通过 https://console.aws.amazon.com/trustedadvisor/home 登录主Trusted Advisor机。
2. 在 E Trusted Advisorn gage 页面上，选择您想要更改其状态的活跃互动的 ID。
3. 在互动详情页面上，您可以将状态更改为 “已取消” 或 “完成”。
   - 当互动状态为 “待回复” 时，您可以选择 “取消”。
   - 当项目状态为 “进行中” 时，您可以选择 “完成”。
   - 您可以为已关闭的活动选择 “重新打开”。取消的互动移至 “待回复”，而 “已完成” 互动移至 “进行中”。

Example：更改参与状态



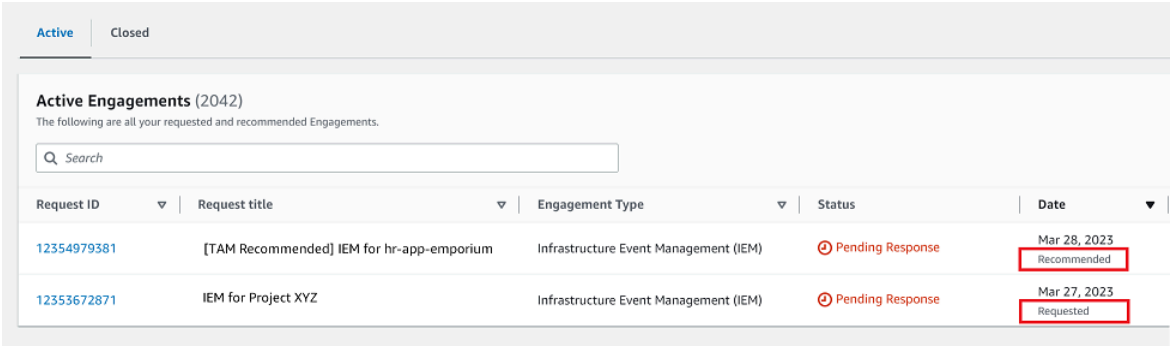
区分推荐的项目和要求的项目

您可以确定互动来源，以了解某项活动是由您请求还是由您的AWS 账户团队推荐。

要查看不同的活跃参与度来源，请执行以下操作：

1. 通过 https://console.aws.amazon.com/trustedadvisor/home 登录主Trusted Advisor机。
2. 在 Eng Trusted Advisorag e 页面上，查看 “日期” 列以区分 “推荐的活动” 和 “请求的活动”：
   - 推荐：由您的AWS 账户团队创建的互动请求。
   - 已请求：用户创建的参与请求。

Example：区分推荐的项目和要求的项目



搜索参与度

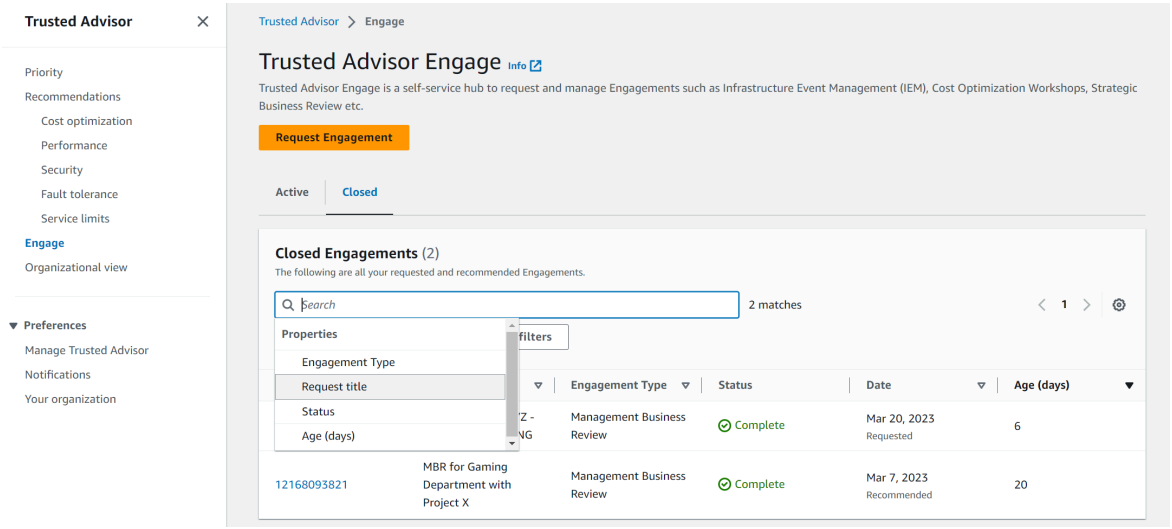
您可以使用筛选条件搜索现有的活跃和已结束的活动。

要搜索参与度，请执行以下操作：

1. 通过 https://console.aws.amazon.com/trustedadvisor/home 登录主Trusted Advisor机。
2. 在 En Trusted Advisorgag e 页面上，您可以从以下过滤器中进行选择：

- 年龄（天）
- 参与类型
- 请求标题
- 状态

Example：搜索参与度



AWS Trusted Advisor 检查引用

您可以在以下引用中查看所有 Trusted Advisor 检查名称、说明和 ID。您也可以登录 Trusted Advisor 控制台查看有关检查、建议操作及其状态的更多信息。

如果您拥有商业、Enterprise On-Ramp 或企业 Support 计划，则还可以使用 AWS Support API 和 AWS Command Line Interface（AWS CLI）访问您的检查。有关更多信息，请参阅以下主题：

- 使用 Trusted Advisor 即 Web 服务 (p. 25)
- AWS CLI 命令参考中的可用 AWS Support 命令

> **Note**
>
> 如果您使用的是基本支持或开发人员支持计划，则可以使用 Trusted Advisor 控制台访问 Service Limits (p. 132) 类别中的所有检查和安全类别中的以下检查：
>
> - Amazon EBS 公有快照 (p. 95)
> - Amazon RDS 公有快照 (p. 96)
> - Amazon S3 存储桶权限 (p. 97)
> - IAM 使用 (p. 105)
> - 根账户的 MFA (p. 106)
> - 安全组 – 不受限制的特定端口 (p. 106)

检查类别

- 成本优化 (p. 66)

- 性能 (p. 83)
- 安全性 (p. 93)
- 容错能力 (p. 108)
- Service Limits (p. 132)

成本优化

您可以使用以下成本优化类别检查。

检查名称

- Amazon Comprehend 未充分利用的端点 (p. 66)
- Amazon EBS 过度预调配卷 (p. 67)
- 适用于 Microsoft SQL Server 的 Amazon EC2 实例整合 (p. 68)
- 使用 Microsoft SQL Server 的 Amazon EC2 实例超限预置 (p. 68)
- Amazon EC2 Reserved Instance Lease Expiration (p. 69)
- Amazon EC2 预留实例优化 (p. 70)
- Amaz ElastiCache on 节点优化 (p. 71)
- Amazon Serv OpenSearch ice 预留 (p. 72)
- Amazon RDS 闲置数据库实例 (p. 72)
- Amazon Redshift 预留节点优化 (p. 73)
- Amazon Relational Database Service (RDS) 预留实例优化 (p. 74)
- Amazon Route 53 延迟资源记录集 (p. 75)
- 过度超时的 AWS Lambda 函数 (p. 75)
- 具有高误差率的 AWS Lambda 函数 (p. 76)
- 相比内存大小过度预调配的 AWS Lambda 函数 (p. 77)
- AWS Well-Architected 成本优化高风险问题 (p. 78)
- 闲置的负载均衡器 (p. 79)
- 低使用率 Amazon EC2 实例 (p. 79)
- Savings Plan (p. 80)
- 未关联的弹性 IP 地址 (p. 81)
- 未充分利用的 Amazon EBS 卷 (p. 81)
- Underutilized Amazon Redshift Clusters (p. 82)

Amazon Comprehend 未充分利用的端点

描述

检查端点的吞吐量配置。当端点未被主动用于实时推理请求时，此检查会提示您。端点未连续使用超过 15 天则会被认为未充分利用。所有端点均根据设置的吞吐量以及端点处于活动状态的时长来累积费用。

Note

此检查每天自动刷新一次。当前，您无法从此检查中排除资源。

检查 ID

```
Cm24dfsM12
```

提醒条件

黄色：端点处于活跃状态，但在过去 15 天内未用于实时推理请求。

Recommended Action（建议的操作）

如果端点在过去 15 天内尚未使用，我们建议使用应用程序 Autoscaling 为资源定义扩缩策略。

如果端点已定义扩缩策略并且在过去 30 天内尚未使用，请考虑删除此终端节点并使用异步推理。有关更多信息，请参阅使用 Amazon Comprehend 删除端点。

报告列

- 状态
- 区域
- 端点 ARN
- 预置推理单元
- AutoScaling 状态
- Reason
- 上次更新时间

Amazon EBS 过度预调配卷

描述

检查在回顾期内任何时刻运行过的 Amazon Elastic Block Store（Amazon EBS）卷。如果有任何 EBS 卷相比您的工作负载而言预调配过度，则该检查会提醒您。如果您有过度预调配的卷，则需要为未使用的资源付费。尽管有些场景可能会导致在设计优化不足的问题，但通常可以通过更改 EBS 卷的配置来降低成本。预估每月节省基于 EBS 卷的当前使用率。如果该卷整月都不存在，则实际节省将会有异。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

```
COr6dfpM03
```

提醒条件

黄色：回顾期间预置过高的 EBS 卷。为了确定卷是否预置过高，我们会考虑所有默认 CloudWatch 指标（包括 IOPS 和吞吐量）。用于识别预置过高的 EBS 卷的算法遵循 AWS 最佳实践。识别新模式后，算法会更新。

Recommended Action（建议的操作）

考虑缩小使用率较低的卷。

有关更多信息，请参阅启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查 (p. 51)：

报告列

- 状态
- 区域
- 卷 ID
- 卷类型
- 卷大小（GB）
- 卷基准 IOPS
- 卷爆增 IOPS
- 卷爆增吞吐量
- 推荐的卷类型
- 推荐的卷大小（GB）
- 推荐的卷基准 IOPS

- 推荐的卷爆增 IOPS
- 推荐的卷基准吞吐量
- 推荐的卷爆增吞吐量
- 回顾期（天）
- 节省机会（%）
- 预估每月节省
- 预估每月节省货币
- 上次更新时间

适用于 Microsoft SQL Server 的 Amazon EC2 实例整合

描述

检查过去 24 小时内运行 SQL Server 的 Amazon Elastic Compute Cloud（Amazon EC2）实例。如果实例的 SQL Server 许可证数量少于最低数量，则此检查会提示您。根据《Microsoft SQL Server 许可指南》，即使实例只有 1 个或 2 个 vCPU，也要支付 4 个 vCPU 许可证。您可以整合较小的 SQL Server 实例以帮助降低成本。

> Note
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`Qsdfp3A4L2`

提醒条件

黄色：使用 SQL Server 的实例少于 4 个 vCPU。

Recommended Action（建议的操作）

考虑将较小的 SQL Server 工作负载整合到至少具有 4 个 vCPU 的实例。

其他资源

- AWS 上的 Microsoft SQL Server
- AWS 上的 Microsoft 许可
- Microsoft SQL Server 许可指南

报告列

- 状态
- 区域
- 实例 ID
- 实例类型
- vCPU
- 最小 vCPU 数
- SQL Server 版本
- 上次更新时间

使用 Microsoft SQL Server 的 Amazon EC2 实例超限预置

描述

检查过去 24 小时内运行 SQL Server 的 Amazon Elastic Compute Cloud（Amazon EC2）实例。SQL Server 数据库对每个实例都有计算容量限制。使用 SQL Server Standard 版的实例最多可以使用 48 个

vCPU。使用 SQL Server Web 版的实例最多可以使用 32 个 vCPU。如果实例超过此 vCPU 限制，则此检查会提示您。

如果您的实例超限预置，则您需要支付全部费用，但并没有实现性能提升。您可以管理实例的数量和大小以帮助降低成本。

预估每月节省基于同一实例系列以及一个 SQL Server 实例可以使用的最大 vCPU 数和按需定价。如果您使用的是预留实例（RI），或者实例未全天运行，则实际节省将会不同。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`Qsdfp3A4L1`

提醒条件

- 红色：使用 SQL Server Standard 版的实例具有超过 48 个 vCPU。
- 红色：使用 SQL Server Web 版的实例具有超过 32 个 vCPU。

Recommended Action（建议的操作）

对于 SQL Server Standard 版，请考虑更改为同一实例系列中具有 48 个 vCPU 的实例。对于 SQL Server Web 版，请考虑更改为同一实例系列中具有 32 个 vCPU 的实例。如果占用大量内存，请考虑更改为内存优化的 R5 实例。有关更多信息，请参阅在 Amazon EC2 上部署 Microsoft SQL Server 的最佳实践。

其他资源

- AWS 上的 Microsoft SQL Server
- 您可以使用 Launch Wizard 简化 SQL Server 在 EC2 上的部署。

报告列

- 状态
- 区域
- 实例 ID
- 实例类型
- vCPU
- SQL Server 版本
- 最大 vCPU 数
- 推荐的实例类型
- 预估每月节省
- 上次更新时间

Amazon EC2 Reserved Instance Lease Expiration

描述

检查计划在未来 30 天内过期，或已在前 30 天内过期的 Amazon EC2 预留实例。

预留实例不会自动续订。您可以继续不中断地使用由预留覆盖的 Amazon EC2 实例，但需支付按需费率。新预留实例可以具有与过期实例相同的参数，也可以购买具有不同参数的预留实例。

预估每月节省是同一实例类型的按需实例费率和预留实例费率之间的差额。

检查 ID

`1e93e4c0b5`

提醒条件

- 黄色：预留实例租赁将在 30 天内过期。
- 黄色：预留实例租赁已在过去 30 天内过期。

Recommended Action（建议的操作）

考虑购买新的预留实例来替换即将到期的预留实例。有关更多信息，请参阅如何购买预留实例和购买预留实例。

其他资源

- 预留实例
- 实例类型

报告列

- 状态
- 区
- 实例类型
- 平台
- 实例计数
- 当前月度成本
- 预估每月节省
- 到期日期
- Reserved Instance ID
- Reason

Amazon EC2 预留实例优化

描述

使用 AWS 的重要部分涉及平衡您的预留实例（RI）购买量和您的按需型实例使用量。此检查提供了关于哪些 RI 可帮助降低使用按需实例产生的成本的建议。

我们通过分析您在过去 30 天内的按需使用情况来创建这些建议。然后，我们将使用情况分为符合条件的预留类别。我们会在生成的使用量类别中模拟每个预留组合以确定要购买的每种 RI 类型的建议数量。这种模拟和优化过程使我们能够最大限度地为您节省成本。此检查涵盖了基于具有部分预付款选项的标准预留实例的建议。

此检查不适用于整合账单中关联的账户。此检查的建议仅适用于付款账户。

检查 ID

```
cX3c2R1chu
```

提醒条件

黄色：优化预付部分费用的预留实例使用量有助于降低成本。

Recommended Action（建议的操作）

请参阅 Cost Explorer 页面，以了解更详细的自定义建议。另请参阅购买指南，了解如何购买预留实例以及可用选项。

其他资源

- 有关预留实例及其如何帮助您节省资金的信息，请单击此处。
- 有关此建议的更多信息，请参阅 Trusted Advisor 常见问题中的预留实例优化检查问题。

报告列

- 区域

- 实例类型
- 平台
- 建议购买的预留实例数量
- 预期平均预留实例使用率
- 建议产生的预估节省（每月）
- 预留实例的预付费用
- 预留实例的预估成本（每月）
- 购买建议预留实例后的预估按需成本（每月）
- 预估收支相抵（月）
- 回顾期（天）
- 期限（年）

Amaz ElastiCache on 节点优化

描述

检查您的预付费 ElastiCache 提供这些建议是为了为了为了

- 回顾期（天）
- 期限（年）

Amazon Serv OpenSearch ice 预留

描述

检查您的 Amazon Ser OpenSearch vice 的使用量，并提供有关购买预留实例的建议。提供这些建议是为了为了为了

如果数据库实例长时间没有连接，您可以删除该实例以降低成本。如果数据库实例在过去 7 天内没有连接，则该实例将被视为空闲。如果实例上的数据需要持久性存储，则可以使用成本较低的选项，例如拍摄和保留数据库快照。手动创建的数据库快照将保留，直到删除它们为止。

检查 ID

`Ti39halfu8`

提醒条件

黄色：活跃数据库实例在过去 7 天内没有连接。

Recommended Action（建议的操作）

考虑为闲置的数据库实例拍摄快照，然后将其停止或删除。停止数据库实例可为其省去某些成本，但无法省去存储成本。停止的实例将基于配置的保留期保留所有自动备份。与删除实例然后仅保留最终快照相比，停止数据库实例通常会产生额外成本。请参阅暂时停止 Amazon RDS 数据库实例和删除带有最终快照的数据库实例。

其他资源

备份和还原

报告列

- 区域
- 数据库实例名称
- 多可用区
- 实例类型
- 预置的存储（GB）
- 自上次连接后的天数
- 预估每月节省（按需）

Amazon Redshift 预留节点优化

描述

检查您的 Amazon Redshift 使用量，并提供有关购买预留节点的建议，以帮助降低使用 Amazon Redshift 按需实例产生的成本。

我们通过分析您在过去 30 天内的按需使用量来生成这些建议。我们使用此分析来模拟生成的使用类别中的每个预留组合。这样，我们就可以确定要购买的每种预留节点的最佳数量，以实现最大的节省成本。此检查涵盖基于部分预付款选项与 1 年或 3 年承诺的建议。

此检查不适用于整合账单中关联的账户。此检查的建议仅适用于付款账户。

检查 ID

`1qw23er45t`

提醒条件

黄色：优化 Amazon Redshift 预留节点的购买有助于降低成本。

Recommended Action（建议的操作）

请参阅 Cost Explorer 页面，以了解更详细的建议、自定义选项（例如回顾期、付款选项等）以及购买 Amazon Redshift 预留节点。

其他资源

- 有关 Amazon Redshift 预留节点及其如何帮助您节省资金的信息，请单击此处。
- 有关此建议的更多信息，请参阅 Trusted Advisor 常见问题中的预留实例优化检查问题。

- 有关字段的更详细描述，请参阅 Cost Explorer 文档

报告列

- 区域
- Family
- 节点类型
- 建议购买的预留节点数量
- 预留节点预期平均使用率
- 建议产生的预估节省（每月）
- UpFront 预付费
- 预留节点预估费用（每月）
- 购买建议预留节点后产生的预估按需成本（每月）
- 预估收支相抵（月）
- 回顾期（天）
- 期限（年）

Amazon Relational Database Service (RDS) 预留实例优化

描述

检查您的 RDS 使用量，并提供有关购买预留实例的建议，以帮助降低使用 RDS 按需实例产生的成本。

我们通过分析您在过去 30 天内的按需使用量来生成这些建议。我们使用此分析来模拟生成的使用类别中的每个预留组合。这样，我们可以确定要购买的每种预留实例的最佳数量，以实现最大的成本节省。此检查涵盖基于部分预付款选项与 1 年或 3 年承诺的建议。

此检查不适用于整合账单中关联的账户。此检查的建议仅适用于付款账户。

检查 ID

```
1qazXsw23e
```

提醒条件

黄色：优化 Amazon RDS 预留实例的购买有助于降低成本。

Recommended Action（建议的操作）

请参阅 Cost Explorer 页面，以了解更详细的建议、自定义选项（例如回顾期、付款选项等）以及购买 Amazon RDS 预留实例。

其他资源

- 有关 Amazon RDS 预留实例及其如何帮助您节省资金的信息，请单击此处。
- 有关此建议的更多信息，请参阅 Trusted Advisor 常见问题中的预留实例优化检查问题。
- 有关字段的更详细描述，请参阅 Cost Explorer 文档

报告列

- 区域
- Family
- 实例类型
- 许可模式
- 数据库版本
- 数据库引擎
- 部署选项
- 建议购买的预留实例数量

- 预留实例预期平均使用率
- 建议产生的预估节省（每月）
- 预留实例预付费
- 预留实例预估费（每月）
- 购买建议预留实例后产生的预估按需成本（每月）
- 预估收支相抵（月）
- 回顾期（天）
- 期限（年）

Amazon Route 53 延迟资源记录集

描述

检查低效配置的 Amazon Route 53 延迟记录集。

为了使 Amazon Route 53 以最新的网络延迟将查询路由到 AWS 区域，您应为不同区域中的特定域名（如 example.com）创建延迟资源记录集。如果您只为域名创建一个延迟资源记录集，则所有查询都将路由到一个区域，并且您需要为基于延迟的路由支付额外费用，但无法获得益处。

AWS 服务创建的托管区域将不会显示在您的检查结果中。

检查 ID

```
51fC20e7I2
```

提醒条件

黄色：仅为特定域名配置了一个延迟资源记录集。

Recommended Action（建议的操作）

如果您的资源分布在多个区域，请务必为每个区域定义延迟资源记录集。请参阅基于延迟的路由。

如果您的资源仅分布在一个 AWS 区域，请考虑在多个 AWS 区域 创建资源，并为每个区域定义延迟资源记录集；请参阅基于延迟的路由。

如果您不想使用多个 AWS 区域，则应该使用简单资源记录集。请参阅使用资源记录集。

其他资源

- Amazon Route 53 开发人员指南
- Amazon Route 53 定价

报告列

- 托管区域名称
- 托管区域 ID
- 资源记录集名称
- 资源记录集类型

过度超时的 AWS Lambda 函数

描述

检查具有可能会导致高成本的高超时率的 Lambda 函数。

Lambda 费用基于您的函数的运行时间和请求的数量。函数超时会导致错误，从而可能会导致重试。重试函数将产生额外的请求和运行时间费用。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

L4dfs2Q3C3

提醒条件

黄色：由于过去 7 天内任何一天的超时，调用超过 10% 的函数以错误结束。

Recommended Action（建议的操作）

检查函数日志记录和 X-ray 跟踪来确定高函数持续时间的贡献者。在相关部分实施代码登录，例如 API 调用或数据库连接之前或之后。默认情况下，AWS SDK 客户端超时可能会长于配置的函数持续时间。将 API 和 SDK 连接客户端调整为在函数超时内重试或失败。如果预期持续时间超过配置的超时，您可以增加函数的超时设置。有关更多信息，请参阅对 Lambda 应用程序进行监控和问题排查。

其他资源

- 对 Lambda 应用程序进行监控和问题排查
- Lambda 函数重试超时 SDK
- 将 AWS Lambda 与 AWS X-Ray 结合使用
- 访问亚马逊 CloudWatch 日志AWS Lambda
- 适用于 AWS Lambda 的错误处理器示例应用程序

报告列

- 状态
- 区域
- 函数 ARN
- 每日最大超时率
- 每日最大超时率的日期
- 每日平均超时率
- 函数超时设置（毫秒）
- 损失的每日计算成本
- 平均每日调用次数
- 当天调用次数
- 当天超时率
- 上次更新时间

具有高误差率的 AWS Lambda 函数

描述

检查具有可能会导致较高成本的高错误率的 Lambda 函数。

Lambda 费用基于您的函数的请求数量和总运行时间。函数错误可能会导致重试，从而产生额外费用。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

L4dfs2Q3C2

提醒条件

黄色：在过去 7 天内任何一天，调用超过 10% 的函数以错误结束。

Recommended Action（建议的操作）

考虑遵照以下指南来减少错误。函数错误包括函数代码返回的错误，以及函数运行时返回的错误。

为了为了为了为了为了为了为了为了为了帮助您排查 Lambda 错误，Lambda 集成了 Amazon CloudWatch 和等服务AWS X-Ray。您可以结合使用日志、指标、警报和 X-Ray 跟踪来快速检测和识别函数代码，API 或支持您的应用程序的其他资源中的问题。有关更多信息，请参阅对 Lambda 应用程序进行监控和问题排查。

有关处理特定运行时错误的更多信息，请参阅 AWS Lambda 中的错误处理和自动重试。

有关其他问题排查，请参阅排查 Lambda 中的问题。

您还可以从 AWS Lambda 合作伙伴提供的监控和可观察性工具的生态系统中选择。有关更多信息，请参阅 AWS Lambda 合作伙伴。

其他资源

- AWS Lambda 中的错误处理和自动重试
- 对 Lambda 应用程序进行监控和问题排查
- Lambda 函数重试超时 SDK
- 排查 Lambda 中的问题
- API 调用错误
- 适用于 AWS Lambda 的错误处理器示例应用程序

报告列

- 状态
- 区域
- 函数 ARN
- 每日最大错误率
- 最大错误率的日期
- 每日平均错误率
- 损失的每日计算成本
- 平均每日调用次数
- 当天调用次数

  当天错误率
- 上次更新时间

相比内存大小过度预调配的 AWS Lambda 函数

描述

检查在回顾期内至少调用过一次的 AWS Lambda 函数。如果有任何 Lambda 函数相比内存大小而言预调配过度，则此检查会提醒您。如果有 Lambda 函数相比内存大小而言预调配过度，则您需要为未使用的资源付费。尽管有些场景可能会导致设计利用率低的问题，但通常可以通过更改 Lambda 函数的配置来降低成本。预估每月节省基于 Lambda 函数的当前使用率。

> **Note**
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`C0r6dfpM05`

提醒条件

黄色：在回顾期内存大小预置过高的 Lambda 函数。为了为了为了为了为了为了为了为了为了为了确定 Lambda 函数是否预置过高，我们会考虑该函数的所有默认 CloudWatch 指标。用于识别内存大小预置过高的 Lambda 函数的算法遵循 AWS 最佳实践。识别新模式后，算法会更新。

Recommended Action（建议的操作）

考虑减少 Lambda 函数的内存大小。

有关更多信息，请参阅启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查 (p. 51)：

报告列

- 状态
- 区域
- 函数名称
- 函数版本
- 内存大小（MB）
- 推荐的内存大小（MB）
- 回顾期（天）
- 节省机会（%）
- 预估每月节省
- 预估每月节省货币
- 上次更新时间

AWS Well-Architected 成本优化高风险问题

描述

对工作负载高风险问题（HRI）的成本优化支柱检查。此检查基于您的 AWS-Well Architected 审查。检查结果取决于您是否使用 AWS Well-Architected 完成了对工作负载的评估。

> **Note**
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`Wxdfp4B1L1`

提醒条件

- 红色：在 AWS Well-Architected 的成本优化支柱中至少发现了一个活跃的高风险问题。
- 绿色：在 AWS Well-Architected 的成本优化支柱中未检测到活跃的高风险问题。

Recommended Action（建议的操作）

AWS Well-Architected 在工作负载评估过程中检测到高风险问题。这些问题为降低风险和节省资金提供了机会。登录 AWS Well-Architected 工具以查看您的答案并采取措施解决活跃的问题。

报告列

- 状态
- 区域
- 工作负载 ARN
- 工作负载名称

- 审核人姓名
- 工作负载类型
- 工作负载开始日期
- 工作负载上次修改日期
- 已确定的成本优化 HRI 数量
- 已解决的成本优化 HRI 数量
- 已回答的成本优化问题数量
- 成本优化支柱中的问题总数
- 上次更新时间

闲置的负载均衡器

描述

检查 Elastic Load Balancing 配置中有无闲置的负载均衡器。

配置的任何负载均衡器都会产生费用。如果负载均衡器没有关联的后端实例，或者如果网络流量受到严重限制，则无法有效地使用负载均衡器。此检查目前仅检查 ELB 服务中的经典负载均衡器类型。它不包括其他 ELB 类型（Application Load Balancer、Network Load Balancer）。

检查 ID

`hjLMh88uM8`

提醒条件

- 黄色：负载均衡器没有活跃的后端实例。
- 黄色：负载均衡器没有运行状况正常的后端实例。
- 黄色：在过去 7 天内，负载均衡器每天的请求数少于 100 个。

Recommended Action（建议的操作）

如果您的负载均衡器没有活跃的后端实例，则考虑注册实例或删除负载均衡器。请参阅使用负载均衡器注册 Amazon EC2 实例或删除负载均衡器。

如果您的负载均衡器没有运行正常的后端实例，请参阅对 Elastic Load Balancing 进行问题排查：运行状况检查配置。

如果您的负载均衡器的请求数较低，则考虑删除负载均衡器。请参阅删除负载均衡器。

其他资源

- 管理负载均衡器
- 对 Elastic Load Balancing 进行问题排查

报告列

- 区域
- 负载均衡器名称
- Reason
- 预估每月节省

低使用率 Amazon EC2 实例

描述

检查过去 14 天内随时运行的 Amazon Elastic Compute Cloud (Amazon EC2) 实例。如果每日 CPU 使用率为 10% 或以下，且网络输入/输出至少在 4 天内不超过 5MB，则此检查会向您发出提示。

正在运行的实例会产生小时使用费。尽管有些场景可能会导致设计上的利用率低，但您通常可以通过管理实例的数量和大小来降低成本。

预估每月节省通过使用按需实例的当前使用率和实例可能未充分利用的预计天数来计算。如果您使用的是预留实例或 Spot 实例，或者实例未运行一整天，则实际节省额将有所不同。要获取每日利用率数据，请下载此检查的报告。

检查 ID

`Qch7DwouX1`

提醒条件

黄色：在过去 14 天的至少 4 天内，实例的每日平均 CPU 使用率未超过 10%，且网络 I/O 未超过 5 MB。

Recommended Action（建议的操作）

考虑停止或终止使用率较低的实例，或通过使用 Auto Scaling 增加实例数量。有关更多信息，请参阅停止和启动实例、终止实例和什么是 Auto Scaling？

其他资源

- 监控 Amazon EC2
- 实例元数据和用户数据
- 亚马逊 CloudWatch 用户指南
- Auto Scaling 开发人员指南

报告列

- 区域/可用区
- 实例 ID
- 实例名称
- 实例类型
- 预估每月节省
- 14 天平均 CPU 使用率
- 14 天平均网络 I/O
- 低使用率天数

Savings Plan

描述

检查您过去 30 天内的 Amazon EC2、Fargate 和 Lambda 的使用量，并提供 Savings Plan 购买建议。这些建议使您承诺在一年或三年期内保持一致的使用量（以每小时美元计量），以换取折扣费率。

这些来源于 AWS Cost Explorer，它可以获得更详细的建议信息。您还可以通过 Cost Explorer 购买 Savings Plan。这些建议应被视为 RI 建议的替代。我们建议您只对一组建议采取措施。对这两组采取措施可能导致过度承诺。

此检查不适用于整合账单中关联的账户。此检查的建议仅适用于付款账户。

检查 ID

`vZ2c2W1srf`

提醒条件

黄色：优化 Savings Plans 的购买有助于降低成本。

Recommended Action（建议的操作）

请参阅 Cost Explorer 页面，以了解更详细的自定义建议以及购买 Savings Plans。

其他资源

- Savings Plan 用户指南
- Savings Plans 常见问题

报告列

- Savings Plans 类型
- 付款选项
- 预付费用
- 要购买的每小时承付款
- 预估平均使用率
- 预估每月节省
- 预估节省百分比
- 期限（年）
- 回顾期（天）

未关联的弹性 IP 地址

描述

检查与正在运行的 Amazon Elastic Compute Cloud (Amazon EC2) 实例没有关联的弹性 IP 地址 (EIP)。

EIP 是专为动态云计算设计的静态 IP 地址。与传统的静态 IP 地址不同，EIP 通过将公有 IP 地址重新映射到您的账户中的另一个实例来屏蔽实例或可用区故障。针对与正在运行的实例无关的 EIP，将收取名义费用。

检查 ID

Z4AUBRNSmz

提醒条件

黄色：分配的弹性 IP 地址（EIP）没有与正在运行的 Amazon EC2 实例关联。

Recommended Action（建议的操作）

将 EIP 与运行的活跃实例关联，或释放未关联的 EIP。有关更多信息，请参阅将弹性 IP 地址与不同的运行实例关联和释放弹性 IP 地址。

其他资源

弹性 IP 地址

报告列

- 区域
- IP 地址

未充分利用的 Amazon EBS 卷

描述

检查 Amazon Elastic Block Store (Amazon EBS) 卷配置，并在卷未充分利用时发出警告。

在创建卷时开始收费。如果卷在一段时间内保持未连接状态或写入活动非常低（不包括启动卷），则该卷未被充分利用。我们建议您删除未充分利用的卷以降低成本。

检查 ID

DAvU99Dc4C

提醒条件

黄色：卷处于未连接状态或过去 7 天里卷每天的 IOPS 小于 1。

Recommended Action（建议的操作）

考虑创建快照并删除卷以减少费用。有关更多信息，请参阅创建 Amazon EBS 快照和删除 Amazon EBS 卷。

其他资源

- Amazon Elastic Block Store (Amazon EBS)
- 监控您的卷状态

报告列

- 区域
- 卷 ID
- 卷名
- 卷类型
- 卷大小
- 每月存储成本
- 快照 ID
- 快照名称
- 快照期限

Note

如果您的账户启用了 AWS Compute Optimizer，我们建议您改用 Amazon EBS 过度预调配卷检查。有关更多信息，请参阅启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查 (p. 51)：

Underutilized Amazon Redshift Clusters

描述

检查您的 Amazon Redshift 配置是否存在似乎未充分利用的集群。

如果 Amazon Redshift 集群长时间没有连接，或者使用的 CPU 量较少，您可以使用成本较低的选项，例如缩小集群规模或关闭集群并拍摄最终快照。即使您删除集群，最终快照也会保留。

检查 ID

```
G31sQ1E9U
```

提醒条件

- 黄色：正在运行的集群在过去 7 天内无连接。
- 黄色：在过去 7 天 99% 的时间内，正在运行的集群的集群级平均 CPU 使用率低于 5%。

Recommended Action（建议的操作）

考虑关闭此集群并拍摄最终快照，或者减小集群的大小。请参阅关闭和删除集群和调整集群大小。

其他资源

亚马逊 CloudWatch 用户指南

报告列

- 状态
- 区域
- 集群

- 实例类型
- Reason
- 预估每月节省

性能

通过检查服务配额（以前称为限制）来提高服务的性能，以便您可以利用预置吞吐量、监控过度使用的实例并检测任何未使用的资源。

您可以使用以下性能类别检查。

检查名称

- Amazon EBS 预置 IOPS (SSD) 卷附件配置 (p. 83)
- Amazon EBS 预调配不足的卷 (p. 84)
- Amazon EC2 至 EBS 的吞吐量优化 (p. 85)
- Amazon Route 53 别名资源记录集 (p. 85)
- 相比内存大小而言预调配不足的 AWS Lambda 函数 (p. 86)
- AWS Well-Architected 性能高风险问题 (p. 87)
- CloudFront 备用域名 (p. 87)
- CloudFront 内容分发优化 (p. 88)
- CloudFront 标头转发和缓存命中率 (p. 89)
- 高使用率 Amazon EC2 实例 (p. 89)
- 应用于实例的大量 EC2 安全组规则 (p. 90)
- EC2 安全组中的大量规则 (p. 91)
- 过度使用的 Amazon EBS 磁性介质卷 (p. 91)
- 亚马逊 EFS 吞吐量模式优化 (p. 92)

Amazon EBS 预置 IOPS (SSD) 卷附件配置

描述

检查附加到未经过 EBS 优化的 Amazon EBS 可优化 Amazon Elastic Compute Cloud (Amazon EC2) 实例的预置 IOPS (SSD) 卷。

Amazon Elastic Block Store (Amazon EBS) 中的预置 IOPS (SSD) 卷仅在附加到 EBS 优化实例时才能提供预期的性能。

检查 ID

```
PPkZrjsH2q
```

提醒条件

黄色：可通过 EBS 优化的 Amazon EC2 实例具有已附加的预调配 IOPS（SSD）卷，但实例未经过 EBS 优化。

Recommended Action（建议的操作）

创建经 EBS 优化的新实例，分离卷，并重新将卷附加到新实例。有关更多信息，请参阅 Amazon EBS 优化的实例和将 Amazon EBS 卷附加到实例。

其他资源

- Amazon EBS 卷类型
- Amazon EBS 卷性能

报告列

- 状态
- 区域/可用区
- 卷 ID
- 卷名
- 卷附件
- 实例 ID
- 实例类型
- EBS 优化

Amazon EBS 预调配不足的卷

描述

检查在回顾期内任何时刻运行过的 Amazon Elastic Block Store（Amazon EBS）卷。如果有任何 EBS 卷相比您的工作负载而言预调配不足，则该检查会提醒您。持续的高利用率可能代表已经优化的稳定性能，但也可能说明应用程序没有足够的资源。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`COr6dfpM04`

提醒条件

黄色：回顾期间预置不足的 EBS 卷。为了确定卷是否预调配不足，我们会考虑所有默认 CloudWatch 指标（包括 IOPS 和吞吐量）。用于识别预置不足的 EBS 卷的算法遵循 AWS 最佳实践。识别新模式后，算法会更新。

Recommended Action（建议的操作）

考虑扩大使用率高的卷。

有关更多信息，请参阅启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查 (p. 51)：

报告列

- 状态
- 区域
- 卷 ID
- 卷类型
- 卷大小（GB）
- 卷基准 IOPS
- 卷爆增 IOPS
- 卷爆增吞吐量
- 推荐的卷类型
- 推荐的卷大小（GB）
- 推荐的卷基准 IOPS
- 推荐的卷爆增 IOPS
- 推荐的卷基准吞吐量
- 推荐的卷爆增吞吐量

- 回顾期（天）
- 性能风险
- 上次更新时间

Amazon EC2 至 EBS 的吞吐量优化

描述

检查其性能可能受其连接到的 Amazon EC2 实例的最大吞吐量能力影响的 Amazon EBS 卷。

要优化性能，您应确保 Amazon EC2 实例的最大吞吐量大于所附加的 EBS 卷的最大总吞吐量。此检查计算前一天内每个 EBS 优化实例（基于协调世界时 (UTC)）每五分钟的 EBS 卷吞吐量，并在超过一半时段的使用率大于 EC2 实例最大吞吐量的 95% 时提醒您。

检查 ID

`Bh2xRR2FGH`

提醒条件

黄色：在前一天（UTC）一半以上的时间中，附加到 EC2 实例的 EBS 卷的总吞吐量（MB/秒）超过了实例与 EBS 卷之间发布吞吐量的 95%。

Recommended Action（建议的操作）

将您的 Amazon EBS 卷的最大吞吐量（请参阅 Amazon EBS 卷类型）与其附加到的 Amazon EC2 实例的最大吞吐量进行比较。请参阅支持 EBS 优化的实例类型。

考虑将您的卷附加到能支持更高 EBS 吞吐量的实例以获得最佳性能。

其他资源

- Amazon EBS 卷类型
- Amazon EBS 优化的实例
- 监控您的卷状态
- 将 Amazon EBS 卷附加到实例
- 将 Amazon EBS 卷与实例分离
- 删除 Amazon EBS 卷

报告列

- 状态
- 区域
- 实例 ID
- 实例类型
- 接近最大时间

Amazon Route 53 别名资源记录集

描述

检查可更改为别名资源记录集以提高性能并节省成本的资源记录集。

别名资源记录集将 DNS 查询路由到 AWS 资源（例如 Elastic Load Balancing 负载均衡器或 Amazon S3 存储桶）或另一个 Route 53 资源记录集。使用别名资源记录集时，Route 53 会将 DNS 查询免费路由到您的 AWS 资源。

AWS 服务创建的托管区域将不会显示在您的检查结果中。

检查 ID

B913Ef6fb4

提醒条件

- 黄色：资源记录集是 Amazon S3 网站的 CNAME。
- 黄色：资源记录集是 Amazon CloudFront 分配的 CNAME。
- 黄色：资源记录集是 Elastic Load Balancing 负载均衡器的 CNAME。

Recommended Action（建议的操作）

将列出的 CNAME 资源记录集替换为别名资源记录集；请参阅在别名和非别名资源记录集之间进行选择。

您还需要将记录类型从 CNAME 更改为 A 或 AAAA，具体取决于 AWS 资源。请参阅在创建或编辑 Amazon Route 53 资源记录集时指定的值。

其他资源

将查询路由到 AWS 资源

报告列

- 状态
- 托管区域名称
- 托管区域 ID
- 资源记录集名称
- 资源记录集类型
- 资源记录集标识符
- 别名目标

相比内存大小而言预调配不足的 AWS Lambda 函数

描述

检查在回顾期内至少调用过一次的 AWS Lambda 函数。如果有任何 Lambda 函数相比内存大小而言预调配不足，则此检查会提醒您。如果 Lambda 函数相比内存大小而言预调配不足，这些函数将需要更长的时间才能完成操作。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

C0r6dfpM06

提醒条件

黄色：在回顾期内存大小预置不足的 Lambda 函数。为了确定 Lambda 函数是否预置不足，我们会考虑该函数的所有默认CloudWatch指标。用于识别内存大小预置不足的 Lambda 函数的算法遵循 AWS 最佳实践。识别新模式后，算法会更新。

Recommended Action（建议的操作）

考虑增加 Lambda 函数的内存大小。

有关更多信息，请参阅启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查 (p. 51)：

报告列

- 状态

- 区域
- 函数名称
- 函数版本
- 内存大小（MB）
- 推荐的内存大小（MB）
- 回顾期（天）
- 性能风险
- 上次更新时间

AWS Well-Architected 性能高风险问题

描述

对工作负载高风险问题（HRI）的性能支柱检查。此检查基于您的 AWS-Well Architected 审查。检查结果取决于您是否使用 AWS Well-Architected 完成了对工作负载的评估。

> Note
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`Wxdfp4B1L2`

提醒条件

- 红色：在 AWS Well-Architected 的性能支柱中至少发现了一个活跃的高风险问题。
- 绿色：在 AWS Well-Architected 的性能支柱中未检测到活跃的高风险问题。

Recommended Action（建议的操作）

AWS Well-Architected 在工作负载评估过程中检测到高风险问题。这些问题为降低风险和节省资金提供了机会。登录 AWS Well-Architected 工具以查看您的答案并采取措施解决活跃的问题。

报告列

- 状态
- 区域
- 工作负载 ARN
- 工作负载名称
- 审核人姓名
- 工作负载类型
- 工作负载开始日期
- 工作负载上次修改日期
- 已确定的性能 HRI 数量
- 已解决的性能 HRI 数量
- 已回答的性能问题数量
- 性能支柱中的问题总数
- 上次更新时间

CloudFront 备用域名

描述

检查Amazon CloudFront 分配中是否存在已错误配置 DNS 设置的备用域名（CNAME）。

如果 CloudFront 分配包含备用域名，则域的 DNS 配置必须将 DNS 查询路由到该分配。

Note

此检查假Amazon Route 53 DNS 和亚马逊CloudFront分配配置在相同中AWS 账户。因此，提示列表可能包括由于此 AWS 账户 外的 DNS 设置而按预期工作的资源。

检查 ID

N420c450f2

提醒条件

- 黄色：CloudFront分配包含备用域名，但未使用 CNAME 记录或 Amazon Route 53 别名资源记录正确设置 DNS 配置。
- 黄色：CloudFront 分配包含备用域名，但 Trusted Advisor 无法评估 DNS 配置，因为存在过多重定向。
- 黄色：CloudFront 分配包含备用域名，但 Trusted Advisor 由于其他某些原因（很可能是因为超时）无法评估 DNS 配置。

Recommended Action（建议的操作）

将 DNS 配置更新为将 DNS 查询路由到 CloudFront 分配；请参阅使用备用域名（CNAME）。

如果您使用 Amazon Route 53 作为 DNS 服务，请参使用域名将流量路由到 Amazon CloudFront Route 53 作为 DNS 服务。如果检查超时，请尝试刷新检查。

其他资源

亚马逊CloudFront开发者指南

报告列

- 状态
- 分配 ID
- 分配域名
- 备用域名
- Reason

CloudFront 内容分发优化

描述

检查可以通过AWS全球内容分发服务 Amazon Simple Storage Service Service (Amazon CloudFront S3) 存储桶的数据传输的情况。

当您配置 CloudFront 以分发内容时，对内容的请求将自动路由到缓存内容的最近边缘站点。此路由可以以最佳的性能将内容分发给您的用户。与存储桶中存储的数据相比，传出的数据比率较高，这表明您可以从使用 Amazon CloudFront 分发数据中受益。

检查 ID

796d6f3D83

提醒条件

- 黄色：检查前 30 天通过 GET 请求从存储桶传输到用户的数据量至少是存储桶中存储的平均数据量的 25 倍。
- 红色：检查前 30 天通过 GET 请求从存储桶传输到用户的数据量至少为 10TB，并且至少是存储桶中存储的平均数据量的 25 倍。

Recommended Action（建议的操作）

考虑使用 CloudFront 以获得更佳性能。查看亚马逊CloudFront商品详情。

如果每月传输的数据为 10TB 或更多，请参 Amazon CloudFront 定价，以了解可能节省的成本。

其他资源

- 亚马逊CloudFront开发者指南
- AWS 案例研究：PBS

报告列

- 状态
- 区域
- 存储桶名称
- S3 存储（GB）
- 数据传出（GB）
- 传输/存储比率

CloudFront 标头转发和缓存命中率

描述

检查 CloudFront 当前从客户端接收并转发到原始服务器的 HTTP 请求标头。

某些标头（如日期或用户代理）会显著降低缓存命中率（从 CloudFront 边缘缓存提供的请求的比例）。这会增加原始服务器的负载并降低性能，因为 CloudFront 必须将更多的请求转发到原始服务器。

检查 ID

N415c450f2

提醒条件

黄色：CloudFront 转发到原始服务器的一个或多个请求标头可能会显著降低缓存命中率。

Recommended Action（建议的操作）

请考虑请求标头是否提供了足够的益处，能够证实对缓存命中率造成的负面影响是有必要的。如果不论给定标头值为何，您的原始服务器均会返回相同的对象，那么我们建议您不要将 CloudFront 配置为将标头转发到原始服务器。有关更多信息，请参基于请求请求标头缓存吞吐CloudFront吞吐吞吐吞吐吞吐吞吐吞吐吞吐吞吐吞吐吞吐

其他资源

- 提升由 CloudFront 边缘缓存提供服务的请求的比例
- CloudFront 缓存统计报告
- HTTP 请求标头和 CloudFront 行为

报告列

- 分配 ID
- 分配域名
- 缓存行为路径模式
- 标头

高使用率 Amazon EC2 实例

描述

检查过去 14 天内随时运行的 Amazon Elastic Compute Cloud (Amazon EC2) 实例。如果在四天或更长时间内每日 CPU 使用率超过 90%，则会发送警报。

一致的高利用率可能表明性能得到优化、稳定。但是，它也可能表示应用程序没有足够的资源。要获取每日 CPU 使用率数据，请下载此检查的报告。

检查 ID

ZRxQlPsb6c

提醒条件

黄色：在过去 14 天中的至少 4 天内，某个实例的日均 CPU 使用率超过 90%。

Recommended Action（建议的操作）

考虑添加更多实例。有关根据需要增加实例数量的信息，请参阅什么是 Auto Scaling？

其他资源

- 监控 Amazon EC2
- 实例元数据和用户数据
- 亚马逊CloudWatch用户指南
- Amazon EC2 Auto Scaling 用户指南

报告列

- 区域/可用区
- 实例 ID
- 实例类型
- 实例名称
- 14 天 CPU 平均使用率
- CPU 使用率超过 90% 的天数

应用于实例的大量 EC2 安全组规则

描述

检查具有大量安全组规则的 Amazon Elastic Compute Cloud (Amazon EC2) 实例。如果实例具有大量规则，性能可能会降低。

检查 ID

j3DFqYTe29

提醒条件

- 黄色：某个 Amazon EC2-VPC 实例拥有超过 50 个安全组规则。
- 黄色：某个 Amazon EC2-Classic 实例拥有超过 100 个安全组规则。

Recommended Action（建议的操作）

通过删除不必要或重叠的规则，减少与实例关联的规则数量。有关更多信息，请参阅从安全组中删除规则。

其他资源

Amazon EC2 安全组

报告列

- 区域
- 实例 ID
- 实例名称
- VPC ID
- 入站规则总数
- 出站规则总数

EC2 安全组中的大量规则

描述

检查每个 Amazon Elastic Compute Cloud (Amazon EC2) 安全组是否存在过多的规则。

如果安全组具有大量规则，则性能可能会降低。

检查 ID

`tfg86AVHAZ`

提醒条件

- 黄色：某个 Amazon EC2-VPC 安全组拥有超过 50 个规则。
- 黄色：某个 Amazon EC2-Classic 安全组拥有超过 100 个规则。

Recommended Action（建议的操作）

删除不必要或重复的规则，以减少安全组中规则的数量。有关更多信息，请参阅从安全组中删除规则。

其他资源

Amazon EC2 安全组

报告列

- 区域
- 安全组名称
- 组 ID
- 描述
- 实例计数
- VPC ID
- 入站规则总数
- 出站规则总数

过度使用的 Amazon EBS 磁性介质卷

描述

检查可能被过度利用且可能受益于更高效配置的 Amazon Elastic Block Store (Amazon EBS) 磁性介质卷。

磁性介质卷设计用于具有中等或突发输入/输出（I/O）要求的应用程序，不保证 IOPS 速率。它平均提供约 100 IOPS，且最大限度能够突增至数百 IOPS。对于一贯较高的 IOPS，您可以使用预置 IOPS (SSD) 卷。对于突发 IOPS，您可以使用通用型 (SSD) 卷。有关更多信息，请参阅 Amazon EBS 卷类型。

有关支持 EBS 优化行为的实例类型列表，请参阅 Amazon EBS 优化的实例。

要获取每日使用率指标，请下载此检查的报告。详细的报告将针对过去 14 天中的每一天显示一列。如果没有活跃 EBS 卷，单元格将为空。如果没有充足的数据来进行可靠的测量，则单元格显示 N/A。如果数据充足，单元格将包含每日中值和中值相对变化百分比（例如，`256 / 20%`）。

检查 ID

`k3J2hns32g`

提醒条件

黄色：Amazon EBS 磁卷附加到实例中，该实例可通过 EBS 优化或作为集群计算网络的组成部分，该集群计算网络的每日中值大于 95 IOPS，并且在过去 14 天中，至少有 7 天的变化幅度小于中值的 10%。

Recommended Action（建议的操作）

对于一贯较高的 IOPS，您可以使用预置 IOPS (SSD) 卷。对于突发 IOPS，您可以使用通用型 (SSD) 卷。有关更多信息，请参阅 Amazon EBS 卷类型。

其他资源

Amazon Elastic Block Store (Amazon EBS)

报告列

- 状态
- 区域
- 卷 ID
- 卷名
- 超过的天数
- 最大每日中值

Note

如果您的账户启用了 AWS Compute Optimizer，我们建议您改用 Amazon EBS 预调配不足卷检查。有关更多信息，请参阅启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查 (p. 51)：

亚马逊 EFS 吞吐量模式优化

描述

检查客户的 Amazon EFS 文件系统当前是否配置为使用突增吞吐量模式。

EFS 突增吞吐量模式 [1] 中的文件系统提供一致的基准吞吐量水平（EFS 标准存储中每 GiB 数据 50 KiB/s），并在 “突发积分” 可用时使用积分模型提供更高级别的 “突发吞吐量” 性能。当您耗尽突发积分时，您的文件系统性能会被限制到这个较低的基准水平，这可能会导致速度变慢、超时或对最终用户或应用程序造成其他形式的性能影响。

检查 ID

```
c1dfprch02
```

提醒条件

- 黄色：文件系统正在使用突增吞吐量模式。

Recommended Action（建议的操作）

为了让您的用户和应用程序达到所需的吞吐量，我们建议您将文件系统配置更新为弹性吞吐量模式 [2]。在弹性吞吐量模式下，您的文件系统可以实现高达 10 GiB/s 的读取吞吐量或 3 GiB/s 的写入吞吐量，具体取决于 AWS 区域 [3]，您只需为使用的吞吐量付费。请注意，您可以更新文件系统配置，按需在 Elastic 和 Bursting 吞吐量模式之间切换，而且 Elastic 吞吐量模式下的文件系统会产生额外的数据传输费用 [4]。

其他资源

- [1] 亚马逊 EFS 性能吞吐量模式
- [2] 亚马逊 EFS 性能弹性吞吐量模式
- [3] 亚马逊 EFS 配额和限制
- [4] 亚马逊 EFS 定价

报告列

- 状态
- 区域
- EFS 文件系统 ID

- 吞吐吞吐吞
- 上次更新时间

安全性

您可以使用以下安全类别检查。

Note

如果为您的 AWS 账户 启用 Security Hub，则可以在 Trusted Advisor 控制台中查看检查结果。有关信息，请参阅 在 AWS Trusted Advisor 中查看 AWS Security Hub 控件 (p. 46)。
您可以查看 AWS 基础安全最佳实践安全标准中的所有控件，但具有 Category: Recover > Resilience（类别：恢复 > 弹性）的控件除外。有关受支持控件的列表，请参阅《AWS Security Hub 用户指南》中的 AWS基础安全最佳实践控件。

检查名称

- 使用终止支持版本的 Microsoft SQL Server 的 Amazon EC2 实例 (p. 93)
- 使用终止支持版本的 Microsoft Windows Server 的 Amazon EC2 实例 (p. 94)
- Amazon EBS 公有快照 (p. 95)
- Amazon RDS 公有快照 (p. 96)
- Amazon RDS 安全组访问风险 (p. 96)
- Amazon Route 53 MX 资源记录集和发件人策略框架 (p. 97)
- Amazon S3 存储桶权限 (p. 97)
- AWS CloudTrail 日志记录 (p. 98)
- 使用弃用运行时的 AWS Lambda 函数 (p. 99)
- AWS Well-Architected 安全性高风险问题 (p. 100)
- CloudFrontIAM 证书存储中的自定义 SSL 证书 (p. 100)
- CloudFront源服务器上的 SSSSL 证书 (p. 101)
- ELB 侦听器安全 (p. 102)
- ELB 安全组 (p. 103)
- Exposed Access Keys (p. 103)
- IAM 访问密钥轮换 (p. 104)
- IAM 密码策略 (p. 105)
- IAM 使用 (p. 105)
- 根账户的 MFA (p. 106)
- 安全组 – 不受限制的特定端口 (p. 106)
- 安全组 – 不受限制的访问 (p. 107)

使用终止支持版本的 Microsoft SQL Server 的 Amazon EC2 实例

描述

检查过去 24 小时内运行的 Amazon Elastic Compute Cloud（Amazon EC2）实例的 SQL Server 版本。如果该版本的支持接近或已经终止，则此检查会提示您。每个 SQL Server 版本都提供 10 年的支持，包括 5 年主流支持和 5 年延伸支持。支持终止后，该 SQL Server 版本将不会收到定期的安全更新。使用不受支持的 SQL Server 版本运行应用程序可能会带来安全或合规风险。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。
当前，您无法从此检查中排除资源。

检查 ID

Qsdfp3A4L3

提醒条件

- 红色：EC2 实例的 SQL Server 版本已达到停止支持。
- 黄色：EC2 实例的 SQL Server 版本将在 12 个月内达到停止支持。

Recommended Action（建议的操作）

要实现 SQL Server 工作负载现代化，请考虑重构到 Amazon Aurora 等 AWS Cloud 原生数据库。有关更多信息，请参阅使用 AWS 实现 Windows 工作负载现代化。

要迁移到完全托管式数据库，请考虑更换平台到 Amazon Relational Database Service（Amazon RDS）。有关更多信息，请参阅 Amazon RDS for SQL Server。

要升级 SQL Server on Amazon EC2，请考虑使用自动化运行手册简化升级。有关更多信息，请参阅 AWS Systems Manager 文档。

如果无法升级 SQL Server on Amazon EC2，请考虑适用于 Windows Server 的停止支持迁移计划（EMP）。有关更多信息，请参阅 EMP 网站。

其他资源

- 使用 AWS 为 SQL Server 做好停止支持的准备
- AWS 上的 Microsoft SQL Server

报告列

- 状态
- 区域
- 实例 ID
- SQL Server 版本
- 支持周期
- 停止支持
- 上次更新时间

使用终止支持版本的 Microsoft Windows Server 的 Amazon EC2 实例

描述

如果该版本的支持接近或已经终止，则此检查会提示您。每个 Windows Server 版本都提供 10 年的支持。这包括 5 年主流支持和 5 年延长支持。支持终止到期后，该 Windows Server 版本将不会收到定期的安全更新信息。如果您使用不受支持的 Windows Server 版本运行应用程序，则这些应用程序的安全性或合规性将面临风险。

检查 ID

Qsdfp3A4L4

提醒条件

- 红色：EC2 实例的 Windows Server 版本（Windows Server 2003、2003 R2、2008 和 2008 R2）已经超过享受支持终止的期限。
- 黄色：目前距 EC2 实例的 Windows Server 版本（Windows Server 2012 和 2012 R2）的支持终止服务结束时间还有不到 18 个月。

Recommended Action（建议的操作）

要让 Windows Server 工作负载现代化，请考虑使用 Modernize Windows Workloads with （使用 AWS 实现 Windows 工作负载现代化）提供的各种选项。

要升级 Windows Server 工作负载以在更新版本的 Windows Server 上运行，您可以使用自动化运行手册。有关更多信息，请参阅 AWS Systems Manager 文档。

如果因应用程序不兼容而无法升级 Windows Server 工作负载，请考虑使用适用于 Windows Server 的终止支持迁移计划（EMP）。有关更多信息，请参阅 EMP 网站。您还可以在产品的“支持终止”日期之后购买最长 3 年的 Microsoft 的扩展安全更新（ESU）。了解更多。

其他资源

- AWS 上的 Windows
- 适用于 Windows Server 的支持终止迁移计划

报告列

- 状态
- 区域
- 实例 ID
- Windows Server 版本
- 支持周期
- 停止支持
- 上次更新时间

Amazon EBS 公有快照

描述

检查 Amazon Elastic Block Store (Amazon EBS) 卷快照的权限设置，并在任何快照被标记为公有快照时发出提醒。

当您将快照公开时，可以为所有 AWS 账户 和用户授予访问快照上的所有数据的权限。如果要仅与特定用户或账户共享快照，请将快照标记为私有。然后，指定要与之共享快照数据的用户或账户。

> Note
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。

检查 ID

```
ePs02jT06w
```

提醒条件

红色：EBS 卷快照标记为公有。

Recommended Action（建议的操作）

除非您确定要与所有 AWS 账户 和用户共享快照中的所有数据，否则请修改权限：将快照标记为私有，然后指定您想向其授予权限的账户。有关更多信息，请参阅共享 Amazon EBS 快照。无法从 Trusted Advisor 控制台的视图中排除此检查。

要直接修改快照的权限，您可以在 AWS Systems Manager 控制台中使用运行手册。有关更多信息，请参阅`AWSSupport-ModifyEBSSnapshotPermission`：

其他资源

Amazon EBS 快照

报告列

- 状态
- 区域
- 卷 ID

- 快照 ID
- 描述

Amazon RDS 公有快照

描述

检查 Amazon Relational Database Service (Amazon RDS) 数据库快照的权限设置，并在任何快照被标记为公有时发出提醒。

当您将快照公开时，可以为所有 AWS 账户 和用户授予访问快照上的所有数据的权限。如果要仅与特定用户或账户共享快照，请将快照标记为私有。然后，指定要与之共享快照数据的用户或账户。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。

检查 ID

`rSs93HQwa1`

提醒条件

红色：Amazon RDS 快照标记为公有。

Recommended Action（建议的操作）

除非您确定要与所有 AWS 账户 和用户共享快照中的所有数据，否则请修改权限：将快照标记为私有，然后指定您想向其授予权限的账户。有关更多信息，请参阅共享数据库快照或数据库集群快照。无法从 Trusted Advisor 控制台的视图中排除此检查。

要直接修改快照的权限，您可以在 AWS Systems Manager 控制台中使用运行手册。有关更多信息，请参阅`AWSSupport-ModifyRDSSnapshotPermission`：

其他资源

备份和还原 Amazon RDS 数据库实例

报告列

- 状态
- 区域
- 数据库实例或集群 ID
- 快照 ID

Amazon RDS 安全组访问风险

描述

检查 Amazon Relational Database Service (Amazon RDS) 的安全组配置，并在安全组规则授予对您的数据库的过度权限时发出警告。安全组规则的建议配置是仅允许从特定的 Amazon Elastic Compute Cloud (Amazon EC2) 安全组或特定 IP 地址进行访问。

检查 ID

`nNauJisYIT`

提醒条件

- 黄色：数据库安全组规则引用了向以下某个端口授予全局访问权限的 Amazon EC2 安全组：20、21、22、1433、1434、3306、3389、4333、5432 和 5500。
- 黄色：数据库安全组规则向多个 IP 地址授予访问权限（CIDR 规则后缀不是 /0 或 /32）。

- 红色：数据库安全组规则授予了全局访问权限（CIDR 规则后缀为 /0）。

Recommended Action（建议的操作）

审核您的安全组规则，将访问权限限制为授权的 IP 地址或 IP 范围。要编辑安全组，请使用 author izeDB SecurityGroupIngress API 或。AWS Management Console有关更多信息，请参阅使用数据库安全组。

其他资源

- Amazon RDS 安全组
- 无类域间路由
- TCP 和 UDP 端口号列表

报告列

- 状态
- 区域
- RDS 安全组名称
- 入口规则
- Reason

Amazon Route 53 MX 资源记录集和发件人策略框架

描述

对于每个 MX 资源记录集，检查 TXT 或 SPF 资源记录集是否包含有效的 SPF 记录。记录必须以“v=spf1”开头。SPF 记录指定有权为您的域发送电子邮件的服务器，这有助于检测和停止电子邮件地址欺骗并减少垃圾邮件。Route 53 建议您使用 TXT 记录而不是 SPF 记录。只要每个 MX 资源记录集至少有一个 SPF 或 TXT 记录，Trusted Advisor 就会将此检查报告为绿色。

检查 ID

`c9D319e7sG`

提醒条件

黄色：MX 资源记录集没有包含有效 SPF 值的 TXT 或 SPF 资源记录。

Recommended Action（建议的操作）

对于每个 MX 资源记录集，创建包含有效 SPF 值的 TXT 资源记录集。有关更多信息，请参阅发件人策略框架：SPF 记录语法和使用 Amazon Route 53 控制台创建资源记录集。

其他资源

- 发件人策略框架
- MX 记录

报告列

- 托管区域名称
- 托管区域 ID
- 资源记录集名称
- 状态

Amazon S3 存储桶权限

描述

检查 Amazon Simple Storage Service (Amazon S3) 中具有开放访问权限，或允许访问任何经过身份验证的 AWS 用户的存储桶。

此检查将检查显式存储桶权限以及可能覆盖这些权限的存储桶策略。建议不要向 Amazon S3 存储桶的所有用户授予列表访问权限。这些权限可能导致非预期的用户频繁地列出存储桶中的对象，从而导致费用高于预期。向每个人授予上载和删除访问权限的权限可能会导致存储桶中出现安全漏洞。

检查 ID

`Pfx0RwqBli`

提醒条件

- 黄色：对于 Everyone（所有人）或 Any Authent icate AWS d User
- 黄色：存储桶策略允许任何种类的开放访问。
- 黄色：存储桶策略具有授予公有访问权限的语句。Block public and cross-account access to buckets that have public policies（阻止对具有公有策略的存储桶进行公有和跨账户存取）设置已打开，并且已限制为只有在删除公有语句之后，才允许该账户的授权用户访问。
- 黄色：Trusted Advisor 无权检查策略，或出于其他原因无法评估策略。
- 红色：对于 Everyone（所有人）或 Any Authenticated AWSUser（所有人）

Recommended Action（建议的操作）

如果存储桶允许开放访问，请确定是否确实需要开放访问。如果不需要，请更新存储桶权限，以只允许拥有者或特定用户访问。使用“Amazon S3 阻止公有访问”来控制允许对您的数据进行公有访问的设置。请参阅设置存储桶和对象访问权限。

其他资源

管理对 Amazon S3 资源的访问权限

报告列

- 状态
- 区域名称
- 区域 API 参数
- 存储桶名称
- ACL 允许列表
- ACL 允许上载/删除
- 策略允许访问

AWS CloudTrail 日志记录

描述

检查您的 AWS CloudTrail 使用。CloudTrailAWS 账户通过记录对账户进行的 AWS API 调用的信息，提高了对您的中的活动的可见性。例如，您可以使用这些日志来确定特定用户在指定时间段内执行了哪些操作，或者哪些用户在指定时间段内对特定资源采取操作。

因为将日志文件CloudTrail传送到 Amazon Simple Storage Service (Amazon S3) 存储桶，因此CloudTrail必须拥有对存储桶的写入权限。如果跟踪应用于所有区域（创建新跟踪时的默认设置），跟踪会多次出现在 Trusted Advisor 报告中。

检查 ID

`vjafUGJ9H0`

提醒条件

- 黄色：CloudTrail 报告跟踪的日志传输错误。
- 红色：尚未为某区域创建跟踪，或已针对某跟踪关闭日志记录。

Recommended Action（建议的操作）

要通过控制台创建跟踪并启动日志记录，请转到 AWS CloudTrail 控制台。

要启动日志记录，请参阅停止和启动跟踪的日志记录。

如果收到日志传输错误，请确保相应存储桶存在，并且已向存储桶附加必要的策略。请参阅 Amazon S3 存储桶策略。

其他资源

- AWS CloudTrail 用户指南
- 支持的区域
- 支持的服务

报告列

- 状态
- 区域
- 跟踪名称
- 日志记录状态
- 存储桶名称
- 上次交付日期

使用弃用运行时的 AWS Lambda 函数

描述

检查配置为使用即将弃用或已弃用的的运行时的 Lambda 函数。我们不向已弃用的运行时提供安全更新或技术支持。

> Note
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

已发布的 Lambda 函数版本不可改变，这意味着这些版本可以叫用，但不能更新。只有 Lambda 函数的 $LATEST 版本才能更新。有关更多信息，请参阅 Lambda 函数版本。

检查 ID

L4dfs2Q4C5

提醒条件

- 红色：此函数在已弃用的运行时运行。
- 黄色：此函数在将在 120 天内弃用的运行时运行。

Recommended Action（建议的操作）

如果您的函数正在接近弃用的运行时运行，您应准备好迁移到受支持的运行时。有关更多信息，请参阅运行时支持策略。

我们建议您删除不再使用的较早的函数版本。

其他资源

Lambda 运行时

报告列

- 状态
- 区域
- 函数 ARN
- 运行时
- 弃用的天数
- 弃用日期

- 平均每日调用次数
- 上次更新时间

AWS Well-Architected 安全性高风险问题

描述

对工作负载高风险问题（HRI）的安全性支柱检查。此检查基于您的 AWS-Well Architected 审查。检查结果取决于您是否使用 AWS Well-Architected 完成了对工作负载的评估。

> Note
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`Wxdfp4B1L3`

提醒条件

- 红色：在 AWS Well-Architected 的安全支柱中至少发现了一个活跃的高风险问题。
- 绿色：在 AWS Well-Architected 的安全支柱中未检测到活跃的高风险问题。

Recommended Action（建议的操作）

AWS Well-Architected 在工作负载评估过程中检测到高风险问题。这些问题为降低风险和节省资金提供了机会。登录 AWS Well-Architected 工具以查看您的答案并采取措施解决活跃的问题。

报告列

- 状态
- 区域
- 工作负载 ARN
- 工作负载名称
- 审核人姓名
- 工作负载类型
- 工作负载开始日期
- 工作负载上次修改日期
- 已确定的安全 HRI 数量
- 已解决的安全 HRI 数量
- 安全问题数量
- 安全支柱中的问题总数
- 上次更新时间

CloudFrontIAM 证书存储中的自定义 SSL 证书

描述

检查 IAM 证书存储中的CloudFront备用域名的 SSSSSSL 证书。如果证书已过期、即将过期、使用过时的加密或未针对分发正确配置，则此检查会提醒您。

当备用域名的自定义证书过期时，显示您的 CloudFront 内容的浏览器可能会显示有关您的网站安全性的警告消息。使用 SHA-1 哈希算法加密的证书已被 Chrome 和 Firefox 等 Web 浏览器弃用。

证书必须包含与查看器请求的主机标头中的源域名或域名匹配的域名。如果不匹配，CloudFront 会向用户返回 HTTP 状态代码 502（错误的网关）。有关更多信息，请参阅使用备用域名和 HTTPS。

检查 ID

N425c450f2

提醒条件

- 红色：自定义 SSL 证书已过期。
- 黄色：自定义 SSL 证书将在七天后过期。
- 黄色：自定义 SSL 证书是使用 SHA-1 哈希算法加密的。
- 黄色：分配中的一个或多个备用域名未出现在自定义 SSL 证书的 Common Name（常用名称）或 Subject Alternative Names（主题备用名称）字段中。

Recommended Action（建议的操作）

续订已过期证书或即将过期的证书。

将使用 SHA-1 哈希算法加密的证书替换为使用 SHA-256 哈希算法加密的证书。

将证书替换为在 Common Name（常用名称）或 Subject Alternative Domain Names（主题备用域名）字段中包含适用值的证书。

其他资源

使用 HTTPS 连接访问对象

报告列

- 状态
- 分配 ID
- 分配域名
- 证书名称
- Reason

CloudFront源服务器上的 SSSSL 证书

描述

检查源服务器是否存在已过期、即将过期、丢失或使用过时加密的 SSL 证书。如果证书存在这些问题之一，CloudFront 会使用 HTTP 状态代码 502（错误网关）响应对您的内容的请求。

使用 SHA-1 哈希算法加密的证书已被 Chrome 和 Firefox 等 Web 浏览器弃用。根据您与 “CloudFront 分配关联的 SSSSSSSSSSL 证书的数量，此检查可能会在 Web 托管提供商（例如，AWS如果您使用 Amazon EC2 或 Elastic Load Balancing 作为CloudFront分配的源服务器，提供商即为）发给您的每月账单上增加少量金额。此检查不会验证您的源证书链或证书颁发机构。您可以在 CloudFront 配置中进行这些检查。

检查 ID

N430c450f2

提醒条件

- 红色：源服务器上的 SSL 证书已过期或缺失。
- 黄色：源服务器上的 SSL 证书将在 30 天后过期。
- 黄色：源服务器上的 SSL 证书是使用 SHA-1 哈希算法加密的。
- 黄色：无法找到源服务器上的 SSL 证书。连接失败，可能是因为超时或其他 HTTPS 连接问题。

Recommended Action（建议的操作）

续订源服务器上已过期或即将过期的证书。

如果证书不存在，请添加证书。

将使用 SHA-1 哈希算法加密的证书替换为使用 SHA-256 哈希算法加密的证书。

其他资源

使用备用域名和 HTTPS

报告列

- 状态
- 分配 ID
- 分配域名
- Origin
- Reason

ELB 侦听器安全

描述

检查负载均衡器的监听器未使用推荐的安全配置进行加密通信。 AWS建议使用安全协议（HTTS、以及使用up-to-date安全密码和协议。

当您为前端连接（客户端到负载均衡器）使用安全协议时，客户端和负载均衡器之间的请求将被加密，从而创建更安全的环境。Elastic Load Balancing 提供预定义的安全策略，其密码和协议符合 AWS 安全最佳实践。新配置可用时，会发布预定义策略的新版本。

检查 ID

```
a2sEc6ILx
```

提醒条件

- 黄色：负载均衡器的任何侦听器均未使用安全协议（HTTPS 或 SSL）。
- 黄色：负载均衡器侦听器使用了过时的预定义 SSL 安全策略。
- 黄色：负载均衡器侦听器使用了不推荐的密码或协议。
- 红色：负载均衡器侦听器使用了不安全的密码或协议。

Recommended Action（建议的操作）

如果传输到负载均衡器的流量必须安全无虞，请使用 HTTPS 或 SSL 协议进行前端连接。

将负载均衡器的预定义 SSL 安全策略升级到最新版本。

只使用推荐的密码和协议。

有关更多信息，请参阅 Elastic Load Balancing 的侦听器配置。

其他资源

- 侦听器配置快速参考
- 更新负载均衡器的 SSL 协商配置
- Elastic Load Balancing 的 SSL 协商配置
- SSL 安全策略表

报告列

- 状态
- 区域
- 负载均衡器名称
- 负载均衡器端口
- Reason

ELB 安全组

描述

检查配置了缺失安全组，或者允许访问未针对负载均衡器配置的端口的安全组的负载均衡器。

如果删除与某个负载均衡器关联的安全组，则负载均衡器将无法按预期工作。如果安全组允许访问未针对负载均衡器配置的端口，则数据丢失或恶意攻击的风险会增加。

检查 ID

`xSqX82fQu`

提醒条件

- 黄色：与负载均衡器关联的 Amazon VPC 安全组的入站规则允许访问未在负载均衡器的侦听器配置中定义的端口。
- 红色：与负载均衡器关联的安全组不存在。

Recommended Action（建议的操作）

配置安全组规则，以将访问限制在负载均衡器侦听器配置中定义的端口和协议，以及用于支持路径 MTU 发现的 ICMP 协议。请参阅经典负载均衡器的侦听器和 VPC 中的负载均衡器的安全组。

如果安全组缺失，请将新安全组应用到负载均衡器。创建安全组规则，将访问限制在负载均衡器侦听器配置中定义的端口和协议。请参阅 VPC 中的负载均衡器的安全组。

其他资源

- Elastic Load Balancing 用户指南
- 配置经典负载均衡器

报告列

- 状态
- 区域
- 负载均衡器名称
- 安全组 ID
- Reason

Exposed Access Keys

描述

检查常用代码存储库是否存在已向公共暴露的访问密钥，以及可能由于访问密钥泄露而导致的不规则 Amazon Elastic Compute Cloud (Amazon EC2) 使用。

访问密钥包含访问密钥 ID 和相应的秘密访问密钥。访问密钥被暴露对您的账户和其他用户构成安全风险，可能导致未经授权的活动或滥用行为造成费用过高，并违反 AWS客户协议。

如果您的访问密钥暴露，请立即采取措施保护您的账户。为了保护您的账户免于产生过高的费用，AWS 会暂时限制您创建一些 AWS 资源的能力。这并不能使您的账户安全。它仅部分限制了您可能需要付费的未经授权的使用。

> **Note**
>
> 此检查并不保证能识别暴露的访问密钥或被泄露的 EC2 实例。您对访问密钥和 AWS 资源的安全和安全性负最终责任。
> 此检查的结果将自动刷新，并且不允许刷新请求。当前，您无法从此检查中排除资源。

如果访问密钥显示截止日期，且在该日期后未授权使用仍未停止，那么 AWS 可能会暂停您的 AWS 账户。如果您认为收到了错误的提醒，请联系 AWS Support。

Trusted Advisor 中显示的信息可能无法反映您账户的最新状态。除非账户中所有泄露的访问密钥都已得到解决，否则任何已泄露的访问密钥均不会标记为已解决。此类数据同步最多可能需要一周时间。

检查 ID

`12Fnkpl8Y5`

提醒条件

- 红色：可能已遭盗用 – AWS 已确定访问密钥 ID 和相应的秘密访问密钥已在互联网上泄露且可能已遭盗用（已使用）。
- 红色：已泄露 – AWS 已确定访问密钥 ID 和相应的秘密访问密钥已在互联网上泄露。
- 红色：疑似盗用 – Amazon EC2 出现异常使用情况，访问密钥可能已遭盗用，但尚未确定已在互联网上泄露。

Recommended Action（建议的操作）

尽快删除受影响的访问密钥。如果此密钥与 IAM 用户关联，请参阅管理对 IAM 用户的访问密钥。

检查您的账户是否存在未授权使用情况。登录到 AWS Management Console，检查每个服务控制台是否存在可疑资源。请特别注意运行中的 Amazon EC2 实例、竞价型实例请求、访问密钥和 IAM 用户。您也可以在账单与成本管理控制台上检查总体使用情况。

其他资源

- 有关管理 AWS 访问密钥的最佳实践
- AWS 安全审计指南

报告列

- 访问密钥 ID
- 用户名（IAM 或根用户）
- 欺诈类型
- 案例 ID
- 更新时间
- 位置
- 截止日期
- 使用量（美元/天）

IAM 访问密钥轮换

描述

检查过去 90 天内未轮换的活动 IAM 访问密钥。

定期轮换访问密钥时，您可以减少在您不知情的情况下使用泄漏的密钥访问资源的可能性。出于此检查的目的，上次轮换日期和时间是创建或最近激活访问密钥的时间。访问密钥编号和日期来自最新 IAM 凭证报告中的 `access_key_1_last_rotated` 和 `access_key_2_last_rotated` 信息。

由于凭证报告的重新生成频率受到限制，刷新此检查可能不会反映最近的变化。有关详细信息，请参阅获取您 AWS 账户 的凭证报告。

为了创建和轮换访问密钥，用户必须具有相应的权限。有关更多信息，请参阅允许用户管理自己的密码、访问密钥和 SSH 密钥。

检查 ID

`DqdJqYeRm5`

提醒条件

- 绿色：访问密钥处于活跃状态且已在过去 90 天内轮换。

- 黄色：访问密钥处于活跃状态且已在过去 2 年内轮换，但距今已超过 90 天。
- 红色：访问密钥处于活跃状态，但在过去 2 年内未进行轮换。

Recommended Action（建议的操作）

定期轮换访问密钥。请参阅轮换访问密钥和管理 IAM 用户的访问密钥。

其他资源

- IAM 最佳实践
- 如何轮换 IAM 用户的访问密钥

报告列

- 状态
- IAM 用户
- 访问密钥
- 上次轮换的密钥
- Reason

IAM 密码策略

描述

检查账户的密码策略，并在未启用密码策略或未启用密码内容要求时发出警告。

密码内容要求通过强制创建强用户密码提高了 AWS 环境的整体安全性。若您创建或更改密码策略，将会立即对新用户强制执行更改，但不会要求现有用户更改其密码。

检查 ID

Yw2K9puPzl

提醒条件

- 黄色：密码策略已启用，但至少有一项内容要求未启用。
- 红色：未启用密码策略。

Recommended Action（建议的操作）

如果部分内容要求未启用，请考虑进行启用。如果未启用任何密码策略，请创建并配置策略。请参阅为 IAM 用户设置账户密码策略。

其他资源

管理密码

报告列

- 密码策略
- 大写
- 小写
- 数字
- 非字母数字

IAM 使用

描述

检查您的 IAM 使用情况。您可以使用 IAM 在 AWS 中创建用户、群组和角色。您还可以使用权限来控制对 AWS 资源的访问。此检查旨在通过检查是否至少存在一个 IAM 用户来阻止使用根访问权限。如果您

遵循在身份提供者或 AWS IAM Identity Center (successor to AWS Single Sign-On) 中集中身份和配置用户的最佳实践，则可以忽略此提醒。

检查 ID

zXCkfM1nI3

提醒条件

黄色：没有为此账户创建 IAM 用户。

Recommended Action（建议的操作）

创建 IAM 用户或使用 AWS IAM Identity Center (successor to AWS Single Sign-On) 创建其他用户，将其权限限制为在您的 AWS 环境中执行特定任务。

其他资源

- 什么是 AWS IAM Identity Center (successor to AWS Single Sign-On)？
- 什么是 IAM？

根账户的 MFA

描述

检查根账户，如果未启用多重身份验证 (MFA)，则发出警告。

为了提高安全性，我们建议您使用 MFA 来保护您的账户，这要求用户在与 AWS Management Console 和相关网站交互时，输入您的 MFA 硬件或虚拟设备提供的唯一身份验证代码。

检查 ID

7DAFEmoDos

提醒条件

红色：未在根账户上启用 MFA。

Recommended Action（建议的操作）

登录根账户并激活 MFA 设备。请参阅检查 MFA 状态和设置 MFA 设备。

其他资源

在 AWS 中使用多重身份验证（MFA）

安全组 – 不受限制的特定端口

描述

检查安全组是否有允许对特定端口进行不受限制访问 (0.0.0.0/0) 的规则。

不受限制的访问增加了恶意活动（黑客denial-of-service攻击、攻击和丢失数据的机会。风险最高的端口标记为红色，风险较小的端口将标记为黄色。标记为绿色的端口通常由需要不受限制访问的应用程序使用，例如 HTTP 和 SMTP。

如果您故意通过这种方式配置了安全组，我们建议您使用其他安全措施来保护您的基础设施（如 IP 表）。

Note

此检查仅评估您创建的安全组及其 IPv4 地址的入站规则。AWS Directory Service 创建的安全组标记为红色或黄色，但它们不会构成安全风险，并且可能会安全地被忽略或被排除在外。有关更多信息，请参阅 Trusted Advisor 常见问题。

检查 ID

HCP4007jGY

提醒条件

- 绿色：访问端口 80、25、443 或 465 不受限制。
- 红色：访问端口 20、21、1433、1434、3306、3389、4333、5432 或 5500 不受限制。
- 黄色：访问任何其他端口不受限制。

Recommended Action（建议的操作）

只有具有此需求的 IP 地址才能访问。要只允许特定 IP 地址进行访问，请将后缀设置为 /32（例如，192.0.2.10/32）。在创建更加严格的规则后，请务必删除过于宽松的规则。

其他资源

- Amazon EC2 安全组

  TCP 和 UDP 端口号列表
- 无类域间路由

报告列

- 状态
- 区域
- 安全组名称
- 安全组 ID
- 协议
- 起始端口
- 终止端口

安全组 – 不受限制的访问

描述

检查安全组是否存在允许不受限制地访问资源的规则。

不受限制的访问增加了恶意活动（黑客denial-of-service攻击、攻击和丢失数据的机会。

> **Note**
>
> 此检查仅评估您创建的安全组及其 IPv4 地址的入站规则。AWS Directory Service 创建的安全组标记为红色或黄色，但它们不会构成安全风险，并且可能会安全地被忽略或被排除在外。有关更多信息，请参阅 Trusted Advisor 常见问题。

检查 ID

1iG5NDGVre

提醒条件

红色：安全组规则有一个后缀为 /0 的源 IP 地址，该后缀可用于 25、80 或 443 以外的端口。

Recommended Action（建议的操作）

只有具有此需求的 IP 地址才能访问。要只允许特定 IP 地址进行访问，请将后缀设置为 /32（例如，192.0.2.10/32）。在创建更加严格的规则后，请务必删除过于宽松的规则。

其他资源

- Amazon EC2 安全组
- 无类域间路由

报告列

- 状态
- 区域
- 安全组名称
- 安全组 ID
- 协议
- 起始端口
- 终止端口
- IP 范围

容错能力

您可以使用以下容错类别检查。

检查名称

- Amazon Aurora 数据库实例可访问性 (p. 109)
- Amazon Comprehend 端点访问风险 (p. 109)
- Amazon EBS 快照 (p. 110)
- Amazon EC2 可用区平衡 (p. 111)
- 使用单一可用区的亚马逊 ECS 服务 (p. 111)
- 亚马逊 ECS 多可用区放置策略 (p. 112)
- 单个可用区中运行 HSM 实例的 AWS CloudHSM 集群 (p. 113)
- 事件管理器复制集AWS 区域中的数量 (p. 113)
- Amazon ElastiCache 多可用区集群 (p. 114)
- Amazon MemoryDB 多可用区集群 (p. 114)
- Amazon RDS 备份 (p. 115)
- Amazon RDS Multi-AZ (p. 115)
- 违反 AWS Resilience Hub 策略 (p. 116)
- AWS Resilience Hub 恢复能力评分 (p. 117)
- AWS Resilience Hub评估年龄 (p. 117)
- Amazon Route 53 已删除运行状况检查 (p. 118)
- Amazon Route 53 故障转移资源记录集 (p. 118)
- Amazon Route 53 高 TTL 资源记录集 (p. 119)
- Amazon Route 53 域名服务器委托 (p. 120)
- Amazon S3 存储桶日志记录 (p. 120)
- Amazon S3 Bucket Versioning (p. 121)
- Auto Scaling 组运行状况检查 (p. 122)
- Auto Scaling 组资源 (p. 123)
- AWS Direct Connect 连接冗余 (p. 123)
- AWS Direct Connect 位置冗余 (p. 124)
- AWS Direct Connect 虚拟接口冗余 (p. 125)
- 无多可用区冗余的 AWS Lambda VPC 支持的函数 (p. 125)
- AWS Well-Architected 可靠性高风险问题 (p. 126)
- ELB Connection Draining (p. 127)
- ELB 跨区域负载均衡 (p. 127)

- 负载均衡器优化 (p. 128)
- VPN 隧道冗余 (p. 128)
- NAT 网关可用区独立性 (p. 129)
- 单一可用区应用程序检查 (p. 130)
- ActiveMQ 可用区冗余 (p. 130)
- RabbitMQ 可用区冗余 (p. 131)
- 亚马逊 EFS 无装载目标冗余 (p. 131)

Amazon Aurora 数据库实例可访问性

描述

检查 Amazon Aurora 数据库集群同时具有私有实例和公有实例的情况。

如果主实例故障，则副本实例可提升为主实例。如果该副本实例是私有的，则只具有公有访问权限的用户将无法在故障转移后连接到数据库。我们建议集群中的所有数据库实例具有相同的可访问性。

检查 ID

```
xuy7H1avtl
```

提醒条件

黄色：Aurora 数据库集群中的实例具有不同的可访问性（公有和私有混合）。

Recommended Action（建议的操作）

修改数据库集群中实例的 `Publicly Accessible` 设置，以便将所有实例设置为公有或私有。有关详细信息，请参阅修改运行 MySQL 数据库引擎的数据库实例中有关 MySQL 实例的说明。

其他资源

Aurora 数据库集群的容错能力

报告列

- 状态
- 区域
- 集群
- 公有数据库实例
- 私有数据库实例
- Reason

Amazon Comprehend 端点访问风险

描述

检查其中使用客户托管式密钥加密基础模型的端点的 AWS Key Management Service (AWS KMS) 密钥权限。如果禁用了客户托管式密钥，或者更改了密钥策略以针对 Amazon Comprehend 更改允许的权限，则端点可用性可能会受到影响。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

```
Cm24dfsM13
```

提醒条件

红色：客户托管式密钥已禁用或者密钥策略已更改以改变 Amazon Comprehend 允许的访问权限。

Recommended Action（建议的操作）

如果客户托管式密钥已禁用，我们建议您启用它。有关更多信息，请参阅启用密钥。如果密钥策略已更改并且您想要继续使用端点，我们建议您更新 AWS KMS 密钥策略。有关更多信息，请参阅更改密钥政策。

其他资源

AWS KMS 密钥加密权限

报告列

- 状态
- 区域
- 端点 ARN
- 模型 ARN
- KMS KeyId
- 上次更新时间

Amazon EBS 快照

描述

检查 Amazon Elastic Block Store (Amazon EBS) 卷（可用或正在使用）的快照的使用期限。

即使复制了 Amazon EBS 卷，也可能会发生故障。快照会保存到亚马逊简单存储服务 (Amazon S3)，以实现持久存储和point-in-time恢复。

检查 ID

`H7IgTzjTYb`

提醒条件

- 黄色：最新的卷快照在 7 到 30 天之间。
- 红色：最新的卷快照超过 30 天。
- 红色：卷没有快照。

Recommended Action（建议的操作）

每周或每月为卷创建一次快照。有关更多信息，请参阅创建 Amazon EBS 快照。

其他资源

Amazon Elastic Block Store (Amazon EBS)

报告列

- 状态
- 区域
- 卷 ID
- 卷名
- 快照 ID
- 快照名称
- 快照期限
- 卷附件

- Reason

Amazon EC2 可用区平衡

描述

检查 Amazon Elastic Compute Cloud (Amazon EC2) 实例在一个区域的可用区之间的分布。

可用区的位置各不相同，用于隔离其他可用区的故障。相同区域中的可用区之间通过廉价、低延迟的网络相连。通过启动相同区域中的多个可用区内的实例，您可以保护您的应用程序不受单点故障的影响。

检查 ID

`wuy7G1zxql`

提醒条件

- 黄色：区域在多个区有实例，但分配不平均（使用的可用区中的最多实例和最少实例的数量相差超过 20%）。
- 红色：区域只在单个可用区有实例。

Recommended Action（建议的操作）

在多个可用区之间平均分配 Amazon EC2 实例。您可以手动启动实例或使用 Auto Scaling 自动进行来实现此操作。有关更多信息，请参阅启动实例和对您的自动扩缩组进行负载均衡。

其他资源

Amazon EC2 Auto Scaling 用户指南

报告列

- 状态
- 区域
- a 区实例
- b 区实例
- c 区实例
- e 区实例
- f 区实例
- Reason

使用单一可用区的亚马逊 ECS 服务

描述

检查您的服务配置是否使用单个可用区 (AZ)。

可用区是不受其他区域故障影响的独特位置。这支持在同一AWS 区域可用区之间进行廉价、低延迟的网络连接。通过在同一地区的多个可用区中启动实例，您可以帮助保护您的应用程序免受单点故障的影响。

> **Note**
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`c1z7dfpz01`

提醒条件

- 黄色：Amazon ECS 服务正在单个可用区中运行所有任务。
- 绿色：Amazon ECS 服务正在至少两个不同的可用区中运行任务。

Recommended Action（建议的操作）

在不同的可用区中为服务至少再创建一个任务。

其他资源

亚马逊 ECS 容量和可用性

报告列

- 状态
- 区域
- ECS 集群名称/ECS 服务名称
- 可用区数量
- 上次更新时间

亚马逊 ECS 多可用区放置策略

描述

检查您的 Amazon ECS 服务是否使用了基于可用区的分散放置策略。此策略在同一可用区 (AZ) 之间分配任务AWS 区域，可以帮助保护您的应用程序免受单点故障的影响。

对于作为 Amazon ECS 服务的一部分运行的任务，spread 是默认的任务放置策略。

该检查还会验证价差是您的启用投放策略列表中的第一个或唯一的策略。

> **Note**
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

```
c1z7dfpz02
```

提醒条件

- 黄色：按可用区分散已禁用或不是您的 Amazon ECS 服务已启用放置策略列表中的第一个策略。
- 绿色：按可用区域分散是您的已启用放置策略列表中的第一个策略，或者是为您的 Amazon ECS 服务启用的唯一放置策略。

Recommended Action（建议的操作）

启用分散任务放置策略，将任务分配到多个可用区。验证按可用区分散是所有已启用的任务放置策略的第一策略还是使用的唯一策略。如果您选择管理可用区放置，则可以在其他可用区使用镜像服务来降低这些风险。

其他资源

亚马逊 ECS 任务放置策略

报告列

- 状态
- 区域
- ECS 集群名称/ECS 服务名称
- 分散任务放置策略已启用并正确应用
- 上次更新时间

单个可用区中运行 HSM 实例的 AWS CloudHSM 集群

描述

检查在单个可用区（AZ）中运行 HSM 实例的集群。如果集群存在没有最新备份的风险，则此检查会提示您。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`hc0dfs7601`

提醒条件

- 黄色：CloudHSM 集群在单个可用区中运行所有 HSM 实例的时间超过 1 小时。
- 绿色：CloudHSM 集群在至少两个不同的可用区中运行所有 HSM 实例。

Recommended Action（建议的操作）

为不同的可用区中的集群至少再创建一个实例。

其他资源

适用于 AWS CloudHSM 的最佳实践

报告列

- 状态
- 区域
- 集群 ID
- HSM 实例的数量
- 上次更新时间

事件管理器复制集AWS 区域中的数量

描述

检查 Incident Manager 复制集的配置是否使用多个AWS 区域来支持区域故障转移和响应。对于由CloudWatch警报或EventBridge事件创建的事件，事件管理器会创建与警报或事件规则AWS 区域相同的事件。如果事件管理器在该区域暂时不可用，则系统会尝试在复制集的另一个区域创建事件。如果复制集仅包含一个区域，则在 Icident Manager 不可用时，系统将无法创建事件记录。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`cIdfp1js9r`

提醒条件

- 绿色：复制集包含多个区域。
- 黄色：复制集包含一个区域。

Recommended Action（建议的操作）

至少再向复制集中再添加一个区域。

其他资源

有关更多信息，请参阅跨区域事件管理。

报告列

- 状态
- 多区域
- 复制集
- 上次更新时间

Amazon ElastiCache 多可用区集群

描述

检查部署在单个可用区（AZ）中的 ElastiCache 集群。如果集群中的多可用区处于非活动状态，则此检查会提示您。

在多个可用区中部署可异步复制到不同可用区中的只读副本，从而增强 ElastiCache 集群可用性。当发生计划内集群维护或主节点不可用时，ElastiCache 会自动将副本提升为主节点。这种失效转移允许恢复集群写入操作，并且不需要管理员干预。

> Note
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`ECHdfsQ402`

提醒条件

- 绿色：集群中的多可用区处于活动状态。
- 黄色：集群中的多可用区处于非活动状态。

Recommended Action（建议的操作）

在与主分片不同的可用区中，每个分片至少创建一个副本。

其他资源

有关更多信息，请参阅通过多可用区最大程度地减少 ElastiCache for Redis 的停机时间。

报告列

- 状态
- 区域
- 集群名称
- 上次更新时间

Amazon MemoryDB 多可用区集群

描述

检查部署在单个可用区（AZ）中的 MemoryDB 集群。如果集群中的多可用区处于非活动状态，则此检查会提示您。

在多个可用区中部署可异步复制到不同可用区中的只读副本，从而增强 MemoryDB 集群可用性。当发生计划内集群维护或主节点不可用时，MemoryDB 会自动将副本提升为主节点。这种失效转移允许恢复集群写入操作，并且不需要管理员干预。

> Note
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

MDBdfsQ401

提醒条件

- 绿色：集群中的多可用区处于活动状态。
- 黄色：集群中的多可用区处于非活动状态。

Recommended Action（建议的操作）

在与主分片不同的可用区中，每个分片至少创建一个副本。

其他资源

有关更多信息，请参阅 Minimizing downtime in MemoryDB with Multi-AZ（通过多可用区最大程度地减少 MemoryDB 停机时间）。

报告列

- 状态
- 区域
- 集群名称
- 上次更新时间

Amazon RDS 备份

描述

检查 Amazon RDS 数据库实例的自动备份。

默认情况下，启用备份，保留期为一天。备份降低了意外数据丢失的风险并允许point-in-time恢复。

检查 ID

opQPADkZvH

提醒条件

红色：数据库实例将备份保留期设置为 0 天。

Recommended Action（建议的操作）

根据您的应用程序的要求，将数据库实例的自动备份的保留期设置为 1 到 35 天。请参阅使用自动备份。

其他资源

Amazon RDS 入门

报告列

- 状态
- 区域/可用区
- 数据库实例
- VPC ID
- 备份保留期

Amazon RDS Multi-AZ

描述

检查部署在单个可用区 (AZ) 中的数据库实例。

多可用区部署通过同步复制到不同可用区中的备用实例，增强数据库可用性。在计划的数据库维护期间，或在数据库实例或可用区发生故障时，Amazon RDS 会自动将故障转移到备用实例。通过此故障转移，数据库操作将快速恢复，无需管理干预。由于 Amazon RDS 不支持 Microsoft SQL Server 的多可用区部署，因此此检查不会检查 SQL Server 实例。

检查 ID

`f2iK5R6Dep`

提醒条件

黄色：在单个可用区中部署数据库实例。

Recommended Action（建议的操作）

如果您的应用程序要求高可用性，请将您的数据库实例修改为启用多可用区部署。请参阅高可用性（多可用区）。

其他资源

区域和可用区

报告列

- 状态
- 区域/可用区
- 数据库实例
- VPC ID
- 多可用区

违反 AWS Resilience Hub 策略

描述

针对未达到策略定义的恢复时间目标（RTO）和恢复点目标（RPO）的应用程序检查 Resilience Hub。如果应用程序未达到您在 Resilience Hub 中为应用程序设置的 RTO 和 RPO 目标，则此检查会提示您。

Note

此检查的结果会自动刷新，不允许刷新请求。当前，您无法从此检查中排除资源。

检查 ID

`RH23stmM02`

提醒条件

- 绿色：应用程序拥有策略并且符合 RTO 和 RPO 目标。
- 黄色：应用程序尚未经过评估。
- 红色：应用程序拥有策略但未达到 RTO 和 RPO 目标。

Recommended Action（建议的操作）

登录 Resilience Hub 控制台并查看建议，以便应用程序达到 RTO 和 RPO 目标。

其他资源

Resilience Hub 概念

报告列

- 状态
- 区域
- Application Name

- 上次更新时间

AWS Resilience Hub 恢复能力评分

描述

检查您是否对 Resilience Hub 中的应用程序进行了评估。如果恢复能力评分低于特定值，则此检查会提示您。

Note

此检查的结果会自动刷新，不允许刷新请求。当前，您无法从此检查中排除资源。

检查 ID

`RH23stmM01`

提醒条件

- 绿色：应用程序的恢复能力评分为 70 或更高。
- 黄色：应用程序的恢复能力评分为 40 到 69。
- 黄色：应用程序尚未经过评估。
- 红色：应用程序的恢复能力评分低于 40。

Recommended Action（建议的操作）

登录 Resilience Hub 控制台并对应用程序进行评估。查看建议以提高恢复能力评分。

其他资源

Resilience Hub 概念

报告列

- 状态
- 区域
- Application Name
- 应用程序恢复能力评分
- 上次更新时间

AWS Resilience Hub评估年龄

描述

检查自您上次运行应用程序评估以来有多长时间。如果您在指定天数内没有运行应用程序评估，此检查会提醒您。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`RH23stmM03`

提醒条件

- 绿色：您的应用程序评估在过去 30 天内运行。
- 黄色：您的应用程序评估在过去 30 天内未运行。

Recommended Action（建议的操作）

登录 Resilience Hub 控制台并对应用程序进行评估。

其他资源

Resilience Hub 概念

报告列

- 状态
- 区域
- Application Name
- 自上次评估运行以来的天数
- 上次评估运行时间
- 上次更新时间

Amazon Route 53 已删除运行状况检查

描述

检查与已删除的运行状况检查关联的资源记录集。

Route 53 不会禁止您删除与一个或多个资源记录集关联的运行状况检查。如果您删除运行状况检查而不更新关联的资源记录集，则 DNS 故障转移配置的 DNS 查询路由将无法按预期运行。

AWS 服务创建的托管区域将不会显示在您的检查结果中。

检查 ID

`Cb877eB72b`

提醒条件

黄色：资源记录集与已删除的运行状况检查关联。

Recommended Action（建议的操作）

创建新的运行状况检查，并将其与资源记录集关联。请参阅创建、更新和删除运行状况检查和为资源记录集添加运行状况检查。

其他资源

- Amazon Route 53 运行状况检查和 DNS 故障转移
- 简单 Amazon Route 53 配置中的运行状况检查的工作原理

报告列

- 托管区域名称
- 托管区域 ID
- 资源记录集名称
- 资源记录集类型
- 资源记录集标识符

Amazon Route 53 故障转移资源记录集

描述

检查具有错误配置的 Amazon Route 53 故障转移资源记录集。

当 Amazon Route 53 运行状况检查确定主资源运行状况不佳时，Amazon Route 53 会使用辅助备份资源记录集响应查询。您必须创建正确配置的主资源记录集和辅助资源记录集，以便进行故障转移。

AWS 服务创建的托管区域将不会显示在您的检查结果中。

检查 ID

b73EEdD790

提醒条件

- 黄色：主要失效转移资源记录集没有对应的辅助资源记录集。
- 黄色：辅助失效转移资源记录集没有对应的主要资源记录集。
- 黄色：具有相同名称的主辅资源记录集与同一个运行状况检查关联。

Recommended Action（建议的操作）

如果失效转移资源集缺失，则创建相应的资源记录集。请参阅创建失效转移资源记录集。

如果您的资源记录集与同一个运行状况检查关联，则为其创建单独的运行状况检查。请参阅创建、更新和删除运行状况检查。

其他资源

Amazon Route 53 运行状况检查和 DNS 故障转移

报告列

- 托管区域名称
- 托管区域 ID
- 资源记录集名称
- 资源记录集类型
- Reason

Amazon Route 53 高 TTL 资源记录集

描述

检查是否有资源记录集可以从较低 time-to-live (TTL) 值中受益。

TTL 指的是 DNS 解析程序缓存资源记录集的秒数。当您指定长 TTL 时，DNS 解析程序需要更长的时间来请求更新的 DNS 记录，这可能会导致重新路由流量发生不必要的延迟。例如，长 TTL 会导致 DNS 故障转移检测到终端节点故障与通过重新路由流量作出响应之间产生延迟。

AWS 服务创建的托管区域将不会显示在您的检查结果中。

检查 ID

C056F80cR3

提醒条件

- 黄色：路由策略为“失效转移”的资源记录集有超过 60 秒的 TTL。
- 黄色：含关联运行状况检查的资源记录集有超过 60 秒的 TTL。

Recommended Action（建议的操作）

为列出的资源记录集输入 60 秒的 TTL 值。有关更多信息，请参阅使用资源记录集。

其他资源

Amazon Route 53 运行状况检查和 DNS 故障转移

报告列

- 状态
- 托管区域名称
- 托管区域 ID
- 资源记录集名称
- 资源记录集类型

- 资源记录集 ID
- TTL

Amazon Route 53 域名服务器委托

描述

检查您的域注册商或 DNS 未使用正确的 Route 53 名称服务器的 Amazon Route 53 托管区域。

当您创建托管区域时，Route 53 将会分配一组四个委托名称服务器。这些服务器的名称为 ns-###.awsdns-##.com、.net、.org 和 .co.uk，其中 ### 和 ## 通常表示不同的数字。在 Route 53 为您的域路由 DNS 查询之前，您必须更新注册商的域名服务器配置以删除注册商分配的名称服务器。然后，您必须在 Route 53 委托集中添加所有四个名称服务器。为了获得最大的可用性，您必须添加所有四个 Route 53 名称服务器。

AWS 服务创建的托管区域不会显示在您的检查结果中。

检查 ID

```
cF171Db240
```

提醒条件

黄色：有托管区的域注册器并未使用委托集中的全部四个 Route 53 名称服务器。

Recommended Action（建议的操作）

通过注册器或域当前的 DNS 服务添加或更新名称服务器记录，以将全部四个名称服务器包含在 Route 53 委托集中。要找到这些值，请参阅获取托管区域的名称服务器。有关添加或更新名称服务器记录的信息，请参阅创建域和子域并迁移到 Amazon Route 53。

其他资源

使用托管区域

报告列

- 托管区域名称
- 托管区域 ID
- 使用的名称服务器委托数量

Amazon S3 存储桶日志记录

描述

检查 Amazon Simple Storage Service (Amazon S3) 存储桶的日志记录配置。

启用服务器访问日志记录后，每小时将详细的访问日志传送到您选择的存储桶。访问日志记录包含与每个请求有关的详细信息，如请求类型、请求中指定的资源和请求的处理时间和日期。默认情况下，存储桶日志记录未启用。如果要执行安全审核或了解有关用户和使用模式的详细信息，则应启用日志记录。

初次启用日志记录时，系统会自动验证配置。但是，将来的修改可能会导致日志记录失败。此检查将检查显式 Amazon S3 存储桶权限，但不会检查可能覆盖存储桶权限的关联存储桶策略。

检查 ID

```
BueAdJ7NrP
```

提醒条件

- 黄色：存储桶没有启用服务器访问日志记录。
- 黄色：目标存储桶权限不包括根账户，所以 Trusted Advisor 无法对其进行检查。

- 红色：目标存储桶不存在。
- 红色：目标存储桶和源存储桶的拥有者不同。
- 红色：日志提交者没有目标存储桶的写入权限。

Recommended Action（建议的操作）

为大多数存储桶启用存储桶日志记录。请参阅使用控制台启用日志记录和以编程方式启用日志记录。

如果目标存储桶权限不包括根账户，并且您希望 Trusted Advisor 检查日志记录状态，则将根账户添加为被授权者。请参阅编辑存储桶权限。

如果目标存储桶不存在，请选择现有存储桶作为目标，或创建一个新存储桶，然后选择它。请参阅管理存储桶日志记录。

如果目标存储桶和源存储桶的拥有者不同，请将目标存储桶更改为拥有者与源存储桶相同的存储桶。请参阅管理存储桶日志记录。

如果日志提交者没有目标存储桶的写入权限（写入权限未启用），请向日志提交组授予上传/删除权限。请参阅编辑存储桶权限。

其他资源

- 使用存储桶
- 服务器访问日志记录
- 服务器访问日志格式
- 删除日志文件

报告列

- 状态
- 区域
- 存储桶名称
- 目标名称
- 目标存在
- 拥有者相同
- 写权限已启用
- Reason

Amazon S3 Bucket Versioning

描述

检查未启用版本控制或已暂停版本控制的 Amazon Simple Storage Service 存储桶。

启用版本控制时，您可以轻松从用户意外操作和应用程序故障中恢复数据。对于存储桶中存储的每个对象，您可以使用版本控制功能来保留、检索和还原它们的任何版本。通过自动将对象归档到 Glacier 存储类，您可以使用生命周期规则来管理对象的所有版本及其相关成本。还可以将规则配置为在指定时间段后删除对象的版本。对于对存储桶进行的任何对象删除或配置更改，您也可以要求进行多重身份验证 (MFA)。

版本控制在启用后无法被停用。但是，它可以暂停，从而防止创建新版本的对象。使用版本控制会增加 Amazon S3 的成本，因为您需要支付多个版本的对象的存储费用。

检查 ID

```
R365s2Qddf
```

提醒条件

- 绿色：存储桶已启用版本控制。

- 黄色：存储桶未启用版本控制。
- 黄色：存储桶已暂停版本控制。

Recommended Action（建议的操作）

在大多数存储桶中启用版本控制以防止意外删除或覆盖。请参阅使用版本控制和以编程方式启用版本控制。

如果存储桶版本控制已暂停，请考虑重新启用版本控制。有关使用已暂停版本控制的存储桶中的对象的信息，请参阅管理已暂停版本控制的存储桶中的对象。

当版本控制处于已启用或已暂停状态时，您可以定义生命周期配置规则来将某些对象版本标记为已过期，或永久删除不需要的对象版本。有关更多信息，请参阅对象生命周期管理。

当存储桶版本控制状态更改或当对象的版本删除时，MFA 删除需要进行额外的身份验证。它要求用户输入凭证和来自批准的身份验证设备的代码。有关更多信息，请参阅 MFA 删除。

其他资源

使用存储桶

报告列

- 状态
- 区域
- 存储桶名称
- 版本控制
- 已启用 MFA 删除

Auto Scaling 组运行状况检查

描述

检查 Auto Scaling 组的运行状况检查配置。

如果 Auto Scaling 组使用的是 Elastic Load Balancing，则建议的配置是启用 Elastic Load Balancing 运行状况检查。如果未使用 Elastic Load Balancing 运行状况检查，则 Auto Scaling 只能针对 Amazon Elastic Compute Cloud (Amazon EC2) 实例的运行状况进行检查。Auto Scaling 不会对实例上运行的应用程序执行操作。

检查 ID

`CL0G40CD08`

提醒条件

- 黄色：自动扩缩组有关联的负载均衡器，但 Elastic Load Balancing 运行状况检查未启用。
- 黄色：自动扩缩组没有关联的负载均衡器，但 Elastic Load Balancing 运行状况检查已启用。

Recommended Action（建议的操作）

如果自动扩缩组有关联的负载均衡器，但 Elastic Load Balancing 运行状况检查未启用，请参阅向自动扩缩组添加 Elastic Load Balancing 运行状况检查。

如果 Elastic Load Balancing 运行状况检查已启用，但没有负载均衡器与自动扩缩组关联，请参阅设置自动扩展且负载均衡的应用程序。

其他资源

Amazon EC2 Auto Scaling 用户指南

报告列

- 状态

- 区域
- 自动扩缩组名
- 关联的负载均衡器
- 运行状况检查

Auto Scaling 组资源

描述

检查与启动配置和 Auto Scaling 组关联的资源的可用性。

指向不可用资源的 Auto Scaling 组无法启动新的 Amazon Elastic Compute Cloud (Amazon EC2) 实例。如果配置正确，Auto Scaling 会在需求高峰期间无缝增加 Amazon EC2 实例的数量，并在需求平缓期间自动减少该数量。指向不可用资源的 Auto Scaling 组和启动配置不能按预期运行。

检查 ID

`8CNsSllI5v`

提醒条件

- 红色：自动扩缩组与删除的负载均衡器关联。
- 红色：启动配置与删除的 Amazon 机器映像（AMI）关联。

Recommended Action（建议的操作）

如果负载均衡器已删除，可以先创建一个新的负载均衡器，然后再创建一个包含此新负载均衡器的新自动扩缩组，也可以创建一个不包含负载均衡器的新自动扩缩组。有关创建包含新负载均衡器的新自动扩缩组的信息，请参阅设置自动扩展且负载均衡的应用程序。有关创建不包含负载均衡器的新自动扩缩组的信息，请参阅通过控制台开始使用 Auto Scaling 中的“创建自动扩缩组”。

如果 AMI 已删除，则使用有效的 AMI 创建新启动配置，然后将其与自动扩缩组关联。请参阅通过控制台开始使用 Auto Scaling 中的“创建启动配置”。

其他资源

- 对 Auto Scaling 进行问题排查：Amazon EC2 AMI
- 对 Auto Scaling 进行问题排查：负载均衡器配置
- Amazon EC2 Auto Scaling 用户指南

报告列

- 状态
- 区域
- 自动扩缩组名
- 启动类型
- 资源类型
- 资源名称

AWS Direct Connect 连接冗余

描述

检查只有一个 AWS Direct Connect 连接的 AWS 区域。连接到您的 AWS 资源应始终配置两个 Direct Connect 连接，以便在设备不可用时提供冗余。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。

检查 ID

`0t121N1Ty3`

提醒条件

黄色：AWS 区域 只有一个 AWS Direct Connect 连接。

Recommended Action（建议的操作）

在此 AWS 区域 中配置其他 Direct Connect 连接，以防止设备不可用。有关更多信息，请参阅使用 AWS Direct Connect 配置冗余连接。要防止站点不可用和添加位置冗余，请将其他 Direct Connect 连接配置到不同的 Direct Connect 位置。

其他资源

- AWS Direct Connect 入门
- AWS Direct Connect 常见问题

报告列

- 状态
- 区域
- 时间戳
- 位置
- 连接 ID

AWS Direct Connect 位置冗余

描述

检查具有一个或多个 AWS Direct Connect 连接且只有一个 AWS Direct Connect 位置的 AWS 区域。与您的 AWS 资源的连接应将 Direct Connect 连接配置到不同的 Direct Connect 位置，以便在位置不可用时提供冗余。

> Note
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。

检查 ID

`8M012Ph3U5`

提醒条件

黄色：AWS 区域 中的 Direct Connect 连接未配置到不同的位置。

Recommended Action（建议的操作）

配置使用不同 Direct Connect 位置的 Direct Connect 连接，以防止位置不可用。有关更多信息，请参见 AWS Direct Connect 入门。

其他资源

- AWS Direct Connect 入门
- AWS Direct Connect 常见问题

报告列

- 状态
- 区域
- 时间戳
- 位置

- 连接详细信息

AWS Direct Connect 虚拟接口冗余

描述

检查至少在两个 AWS Direct Connect 连接上未配置 AWS Direct Connect 虚拟接口 (VIF) 的虚拟私有网关。与虚拟私有网关的连接应将多个 VIF 配置在多个 Direct Connect 连接和位置间。这可以在设备或位置不可用时提供冗余。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。

检查 ID

`4g3Nt5M1Th`

提醒条件

黄色：虚拟私有网关的虚拟接口少于两个，或接口未配置给多个 Direct Connect 连接。

Recommended Action（建议的操作）

至少配置两个虚拟接口，并且将其配置给两个 Direct Connect 连接，以防止设备或位置不可用。请参阅创建虚拟接口。

其他资源

- AWS Direct Connect 入门
- AWS Direct Connect 常见问题
- 使用 AWS Direct Connect 虚拟接口

报告列

- 状态
- 区域
- 时间戳
- 网关 ID
- VIF 位置
- VIF 的连接 ID

无多可用区冗余的 AWS Lambda VPC 支持的函数

描述

检查单个可用区中易受服务中断影响的启用 VPC 的 Lambda 函数。建议将启用 VPC 的功能连接到多个可用区，以实现高可用性。

Note

此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`L4dfs2Q4C6`

提醒条件

黄色：连接到单个可用区中的子网的启用了 VPC 的 Lambda 函数。

Recommended Action（建议的操作）

在配置访问 VPC 的函数时，请选择多个可用区中的子网以确保高可用性。

其他资源

- 配置 Lambda 函数以访问 VPC 中的资源
- AWS Lambda 中的故障恢复能力

报告列

- 状态
- 区域
- 函数 ARN
- VPC ID
- 平均每日调用次数
- 上次更新时间

AWS Well-Architected 可靠性高风险问题

描述

对工作负载高风险问题（HRI）的可靠性支柱检查。此检查基于您的 AWS-Well Architected 审查。检查结果取决于您是否使用 AWS Well-Architected 完成了对工作负载的评估。

> **Note**
>
> 此检查的结果将每天自动刷新多次，并且不允许刷新请求。更改可能需要几个小时才能显示。当前，您无法从此检查中排除资源。

检查 ID

`Wxdfp4B1L4`

提醒条件

- 红色：在 AWS Well-Architected 的可靠性支柱中至少发现了一个活跃的高风险问题。
- 绿色：在 AWS Well-Architected 的可靠性支柱中未检测到活跃的高风险问题。

Recommended Action（建议的操作）

AWS Well-Architected 在工作负载评估过程中检测到高风险问题。这些问题为降低风险和节省资金提供了机会。登录 AWS Well-Architected 工具以查看您的答案并采取措施解决活跃的问题。

报告列

- 状态
- 区域
- 工作负载 ARN
- 工作负载名称
- 审核人姓名
- 工作负载类型
- 工作负载开始日期
- 工作负载上次修改日期
- 已确定的可靠性 HRI 数量
- 已解决的可靠性 HRI 数量
- 已回答的可靠性问题数量
- 可靠性支柱中的问题总数

- 上次更新时间

ELB Connection Draining

描述

检查没有启用连接耗尽的负载均衡器

当未启用连接耗尽并且您从负载均衡器取消注册 Amazon EC2 实例时，负载均衡器将停止将流量路由到该实例并关闭连接。启用连接耗尽后，负载均衡器将停止向已取消注册的实例发送新请求，但会保持连接打开以提供活动请求。

检查 ID

`7qGXsKIUw`

提醒条件

黄色：负载均衡器未启用连接耗尽。

Recommended Action（建议的操作）

为负载均衡器启用连接耗尽。有关更多信息，请参阅连接耗尽和为负载均衡器启用或禁用连接耗尽。

其他资源

Elastic Load Balancing 概念

报告列

- 状态
- 区域
- 负载均衡器名称
- Reason

ELB 跨区域负载均衡

描述

关闭跨区域负载均衡后，存在由于流量分布不均或后端过载而导致服务不可用的风险。当客户端错误地缓存 DNS 信息时，可能会出现此问题。当每个可用区中的实例数量不相等（例如，如果您已关闭某些实例以进行维护）时，也会出现此问题。

检查 ID

`xdeXZKIUy`

提醒条件

黄色：负载均衡器未启用跨区负载均衡。

Recommended Action（建议的操作）

确认负载均衡器中注册的 Amazon EC2 实例已在多个可用区中启动，然后再为负载均衡器启用跨区负载均衡。有关更多信息，请参阅可用区和区域和为负载均衡器启用或禁用跨区负载均衡。

其他资源

- 请求路由
- Elastic Load Balancing 概念

报告列

- 状态
- 区域

- 负载均衡器名称
- Reason

负载均衡器优化

描述

检查您的负载均衡器配置。

为了帮助在使用 Elastic Load Balancing 时提高 Amazon Elastic Compute Cloud (Amazon EC2) 的容错能力级别，我们建议在一个区域的多个可用区中运行相同数量的实例。配置的负载均衡器会产生费用，因此这也是成本优化检查。

检查 ID

`iqdCTZKCUp`

提醒条件

- 黄色：已为单个可用区启用负载均衡器。
- 黄色：已为没有活跃实例的可用区启用负载均衡器。
- 黄色：在负载均衡器注册的 Amazon EC2 实例未在可用区之间平均分配。（使用的可用区中的最高实例数与最低实例数之差大于 1，且差值大于最高数量的 20%。）

Recommended Action（建议的操作）

确保负载均衡器指向至少两个可用区内活跃并运行正常的实例。有关更多信息，请参见添加可用区。

如果负载均衡器配置的对象是没有正常运行实例的可用区，或者可用区之间的实例分配不均衡，请确定所有可用区是否都是必要的。删除所有不必要的可用区，并确保实例在其余可用区之间均衡分配。有关更多信息，请参阅删除可用区。

其他资源

- 可用区和区域
- 管理负载均衡器
- 评估 Elastic Load Balancing 的最佳实践

报告列

- 状态
- 区域
- 负载均衡器名称
- 区域数量
- a 区实例
- b 区实例
- c 区实例
- d 区实例
- e 区实例
- f 区实例
- Reason

VPN 隧道冗余

描述

检查每个 VPN 中处于活动状态的隧道数。

VPN 应始终配置两个隧道。这样可以在 AWS 终端节点的设备中断或计划进行维护时提供冗余。对于某些硬件，每次只有一个隧道处于活动状态。如果 VPN 没有活动隧道，可能仍会收取 VPN 费用。有关更多信息，请参阅 AWS Client VPN 管理员指南。

检查 ID

S45wrEXrLz

提醒条件

- 黄色：VPN 有一个活跃隧道（对于某些硬件来说这是正常情况）。
- 黄色：VPN 没有活跃隧道。

Recommended Action（建议的操作）

请确保为您的 VPN 连接配置两个隧道，并且两个都处于活跃状态（如果硬件支持）。如果您不再需要某个 VPN 连接，则可将其删除以避免收费。有关更多信息，请参阅您的客户网关或删除 VPN 连接。

其他资源

- AWS 站点到站点 VPN 用户指南
- 在您的 VPC 中添加硬件虚拟专用网关

报告列

- 状态
- 区域
- VPN ID
- VPC
- 虚拟专用网关
- 客户网关
- 活跃隧道
- Reason

NAT 网关可用区独立性

描述

检查您的 NAT 网关是否配置了独立于可用区 (AZ)。

NAT 网关使您的私有子网中的资源能够使用 NAT 网关的 IP 地址安全地连接到子网外的服务，并丢弃任何未经请求的入站流量。每个 NAT 网关都在指定的可用区 (AZ) 内运行，并且仅在该可用区内构建冗余。因此，您在特定可用区中的资源应使用同一可用区中的 NAT 网关，以便 NAT 网关或其可用区的任何潜在中断都不会影响您在其他可用区中的资源。

检查 ID

c1dfptbg10

提醒条件

- 红色：来自一个可用区内子网的流量正通过另一可用区中的 NATGW 路由。
- 绿色：来自您的子网位于一个可用区的流量正通过同一可用区中的 NATGW 路由。

Recommended Action（建议的操作）

请检查您的子网的可用区并通过同一 AZ 中的 NAT 网关路由流量。

如果 AZ 中没有 NATGW，请创建一个，然后通过它路由您的子网流量。

如果您在不同可用区的子网之间关联了相同的路由表，请将此路由表与与 NAT 网关位于同一可用区的子网相关联，对于另一可用区中的子网，请将单独的路由表与指向另一可用区中 NAT 网关的路由相关联。

我们建议为您的 Amazon VPC 中的架构更改选择维护窗口。

其他资源

- 如何创建 NAT 网关
- 如何为不同的 NAT 网关用例配置路由

报告列

- 状态
- 区域
- NAT 可用区
- NAT ID
- 子网可用区
- 子网 ID
- 路由表 ID
- NAT ARN
- 上次更新时间

单一可用区应用程序检查

描述

检查您的出口网络流量是否通过单个可用区 (AZ) 进行路由。

可用区是与其他区域隔绝任何冲击的独特位置。通过将服务分散到多个可用区，可以限制可用区故障的爆炸半径。

检查 ID

```
c1dfptbg11
```

提醒条件

- 黄色：根据观察到的出口网络模式，您的应用程序可能仅部署在一个可用区中。如果这是真的，并且您的应用程序需要高可用性，我们建议您预置应用程序资源并实施网络流以利用多个可用区。

Recommended Action（建议的操作）

如果您的应用程序需要高可用性，请考虑实施多可用区架构以提高可用性。

报告列

- 状态
- 区域
- VPC ID
- 上次更新时间

ActiveMQ 可用区冗余

描述

检查 Amazon MQ for ActiveMQ 代理是否已配置为具有高可用性，并在多个可用区中使用活动/备用代理。

检查 ID

```
c1t3k8mqv1
```

提醒条件

- 黄色：适用于 ActiveMQ 代理的亚马逊 MQ 是在单个可用区中配置的。

  绿色：在至少两个可用区中配置了适用于 ActiveMQ 的亚马逊 MQ 代理。

Recommended Action（建议的操作）

使用活动/备用部署模式创建新代理。

其他资源

- 创建 ActiveMQ 经纪人

报告列

- 状态
- 区域
- ActiveMQ 经纪人 ID
- 经纪人引擎类型
- 部署模式
- 上次更新时间

RabbitMQ 可用区冗余

描述

检查 Amazon MQ for RabbitMQ 代理是否已配置为在多个可用区使用集群实例实现高可用性。

检查 ID

```
c1t3k8mqv2
```

提醒条件

- 黄色：适用于 RabbitMQ 的亚马逊 MQ 代理是在单个可用区中配置的。

  绿色：在多个可用区中配置了适用于 RabbitMQ 的亚马逊 MQ 代理。

Recommended Action（建议的操作）

使用集群部署模式创建新代理。

其他资源

- 创建 RabbitMQ 经纪人

报告列

- 状态
- 区域
- RabbitMQ 经纪人 ID
- 经纪人引擎类型
- 部署模式
- 上次更新时间

亚马逊 EFS 无装载目标冗余

描述

检查 Amazon EFS 文件系统的多个可用区中是否存在装载目标。

可用区是与其他区域的故障隔离开来的独特位置。通过在一个 AWS 区域内多个地理上分隔的可用区中创建装载目标，您可以为您的 Amazon EFS 文件系统实现最高级别的可用性和持久性。

检查 ID

```
c1dfprch01
```

提醒条件

- 黄色：文件系统在单个可用区中创建了 1 个装载目标。

  绿色：文件系统在多个可用区中创建了 2 个或更多装载目标。

Recommended Action（建议的操作）

对于使用 One Zone 存储类的 EFS 文件系统，我们建议您通过恢复到新文件系统的备份来创建使用标准存储类的新文件系统。然后在多个可用区中创建装载目标。

对于使用标准存储类的 EFS 文件系统，我们建议您在多个可用区中创建装载目标。

其他资源

- 使用 Amazon EFS 控制台管理装载目标
- 亚马逊 EFS 配额和限制

报告列

- 状态
- 区域
- EFS 文件系统 ID
- 坐骑目标的数量
- 可用区数量
- 上次更新时间

Service Limits

请参阅以下有关服务限制（也称为配额）类别的检查。

此类别中的所有检查都有以下描述：

提醒条件

- 黄色：已达到限制的 80%。
- 红色：已达到限制的 100%。
- 蓝色：Trusted Advisor 无法检索一个或多个 AWS 区域 中的使用率或限制。

Recommended Action（建议的操作）

如果您预计超出服务限制，请直接从服务限额控制台请求增加。如果服务限额还不支持您的服务，则可以在支持中心创建未结支持案例。

报告列

- 状态
- 服务
- 区域
- 限制数量
- 当前使用量

Note

- 值基于快照，因此您的当前使用量可能会有所不同。配额和使用数据最长可能需要 24 小时才能反映出任何更改。在最近增加了配额的情况下，您可能会暂时发现利用率超出配额。

检查名称

- Auto Scaling 组 (p. 134)

- Auto Scaling 启动配置 (p. 134)
- CloudFormation 堆栈 (p. 134)
- DynamoDB 读取容量 (p. 134)
- DynamoDB 写入容量 (p. 135)
- EBS 活动快照 (p. 135)
- EBS 冷 HDD (sc1) 卷存储 (p. 135)
- EBS 通用型 SSD (gp2) 卷存储 (p. 135)
- EBS 通用型 SSD (gp3) 卷存储 (p. 136)
- EBS 磁介质（标准）卷存储 (p. 136)
- EBS 预置 IOPS (SSD) 卷聚合 IOPS (p. 136)
- EBS 预置 IOPS SSD (io1) 卷存储 (p. 136)
- EBS 预置 IOPS SSD (io2) 卷存储 (p. 136)
- EBS 吞吐量优化型 HDD (st1) 卷存储 (p. 137)
- EC2 按需实例 (p. 137)
- EC2 预留实例租赁 (p. 137)
- EC2-Classic 弹性 IP 地址 (p. 137)
- EC2-VPC 弹性 IP 地址 (p. 138)
- ELB Application Load Balancer (p. 138)
- ELB 经典负载均衡器 (p. 138)
- ELB Network Load Balancer (p. 138)
- IAM 组 (p. 138)
- IAM 实例配置文件 (p. 139)
- IAM policy (p. 139)
- IAM 角色 (p. 139)
- IAM 服务器证书 (p. 139)
- IAM 用户 (p. 140)
- 每个区域的 Kinesis 分区数 (p. 140)
- RDS 集群参数组 (p. 140)
- RDS 集群角色数 (p. 140)
- RDS 集群 (p. 140)
- RDS 数据库实例 (p. 141)
- RDS 数据库手动快照 (p. 141)
- RDS 数据库参数组 (p. 141)
- RDS 数据库安全组 (p. 141)
- RDS 事件订阅 (p. 142)
- 每个安全组的 RDS 最大身份验证次数 (p. 142)
- RDS 选项组 (p. 142)
- 每个主实例的 RDS 只读副本 (p. 142)
- RDS 预留实例 (p. 142)
- RDS 子网组 (p. 143)
- 每个子网组的 RDS 子网数 (p. 143)
- RDS 总存储配额 (p. 143)
- Route 53 托管区域 (p. 143)
- Route 53 最大运行状况检查次数 (p. 144)

- Route 53 可重用的委托集 (p. 144)
- Route 53 流量策略 (p. 144)
- Route 53 流量策略实例 (p. 144)
- SES 日发送配额 (p. 144)
- VPC (p. 145)
- VPC 互联网网关 (p. 145)

Auto Scaling 组

描述

检查使用量是否超过 Auto Scaling 组配额 80%。

检查 ID

`fW7HH017J9`

其他资源

Auto Scaling 配额

Auto Scaling 启动配置

描述

检查使用量是否超过 Auto Scaling 启动配置配额 80%。

检查 ID

`aW7HH017J9`

其他资源

Auto Scaling 配额

CloudFormation 堆栈

描述

检查使用量是否超过 CloudFormation CTACKS 配额的 80%。

检查 ID

`gW7HH017J9`

其他资源

AWS CloudFormation 配额

DynamoDB 读取容量

描述

检查使用量是否超过每个 AWS 账户 的读取次数的 DynamoDB 预置吞吐量限制的 80%。

检查 ID

`6gtQddfEw6`

其他资源

DynamoDB 配额

DynamoDB 写入容量

描述

检查使用量是否超过每个 AWS 账户 的写入次数的 DynamoDB 预置吞吐量限制的 80%。

检查 ID

`c5ftjdfkMr`

其他资源

DynamoDB 配额

EBS 活动快照

描述

检查使用量是否超过 EBS 活动快照配额的 80%。

检查 ID

`eI7KK0l7J9`

其他资源

Amazon EBS 限制

EBS 冷 HDD (sc1) 卷存储

描述

检查使用量是否超过 EBS 冷 HDD (sc1) 卷存储配额的 80%。

检查 ID

`gH5CC0e3J9`

其他资源

Amazon EBS 限制

EBS 通用型 SSD (gp2) 卷存储

描述

检查使用量是否超过 EBS 通用型 SSD (gp2) 卷存储配额的 80%。

检查 ID

`dH7RR0l6J9`

其他资源

Amazon EBS 限制

EBS 通用型 SSD (gp3) 卷存储

描述

检查使用量是否超过 EBS 通用型 SSD (gp3) 卷存储配额的 80%。

检查 ID

dH7RR0l6J3

其他资源

Amazon EBS 限制

EBS 磁介质（标准）卷存储

描述

检查使用量是否超过 EBS 磁性介质（标准）卷存储配额的 80%。

检查 ID

cG7HH0l7J9

其他资源

Amazon EBS 限制

EBS 预置 IOPS (SSD) 卷聚合 IOPS

描述

检查使用量是否超过 EBS 预置 IOPS (SSD) 卷聚合 IOPS 配额的 80%。

检查 ID

tV7YY0l7J9

其他资源

Amazon EBS 限制

EBS 预置 IOPS SSD (io1) 卷存储

描述

检查使用量是否超过 EBS 预置 IOPS SSD (io1) 卷存储配额的 80%。

检查 ID

gI7MM0l7J9

其他资源

Amazon EBS 限制

EBS 预置 IOPS SSD (io2) 卷存储

描述

检查使用量是否超过 EBS 预置 IOPS SSD (io2) 卷存储配额的 80%。

检查 ID

gI7MM0l7J2

其他资源

Amazon EBS 限制

EBS 吞吐量优化型 HDD (st1) 卷存储

描述

检查使用量是否超过 EBS 吞吐量优化 HDD (st1) 卷存储配额的 80%。

检查 ID

wH7DD0l3J9

其他资源

Amazon EBS 限制

EC2 按需实例

描述

检查使用量是否超过 EC2 按需实例配额的 80%。

检查 ID

0Xc6LMYG8P

其他资源

Amazon EC2 配额

EC2 预留实例租赁

描述

检查使用量是否超过 EC2 预留实例租赁配额的 80%。

检查 ID

iH7PP0l7J9

其他资源

Amazon EC2 配额

EC2-Classic 弹性 IP 地址

描述

检查使用量是否超过 EC2-Classic 弹性 IP 地址配额的 80%。

检查 ID

aW9HH0l8J6

其他资源

Amazon EC2 配额

EC2-VPC 弹性 IP 地址

描述

检查使用量是否超过 EC2-VPC 弹性 IP 地址配额的 80%。

检查 ID

`lN7RR0l7J9`

其他资源

VPC 弹性 IP 配额

ELB Application Load Balancer

描述

检查使用量是否超过 ELB Application Load Balancer 配额的 80%。

检查 ID

`EM8b3yLRTr`

其他资源

Elastic Load Balancing 配额

ELB 经典负载均衡器

描述

检查使用量是否超过 ELB 经典负载均衡器配额的 80%。

检查 ID

`iK7O0l7J9`

其他资源

Elastic Load Balancing 配额

ELB Network Load Balancer

描述

检查使用量是否超过 ELB Network Load Balancer 配额的 80%。

检查 ID

`8wIqYSt25K`

其他资源

Elastic Load Balancing 配额

IAM 组

描述

检查使用量是否超过 IAM 组配额的 80%。

检查 ID

sU7XX017J9

其他资源

IAM 配额

IAM 实例配置文件

描述

检查使用量是否超过 IAM 实例配置文件配额的 80%。

检查 ID

nO7SS017J9

其他资源

IAM 配额

IAM policy

描述

检查使用量是否超过 IAM policy 配额的 80%。

检查 ID

pR7UU017J9

其他资源

IAM 配额

IAM 角色

描述

检查使用量是否超过 IAM 角色配额的 80%。

检查 ID

oQ7TT017J9

其他资源

IAM 配额

IAM 服务器证书

描述

检查使用量是否超过 IAM 服务器证书配额的 80%。

检查 ID

rT7WW017J9

其他资源

IAM 配额

IAM 用户

描述

检查使用量是否超过 IAM 用户配额的 80%。

检查 ID

qS7VV0l7J9

其他资源

IAM 配额

每个区域的 Kinesis 分区数

描述

检查使用量是否超过每个区域的 Kinesis 分区数配额 80%。

检查 ID

bW7HH0l7J9

其他资源

Kinesis 配额

RDS 集群参数组

描述

检查使用量是否超过 RDS 集群参数组配额的 80%。

检查 ID

jtlIMO3qZM

其他资源

Amazon RDS 配额

RDS 集群角色数

描述

检查使用量是否超过 RDS 集群角色配额的 80%。

检查 ID

7fuccf1Mx7

其他资源

Amazon RDS 配额

RDS 集群

描述

检查使用量是否超过 RDS 集群配额的 80%。

检查 ID

gjqMBn6pjz

其他资源

Amazon RDS 配额

RDS 数据库实例

描述

检查使用量是否超过 RDS 数据库实例配额的 80%。

检查 ID

XG0aXHpIEt

其他资源

Amazon RDS 配额

RDS 数据库手动快照

描述

检查使用量是否超过 RDS 数据库手动快照配额的 80%。

检查 ID

dV84wpqRUs

其他资源

Amazon RDS 配额

RDS 数据库参数组

描述

检查使用量是否超过 RDS 数据库参数组配额的 80%。

检查 ID

jEECYg2YVU

其他资源

Amazon RDS 配额

RDS 数据库安全组

描述

检查使用量是否超过 RDS 数据库安全组配额的 80%。

检查 ID

gfZAn3W7wl

其他资源

Amazon RDS 配额

RDS 事件订阅

描述

检查使用量是否超过 RDS 事件订阅配额的 80%。

检查 ID

keAhfbH5yb

其他资源

Amazon RDS 配额

每个安全组的 RDS 最大身份验证次数

描述

检查使用量是否超过每个安全组的 RDS 最大身份验证次数配额的 80%。

检查 ID

dBkuNCvqn5

其他资源

Amazon RDS 配额

RDS 选项组

描述

检查使用量是否超过 RDS 选项组配额的 80%。

检查 ID

3Njm0DJQO9

其他资源

Amazon RDS 配额

每个主实例的 RDS 只读副本

描述

检查使用量是否超出每个主实例的 RDS 只读副本配额的 80%。

检查 ID

pYW8UkYz2w

其他资源

Amazon RDS 配额

RDS 预留实例

描述

检查使用量是否超过 RDS 预留实例配额的 80%。

检查 ID

UUDv0a5r34

其他资源

Amazon RDS 配额

RDS 子网组

描述

检查使用量是否超过 RDS 子网组配额的 80%。

检查 ID

dYWBaXaaMM

其他资源

Amazon RDS 配额

每个子网组的 RDS 子网数

描述

检查使用量是否超过每个子网组的 RDS 子网配额的 80%。

检查 ID

jEhCtdJK0Y

其他资源

Amazon RDS 配额

RDS 总存储配额

描述

检查使用量是否超过 RDS 总存储配额的 80%。

检查 ID

P1jhKWEmLa

其他资源

Amazon RDS 配额

Route 53 托管区域

描述

检查使用量是否超过每个账户的 Route 53 托管区域配额的 80%。

检查 ID

dx3xfcdfMr

其他资源

Route 53 配额

Route 53 最大运行状况检查次数

描述

检查使用量是否超过每个账户的 Route 53 运行状况检查配额的 80%。

检查 ID

`ru4xfcdfMr`

其他资源

Route 53 配额

Route 53 可重用的委托集

描述

检查使用量是否超过每个账户的 Route 53 可重用的委托集配额的 80%。

检查 ID

`ty3xfcdfMr`

其他资源

Route 53 配额

Route 53 流量策略

描述

检查使用量是否超过每个账户的 Route 53 流量策略配额的 80%。

检查 ID

`dx3xfbjfMr`

其他资源

Route 53 配额

Route 53 流量策略实例

描述

检查使用量是否超过每个账户的 Route 53 流量策略实例配额的 80%。

检查 ID

`dx8afcdfMr`

其他资源

Route 53 配额

SES 日发送配额

描述

检查使用量是否超过 Amazon SES 日发送配额的 80%。

检查 ID

`hJ7NN017J9`

其他资源

Amazon SES 配额

VPC

描述

检查使用量是否超过 VPC 配额的 80%。

检查 ID

`jL7PP017J9`

其他资源

VPC 配额

VPC 互联网网关

描述

检查使用量是否超过 VPC 互联网网关配额的 80%。

检查 ID

`kM7QQ017J9`

其他资源

VPC 配额

AWS Trusted Advisor 的更改日志

请参阅以下主题以了解对 Trusted Advisor 检查的最近更改。

> **Note**
>
> 如果您使用 Trusted Advisor 控制台或 AWS Support API，删除的检查不会出现在检查结果中。如果您使用任何已删除的检查，例如在 AWS Support API 操作或您的代码中指定检查 ID，您必须删除这些检查以避免 API 调用错误。

有关可用检查的更多信息，请参阅 AWS Trusted Advisor 检查引用 (p. 65)。

新的容错能力和性能检查

Trusted Advisor于 2021 2 1 2 1 2 1 2 1 6 月 1 日增加了了以下检查。

- 亚马逊 EFS 无装载目标冗余
- 亚马逊 EFS 吞吐量模式优化
- ActiveMQ 可用区冗余
- Rabbitmay 可用区冗余

有关更多信息，请参阅容错能力 (p. 108)类别和性能 (p. 83)类别。

新的容错能力检查

Trusted Advisor于 2021 2 1 2 1 2 1 2 1 5 月 16 日增加了了增加了了以下检查

- NAT Gateway
- 单一可用区应用程序检查

有关更多信息，请参阅 容错能力 (p. 108) 类别。

新的容错能力检查

Trusted Advisor2023 年 4 月 27 日增加了以下支票。

- 事件管理器复制集AWS 区域中的数量
- AWS Resilience Hub评估年龄

有关更多信息，请参阅 容错能力 (p. 108) 类别。

亚马逊 ECS 容错检查的区域扩展

Trusted Advisor2023 年 4 月 27 日，将以下检查范围扩大到其他地区。 Trusted Advisor现在，亚马逊 ECS 的检查已在所有正式可用 Amazon ECS 的区域提供。

- 使用单一可用区的 Amazon ECS 服务
- 亚马逊 ECS 多可用区放置策略

扩展到非洲（开普敦）、亚太地区（香港）、亚太地区（海得拉巴）、亚太地区（雅加达）、亚太地区（墨尔本）、欧洲地区（米兰）、欧洲（西班牙）、欧洲（苏黎世）、中东（巴林）、中东（阿联酋）。

新的容错能力检查

Trusted Advisor于 2021 3 月 30 日增加了了增加了了以下检查。

- 使用单一可用区的 Amazon ECS 服务
- 亚马逊 ECS 多可用区放置策略

有关更多信息，请参阅 容错能力 (p. 108) 类别。

新的容错能力检查

Trusted Advisor 于 2022 年 12 月 15 日新增了以下检查。

- 单个可用区中运行 HSM 实例的 AWS CloudHSM 集群
- Amazon ElastiCache 多可用区集群
- Amazon MemoryDB 多可用区集群

要在中Trusted Advisor接收AWS CloudHSM、ElastiCache和 MemoryDB 集群的结果，可用区中必须具有集群，可用区中必须具有集群。有关更多信息，请参阅以下文档：

- AWS CloudHSM 用户指南

- 适用于 Redis 的 Amazon MemoryDB 开发人员指南
- 亚马逊 Red ElastiCache is 版用户指南

Trusted Advisor 于 2022 年 12 月 15 日更新了以下检查信息。

- 违反 AWS Resilience Hub 策略：App Name 已更新为 Application Name
- AWS Resilience Hub 恢复能力评分：App Name 和 App Resilience Score 已更新为 Application Name 和 Application Resilience Score

有关更多信息，请参阅 容错能力 (p. 108) 类别。

更新了与 AWS Security Hub 集成的 Trusted Advisor

Trusted Advisor 于 2022 年 11 月 17 日进行了以下更新。

如果您禁用 AWS 区域的 Security Hub 或 AWS Config，Trusted Advisor 将会在 7 至 9 天内删除您对 AWS 区域的控件检查结果。之前，从 Trusted Advisor 删除 Security Hub 数据的时间范围为 90 天。

有关更多信息，请参阅 问题排查 (p. 49) 主题中的以下章节：

- 我关闭了 Security Hub 或 AWS Config 在一个区域 (p. 51)
- 我的控件已归档在 Security Hub 中，但 Trusted Advisor 中仍显示检查结果。 (p. 51)

新的 AWS Resilience Hub 容错能力检查

Trusted Advisor 于 2022 年 11 月 17 日新增了以下检查。

- 违反 AWS Resilience Hub 策略
- AWS Resilience Hub 恢复能力评分

您可以使用这些检查来查看应用程序的最新弹性策略状态和弹性得分。Resilience Hub 为您提供了一个中心位置来定义、跟踪和管理应用程序的弹性和可用性。

要在 Trusted Advisor 中接收 Resilience Hub 应用程序的结果，您必须部署 AWS 应用程序并使用 Resilience Hub 来跟踪应用程序的弹性状态。有关更多信息，请参阅 AWS Resilience Hub 用户指南。

要在中接收ElastiCache和 MemoryDB 集群Trusted Advisor的结果，可用区中必须具有集群，可用区中必须具有集群。有关更多信息，请参阅以下文档：

- 适用于 Redis 的 Amazon MemoryDB 开发人员指南
- 亚马逊 Red ElastiCache is 版用户指南

有关更多信息，请参阅 容错能力 (p. 108) 类别。

对 Trusted Advisor 控制台的更新

Trusted Advisor 于 2022 年 11 月 16 日新增了以下更改。

控制台中的 Trusted Advisor 控制面板现在是 Trusted Advisor 建议。Trusted Advisor 建议页面仍然显示检查结果以及关于您 AWS 账户每个类别的可用检查。

此名称更改仅会更新 Trusted Advisor 控制台。您可以像往常一样使用 Trusted Advisor 控制台和 AWS Support API 中的 Trusted Advisor 操作。

有关更多信息，请参阅开始使用 Trusted Advisor 建议 (p. 19)：

Amazon EC2 的新检查

Trusted Advisor 于 2022 年 9 月 1 日增加了以下检查。

- 使用终止支持版本的 Microsoft Windows Server 的 Amazon EC2 实例

有关更多信息，请参阅 安全性 (p. 93) 类别。

已将 Security Hub 检查添加到 Trusted Advisor

截至 2022 年 6 月 23 日，Trusted Advisor 仅支持 2022 年 4 月 7 日之前可用的 Security Hub 控件。此版本支持 AWS 基础安全最佳实践安全标准中的所有控件，但 Category: Recover > Resilience（类别：恢复 > 弹性）中的控件除外。有关更多信息，请参阅在 AWS Trusted Advisor 中查看 AWS Security Hub 控件 (p. 46)：

有关受支持控件的列表，请参阅《AWS Security Hub 用户指南》中的 AWS基础安全最佳实践控件。

增加了来自 AWS Compute Optimizer 的检查

Trusted Advisor 于 2022 年 5 月 4 日增加了以下检查。

检查名称	检查类别	检查 ID
Amazon EBS 过度预调配卷	成本优化	COr6dfpM03
Amazon EBS 预调配不足的卷	性能	COr6dfpM04
相比内存大小过度预调配的 AWS Lambda 函数	成本优化	COr6dfpM05
相比内存大小而言预调配不足的 AWS Lambda 函数	性能	COr6dfpM06

您必须为您的 AWS 账户 中启用 Compute Optimizer，才能让这些检查从您的 Lambda 和 Amazon EBS 资源接收数据。有关更多信息，请参阅启用 AWS Compute Optimizer 以执行 Trusted Advisor 检查 (p. 51)：

有关已泄露的访问密钥检查的更新

Trusted Advisor 于 2022 年 4 月 25 日更新了以下检查。

检查名称	检查类别	检查 ID
Exposed Access Keys	安全性	12Fnkpl8Y5

Trusted Advisor 现在可以自动为您刷新此检查。此检查不能从 Trusted Advisor 控制台或通过 AWS Support API 手动刷新。如果您的应用程序或代码为您的 AWS 账户刷新了此检查，我们建议您将其更新以不再刷新此检查。否则，您会收到 `InvalidParameterValue` 错误。

您在此次更新之前排除的任何访问密钥将不再被排除，并将显示为受影响的资源。您不能从检查结果中排除访问密钥。有关更多信息，请参阅Exposed Access Keys (p. 103)：

Note

如果您的 AWS 账户是在 2022 年 4 月 25 日之后创建的，则即使对于已泄露的访问密钥，已泄露的访问密钥检查的结果最初将显示为灰色图标（ ）。这表示 Trusted Advisor 没有发现该检查有任何更改。

如果 Trusted Advisor 发现某个资源存在风险，则其状态将更改为建议执行操作图标（ ）。修复或删除该资源后，检查结果将显示勾号图标（ ）。

更新了对 AWS Direct Connect 的检查

Trusted Advisor 于 2022 年 3 月 29 日增加了以下检查。

检查名称	检查类别	检查 ID
AWS Direct Connect 连接冗余	容错能力	`0t121N1Ty3`
AWS Direct Connect 位置冗余	容错能力	`8M012Ph3U5`
AWS Direct Connect 虚拟接口冗余	容错能力	`4g3Nt5M1Th`

- Region（区域）列的值现已显示 AWS 区域 代码，而不是完整名称。例如，美国东部（弗吉尼亚北部）中的资源现在拥有 `us-east-1` 值。
- Time Stamp（时间戳）列的值现在以 RFC 3339 格式显示，例如 `2022-03-30T01:02:27.000Z`。
- 未检测到任何问题的资源现在将显示在检查表中。这些资源的旁边具有一个检查标记图标 ( )。

  以前，只有您调查的 Trusted Advisor 建议的资源才会显示在此表中。这些资源旁边拥有一个警告图标 ( )。

AWS Trusted Advisor 控制台增加了 AWS Security Hub 控件

2022 年 1 月 18 日，AWS Trusted Advisor 增加了 111 个 Security（安全）类别的 Security Hub 控件。

您可以查看来自 AWS 基础安全最佳实践安全标准的 Security Hub 控件检查结果。此集成不包括 Category: Recover > Resilience（类别：恢复 > 弹性）的控件。

有关此功能的更多信息，请参阅在 AWS Trusted Advisor 中查看 AWS Security Hub 控件 (p. 46)。

新的 Amazon EC2 和 AWS Well-Architected 检查

2021 年 12 月 20 日，Trusted Advisor 增加了以下检查。

- 适用于 Microsoft SQL Server 的 Amazon EC2 实例整合
- 使用 Microsoft SQL Server 的 Amazon EC2 实例超限预置
- 使用终止支持版本的 Microsoft SQL Server 的 Amazon EC2 实例
- AWS Well-Architected 成本优化高风险问题
- AWS Well-Architected 性能高风险问题
- AWS Well-Architected 安全性高风险问题

- AWS Well-Architected 可靠性高风险问题

有关更多信息，请参阅 AWS Trusted Advisor 检查参考。

更新了 Ama OpenSearch y 的检查名称

Trusted Advisor 于 2021 年 9 月 8 日更新了 Amazon OpenSearch Service Reserved Instance Optimization 检查的名称。

检查建议、类别和 ID 是相同的。

检查名称	检查类别	检查 ID
亚马逊OpenSearch服务预留实例优化	成本优化	7ujm6yhn5t

Note

如果您将用Trusted Advisor于 Amazon CloudWatch 指标，此检查的指标名称也会更新。有关更多信息，请参阅创建亚马逊 CloudWatch 警报以监控AWS Trusted Advisor指标 (p. 329)：

增加了 Amazon Elastic Block Store 卷存储的检查

Trusted Advisor 于 2021 年 6 月 8 日增加了以下检查。

检查名称	检查类别	检查 ID
EBS 通用型 SSD (gp3) 卷存储	Service Limits	dH7RR016J3
EBS 预置 IOPS SSD (io2) 卷存储	Service Limits	gI7MM017J2

增加了 AWS Lambda 的检查

Trusted Advisor 于 2021 年 3 月 8 日增加了以下检查。

检查名称	检查类别	检查 ID
过度超时的 AWS Lambda 函数	成本优化	L4dfs2Q3C3
具有高误差率的 AWS Lambda 函数	成本优化	L4dfs2Q3C2
使用弃用运行时的 AWS Lambda 函数	安全性	L4dfs2Q4C5
无多可用区冗余的 AWS Lambda VPC 支持的函数	容错能力	L4dfs2Q4C6

有关如何将这些检查用于 Lambda 的更多信息，请参阅 AWS Lambda 开发人员指南中的查看建议的示例 AWS Trusted Advisor 工作流。

Trusted Advisor 检查删除

Trusted Advisor 于 2021 年 3 月 8 日删除了 AWS GovCloud (US) Region 的以下检查。

检查名称	检查类别	检查 ID
EC2 弹性 IP 地址	Service Limits	aW9HH0l8J6

更新了 Amazon Elastic Block Store 的检查

Trusted Advisor 于 2021 年 3 月 5 日在以下检查中将 Amazon EBS 卷的单位从 GiB 更新到 TiB。

> Note
>
> 如果您将用Trusted Advisor于 Amazon CloudWatch 指标，这五项检查的指标名称也会更新。有关更多信息，请参阅创建亚马逊 CloudWatch 警报以监控AWS Trusted Advisor指标 (p. 329)：

检查名称	检查类别	检查 ID	更新了的CloudWatch指标 ServiceLimit
EBS 冷 HDD (sc1) 卷存储	Service Limits	gH5CC0e3J9	冷 HDD (sc1) 卷存储 (TiB)
EBS 通用型 SSD (gp2) 卷存储	Service Limits	dH7RR0l6J9	通用型 SSD (gp2) 卷存储 (TiB)
EBS 磁介质（标准）卷存储	Service Limits	cG7HH0l7J9	磁介质（标准）卷存储 (TiB)
EBS 预置 IOPS SSD (io1) 卷存储	Service Limits	gI7MM0l7J9	预置 IOPS (SSD) 存储 (TiB)
EBS 吞吐量优化型 HDD (st1) 卷存储	Service Limits	wH7DD0l3J9	吞吐量优化型 HDD (st1) 卷存储 (TiB)

Trusted Advisor 检查删除

> Note
>
> Trusted Advisor 于 2020 年 11 月 18 日删除了以下检查。

2020 年 11 月 18 日删除的检查	检查类别	检查 ID
适用于 EC2 Windows 实例的 EC2Config 服务	容错能力	V77iOLlBqz
适用于 EC2 Windows 实例的 ENA 驱动程序版本	容错能力	TyfdMXG69d
适用于 EC2 Windows 实例的 NVMe 驱动程序版本	容错能力	yHAGQJV9K5
适用于 EC2 Windows 实例的 PV 驱动程序版本	容错能力	Wnwm9Il5bG

2020 年 11 月 18 日删除的检查	检查类别	检查 ID
EBS 活动卷	Service Limits	fH7LL0l7J9

Amazon Elastic Block Store 对您可以预置的卷数量不再有相应的限制。

您可以通过使用 AWS Systems Manager Distributor、其他第三方工具监控 Amazon EC2 实例并验证它们是否处于最新状态，或编写自己的脚本以返回 Windows Management Instrumentation (WMI) 的驱动程序信息。

Trusted Advisor 检查删除

Trusted Advisor 于 2020 年 2 月 18 日删除了以下检查。

检查名称	检查类别	检查 ID
Service Limits	性能	eW7HH0l7J9

Slack 中的 AWS Support App

您可以使用 AWS Support App 在 Slack 中管理 AWS 支持案例。您可以邀请您的团队成员加入聊天通道，回复案例更新，并直接与支持座席聊天。AWS Support App 可帮助您在 Slack 中快速直接地管理支持案例。

您可以使用 AWS Support App 执行以下操作：

- 在 Slack 通道中创建、更新、搜索和解决支持案例
- 将文件附加到支持案例
- 从服务限额请求增加限额
- 无需离开 Slack 通道，即可与您的团队共享支持案例详细信息
- 与支持座席开始实时聊天会话

当您在 AWS Support App 中创建、更新或解决支持案例时，案例也会在 AWS Support Center Console 中进行更新。无需登录支持中心工作台，即可对支持案例进行单独管理。

注意

- 无论您是从 Slack 还是从支持中心工作台创建案例，支持案例的响应时间始终相同。
- 您可以为账户和账单支持、服务限额增加和技术支持创建支持案例。

主题

- 先决条件 (p. 153)
- 授权 Slack 工作区 (p. 159)
- 配置 Slack 通道 (p. 160)
- 在 Slack 通道中创建支持案例 (p. 165)
- 在 Slack 中回复支持案例 (p. 170)
- 加入与 AWS Support 的实时聊天会话 (p. 172)
- 在 Slack 中搜索支持案例 (p. 176)
- 在 Slack 中解决支持案例 (p. 179)
- 在 Slack 中重新打开支持案例 (p. 180)
- 请求增加服务限额 (p. 181)
- 从 AWS Support App 中删除 Slack 通道配置 (p. 182)
- 从 AWS Support App 中删除 Slack 工作区配置 (p. 183)
- Slack 中的 AWS Support App 命令 (p. 184)
- 在 AWS Support Center Console 中查看 AWS Support App 通信信息 (p. 185)
- 使用 AWS CloudFormation 创建 Slack 中的 AWS Support App 资源 (p. 185)

先决条件

您必须满足以下要求才能使用 Slack 中的 AWS Support App：

- 您拥有商业、Enterprise On-Ramp 或企业 Support 计划。您可以从 AWS Support Center Console 或从支持计划页面中查找您的支持计划。有关更多信息，请参阅比较 AWS Support 计划。
- 您已为您的组织创建 Slack 工作区和通道。您必须是 Slack 工作区管理员，或者有权将应用程序添加到该 Slack 工作区。有关更多信息，请参阅 Slack 帮助中心。
- 您以具有所需权限的 AWS Identity and Access Management（IAM）用户或角色登录 AWS 账户。有关更多信息，请参阅管理对 AWS Support App 小组件的访问 (p. 154)：
- 您需要创建一个 IAM 角色，该角色具有执行操作所需的权限。AWS Support App 使用此角色对不同的服务进行 API 调用。有关更多信息，请参阅 管理对 AWS Support App 的访问 (p. 155)。

主题

- 管理对 AWS Support App 小组件的访问 (p. 154)
- 管理对 AWS Support App 的访问 (p. 155)

管理对 AWS Support App 小组件的访问

您可以附上 AWS Identity and Access Management（IAM）policy 以授予 IAM 用户配置 AWS Support 中的 AWS Support Center Console App 小组件的权限。

有关如何将策略附加到 IAM 实体的更多信息，请参阅《IAM 用户指南》中的添加 IAM 身份权限（控制台）。

> Note
>
> 您也可以用根用户身份登录 AWS 账户，但不建议您这样做。有关根用户访问权限的更多信息，请参阅《IAM 用户指南》中的保护您的根用户凭证，不要将其用于日常任务。

示例 IAM policy

您可以将以下策略附加到实体上，例如 IAM 用户或群组。此策略允许用户授权 Slack 工作区并在支持中心控制台中配置 Slack 通道。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportapp:GetSlackOauthParameters",
                "supportapp:RedeemSlackOauthCode",
                "supportapp:DescribeSlackChannels",
                "supportapp:ListSlackWorkspaceConfigurations",
                "supportapp:ListSlackChannelConfigurations",
                "supportapp:CreateSlackChannelConfiguration",
                "supportapp:DeleteSlackChannelConfiguration",
                "supportapp:DeleteSlackWorkspaceConfiguration",
                "supportapp:GetAccountAlias",
                "supportapp:PutAccountAlias",
                "supportapp:DeleteAccountAlias",
                "supportapp:UpdateSlackChannelConfiguration",
                "iam:ListRoles"
            ],
            "Resource": "*"
        }
    ]
}
```

将 AWS Support App 连接到 Slack 所需的权限

AWS Support App 包括仅限权限操作，这些操作不会直接响应 API 操作。服务授权参考中用“[仅权限]”指明了这些操作。

AWS Support App 使用以下 API 操作连接到 Slack，然后在 AWS Support Center Console 中列出您的公共 Slack 通道：

- `supportapp:GetSlackOauthParameters`
- `supportapp:RedeemSlackOauthCode`
- `supportapp:DescribeSlackChannels`

这些 API 操作不应由您的代码调用。因此，这些 API 操作未包含在 AWS CLI 和 AWS 开发工具包中。

管理对 AWS Support App 的访问

在您拥有 AWS Support App 小组件的权限之后，还必须创建一个 AWS Identity and Access Management（IAM）角色。此角色可为您执行其他 AWS 服务 的操作，例如 AWS Support API 和服务限额。

然后，您可以将 IAM policy 附加到该角色，以便该角色拥有完成这些操作所需的权限。在支持中心控制台中创建 Slack 通道配置时，您可以选择此角色。

Slack 通道中的用户拥有您授予 IAM 角色的同一权限。例如，如果您为支持案例指定只读访问权限，则 Slack 通道中的用户可以查看您的支持案例，但无法更新支持案例。

> Important
>
> 当您请求与支持座席进行实时聊天时，App 会创建一个单独的 Slack 通道，AWS SupportApp 会创建一个单独的 Slack 通道。此 Slack 通道拥有与您创建案例或发起聊天的通道相同的权限。
> 如果您更改 IAM 角色或 IAM policy，您的更改将应用于您配置的 Slack 通道以及 AWS Support App 为您创建的任何新的实时聊天 Slack 通道。

按照以下步骤创建您的 IAM 角色和策略。

主题

- 使用 AWS 托管策略或创建客户管理型策略 (p. 155)
- 创建 IAM 角色 (p. 157)
- 问题排查 (p. 157)

使用 AWS 托管策略或创建客户管理型策略

要授予角色权限，您可以使用 AWS 托管策略或客户管理型策略。

> Tip
>
> 如果您不想手动创建策略，我们建议您使用 AWS 托管策略并跳过此过程。托管策略自动拥有 AWS Support App 的所需权限。您无需手动更新策略。有关更多信息，请参阅用于 Slack 中 AWS Support App 的 AWS 托管策略 (p. 211)：

按照此步骤为您的角色创建客户管理型策略。此过程使用 IAM 控制台中的 JSON 策略编辑器。

为 AWS Support App 创建客户管理型策略

1. 登录AWS Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。

2. 在导航窗格中，选择 Policies (策略)。
3. 选择创建策略。
4. 请选择 JSON 选项卡。
5. 输入您的 JSON，然后在编辑器中替换默认 JSON。您可以使用示例策略 (p. 156)。
6. 请选择下一步：标签。
7. （可选）您可以使用标签作为键值对将元数据添加到策略。
8. 选择 Next: Review（下一步: 审核）。
9. 在查看策略页面，输入 Name（名称），例如 *AWSSupportAppRolePolicy* 和 Description（描述）（可选）。
10. 查看 Summary（摘要）页面以查看策略允许的权限，然后选择 Create policy（创建策略）。

此策略定义角色可以执行的操作。有关更多信息，请参阅《IAM 用户指南》中的创建 IAM policy（控制台）。

示例 IAM policy

您可以将下列示例策略附加到 IAM 角色。此策略允许角色对 AWS Support App 的所有必要操作拥有完全权限。在您为 Slack 通道配置角色后，该通道中的任何用户都具有相同的权限。

> **Note**
>
> 有关 AWS 托管策略的列表，请参阅 用于 Slack 中 AWS Support App 的 AWS 托管策略 (p. 211)。

您可以更新策略以从 AWS Support App 中删除权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

有关每项操作的描述，请参阅《服务授权参考》中的以下主题：

- AWS Support 的操作、资源和条件键
- 服务限额的操作、资源和条件键
- AWS Identity and Access Management 的操作、资源和条件键

创建 IAM 角色

创建策略后，您必须创建 IAM 角色，并将策略附加到该角色。在支持中心控制台中创建 Slack 通道配置时，您可以选择此角色。

为 AWS Support App 创建角色

1. 登录AWS Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择 Roles (角色)，然后选择 Create role (创建角色)。
3. 对于 Select trusted entity（选择受信任实体），选择 AWS 服务。
4. 选择 AWS Support App。
5. 选择Next: Permissions（下一步: 权限）。
6. 输入策略名称。您可以选择 AWS 托管策略或选择您创建的客户管理型策略，例如 *AWSSupportAppRolePolicy*。选中策略旁的复选框。
7. 请选择下一步：标签。
8. （可选）您可以使用标签作为键值对将元数据添加到角色。
9. 选择 Next: Review（下一步: 审核）。
10. 对于 Role name（角色名称），输入名称，例如 *AWSSupportAppRole*。
11. （可选）对于 Role description(角色描述)，输入角色的描述。
12. 检查角色，然后选择 Create role。在支持中心控制台中创建 Slack 通道配置时，您可以选择此角色。请参阅配置 Slack 通道 (p. 160)。

有关更多信息，请参阅《IAM 用户指南》中的创建用于 AWS 服务的角色。

问题排查

请参阅以下主题以管理对 AWS Support App 的访问。

目录

- 我想限制 Slack 通道中的特定用户执行特定操作 (p. 157)
- 我配置 Slack 通道时，看不到我创建的 IAM 角色 (p. 158)
- 我的 IAM 角色缺少权限 (p. 158)
- Slack 错误消息显示我的 IAM 角色无效 (p. 158)
- AWS Support App 显示我缺少服务限额的 IAM 角色 (p. 158)

我想限制 Slack 通道中的特定用户执行特定操作

默认情况下，Slack 通道中的用户拥有的权限与附加到您创建的 IAM 角色中的 IAM policy 所指定的权限相同。这意味着通道中的任何人对支持案例都具有读取或写入权限，无论他们是否拥有 AWS 账户 或 IAM 用户。

我们建议您遵循以下最佳实践：

- 为 AWS Support App 配置专用 Slack 通道
- 仅邀请需要访问支持案例的用户加入您的通道
- 使用对 AWS Support App 具有最低所需权限的 IAM policy。请参阅用于 Slack 中 AWS Support App 的 AWS 托管策略 (p. 211)。

我配置 Slack 通道时，看不到我创建的 IAM 角色

如果 IAM 角色未出现在 AWS Support App 列表的 IAM 角色中，这意味着该角色没有将 AWS Support App 作为可信实体，或者该角色已被删除。您可以更新现有角色或创建一个新角色。请参阅创建 IAM 角色 (p. 157)。

我的 IAM 角色缺少权限

您为 Slack 通道创建的 IAM 角色需要权限才能执行您需要的操作。例如，如果您想让 Slack 中的用户创建支持案例，则该角色必须具有 `support:CreateCase` 权限。AWS Support App 将担任此角色为您执行这些操作。

如果您从 AWS Support App 收到有关缺少权限的错误消息，请验证附加到角色的策略是否具有所需权限。

请参阅前面的 示例 IAM policy (p. 156)。

Slack 错误消息显示我的 IAM 角色无效

请确认您为通道配置选择了正确的角色。

验证您的角色

1. 在 https://console.aws.amazon.com/support/app#/config 页面登录 AWS Support Center Console。
2. 选择您为 AWS Support App 配置的通道。
3. 从 Permissions（权限）部分中，找到您选择的 IAM 角色名称。
   - 若要更改角色，请选择 Edit（编辑），选择另一个角色，然后选择 Save（保存）。
   - 若要更新角色或附加到该角色的策略，请登录 IAM 控制台。

AWS Support App 显示我缺少服务限额的 IAM 角色

您必须在账户中拥有从服务限额请求增加限额的 `AWSServiceRoleForServiceQuotas` 角色。如果您收到有关缺少资源的错误消息，请完成以下步骤之一：

- 使用服务限额控制台请求增加限额。成功发送请求后，服务限额会自动为您创建此角色。然后，您可以使用 AWS Support App 在 Slack 中请求增加限额。有关更多信息，请参阅 Requesting a quota increase（请求增加限额）。
- 更新附加到角色的 IAM policy。这将授予角色对服务限额的权限。示例 IAM policy (p. 156) 中的以下部分允许 AWS Support App 为您创建服务限额角色。

```
{
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
     }
}
```

如果您要删除为通道配置的 IAM 角色，则必须手动创建该角色或更新 IAM policy 以允许 AWS Support App 为您创建一个新角色。

授权 Slack 工作区

授权工作区并向 AWS Support App 授予工作区访问权限后，您的 AWS 账户 需要一个 AWS Identity and Access Management（IAM）角色。AWS Support App 将使用此角色，为您从 AWS Support 和服务限额调用 API 操作。例如，AWS Support App 会使用角色来调用 `CreateCase` 操作，以在 Slack 中为您创建支持案例。

注意

- Slack 通道会继承 IAM 角色的权限。这意味着，Slack 通道中任何用户的权限都与附加到该角色的 IAM policy 中指定的权限相同。

  例如，如果您的 IAM policy 允许该角色具有对支持案例的完全读取和写入权限，则 Slack 通道中的任何用户均可创建、更新和解决支持案例。如果 IAM policy 允许该角色具有只读权限，则 Slack 通道中的用户仅具有读取支持案例的权限。
- 我们建议您添加管理支持操作所需的 Slack 工作区和通道。我们建议您配置专用通道，并且只邀请所需用户。

您必须授权每个要用于 AWS 账户 的 Slack 工作区。如果您有多个 AWS 账户，则必须登录每个账户并重复以下步骤才能授权工作区。如果您的账户属于 AWS Organizations 中的某个组织，并且您想要授权多个账户，请跳至 Authorize multiple accounts（授权多个账户）。

为 AWS 账户 授权 Slack 工作区

1. 登录到 AWS Support Center Console，然后选择 Slack configuration（Slack 配置）。
2. 在入门页面上，选择 Authorize workspace（授权工作区）。
3. 如果尚未登录到 Slack，请在 Sign in to your workspace（登录到工作区）页面上，输入工作区名称，然后选择 Continue（继续）。
4. 在AWS Support请求访问 your-workspace-name Slack 页面的权限上，选择 “允许”。

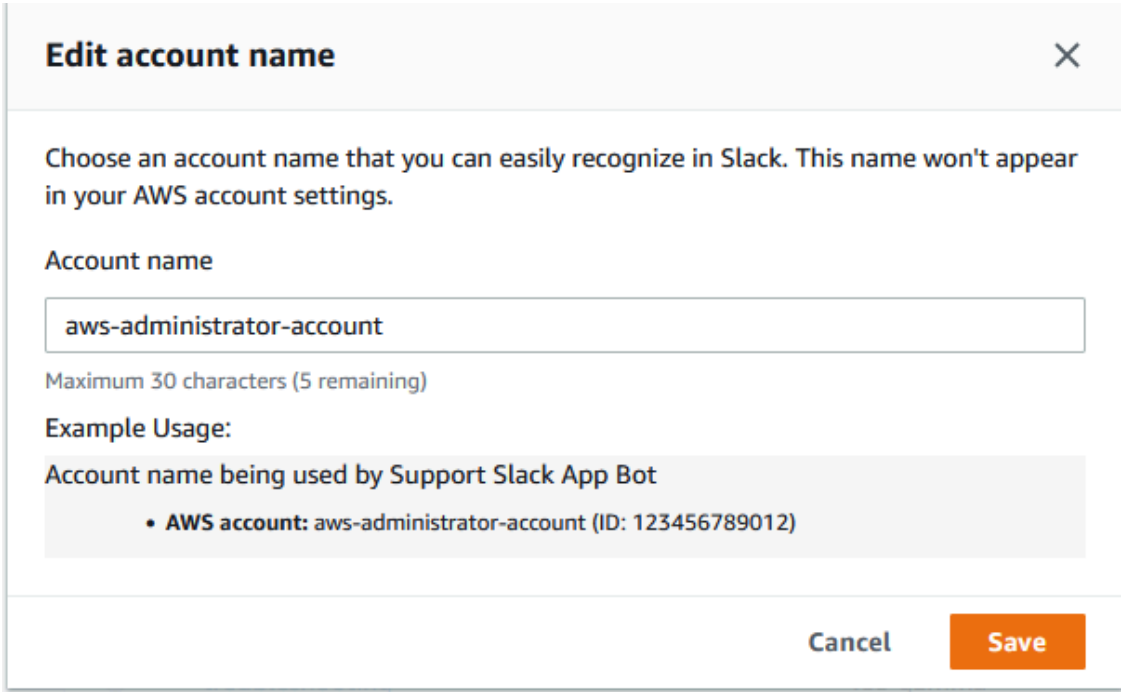
   Note

   如果您无法允许 Slack 访问工作区，请确保您拥有 Slack 管理员权限，可将 AWS Support App 添加到工作区。请参阅先决条件 (p. 153)。

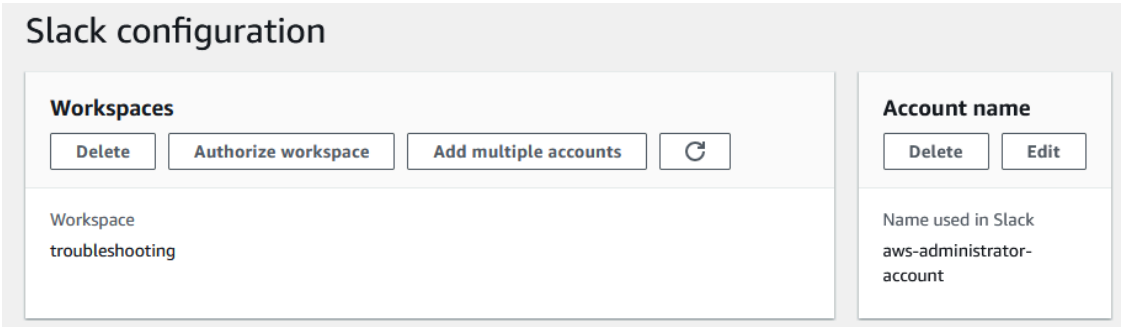
   在 Slack 配置页面上，Workspaces（工作区）下方会显示您的工作区名称。
5. （可选）要添加更多工作区，请选择 Authorize workspace（授权工作区）然后重复步骤 3-4。您最多可以向您的账户添加五个工作区。
6. （可选）默认情况下，您的 AWS 账户 ID 号会显示为 Slack 通道中的账户名称。要更改此值，请在 Account name（账户名称）下选择 Edit（编辑），输入账户名称，然后选择 Save（保存）。

   Tip

   使用便于您和您的团队轻松识别的名称。AWS Support App 会使用此名称来识别您在 Slack 通道中的账户。您可以随时更新此名称。



Slack 配置页面会显示您的工作区名称和账户名称。



授权多个账户

要授权多个 AWS 账户使用 Slack 工作区，您可以使用 AWS CloudFormation (p. 185) 或 Terraform (p. 189) 来创建 AWS Support App 资源。

配置 Slack 通道

授权 Slack 工作区后，您可以配置 Slack 通道以使用 AWS Support App。

在您邀请和添加 AWS Support App 的通道中，您可以创建和搜索案例以及接收案例通知。该通道会显示案例更新，例如新创建的案例或已解决的案例、已添加的通信和共享的案例详细信息。

Slack 通道会继承 IAM 角色的权限。这意味着，Slack 通道中任何用户的权限都与附加到该角色的 IAM policy 中指定的权限相同。

例如，如果您的 IAM policy 允许该角色具有对支持案例的完全读取和写入权限，则 Slack 通道中的任何用户均可创建、更新和解决支持案例。如果 IAM policy 允许该角色具有只读权限，则 Slack 通道中的用户仅具有读取支持案例的权限。

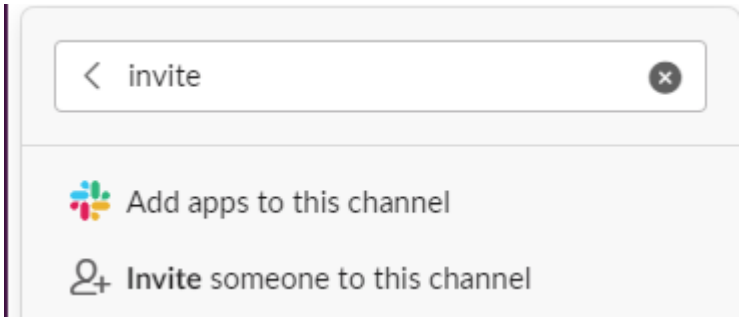
您最多可以为一个账户添加 20 个通道。一个 Slack 通道最多可拥有 100 个 AWS 账户。这意味着只有 100 个账户可以将相同的 Slack 通道添加到 AWS Support App。我们建议您仅添加管理组织中的支持案例所需的账户，这样可以减少您在通道中接收的通知数量，从而减少对您和您的团队的干扰。

每个 AWS 账户 都必须在 AWS Support App 中单独配置一个 Slack 通道，这样，AWS Support App 才能访问该 AWS 账户 中的支持案例。如果您组织中的其他 AWS 账户 已邀请 AWS Support App 加入该 Slack 通道，请跳至步骤 3。

> **Note**
>
> 您可以配置作为 Slack Connect 一部分的通道以及与多个工作区共享的通道。但是，只有为 AWS 账户配置了共享通道的第一个工作区才能使用 AWS Support App。如果您尝试为另一个工作区配置相同的 Slack 通道，AWS Support App 会返回一条错误消息。

配置 Slack 通道

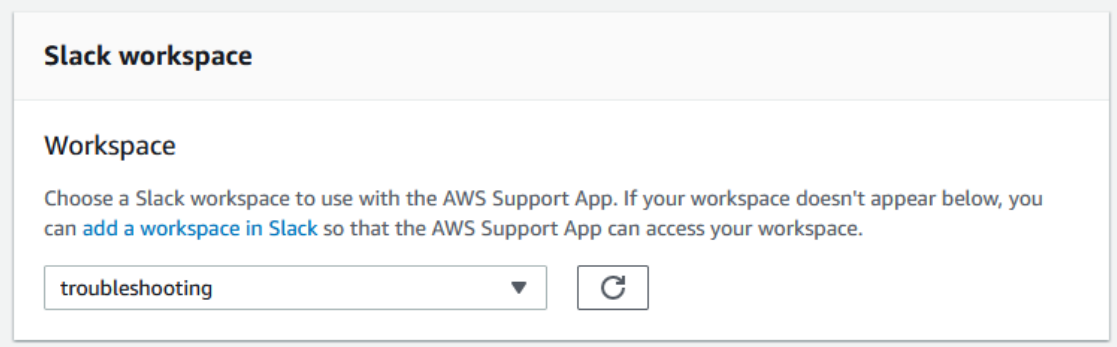
1. 在 Slack 应用程序中，选择要与 AWS Support App 结合使用的 Slack 通道。
2. 完成以下步骤以邀请 AWS Support App 加入您的通道：
   a. 选择 + 图标并输入 `invite`，然后在出现提示时选择 Add apps to this channel（将应用程序添加到此通道）。



   b. 要搜索应用程序，请在 Add apps to channelName（将应用程序添加到 channelName）下，输入 AWS Support App。
   c. 选择 AWS Support App 旁边的 Add（添加）。



3. 登录支持中心控制台，然后选择 Slack configuration（Slack 配置）。
4. 选择 Add channel（添加通道）。
5. 在 Add channel（添加通道）页面上，Workspace（工作区）下，选择您之前授权的工作区名称。如果列表未显示此工作区名称，您可以选择刷新图标。

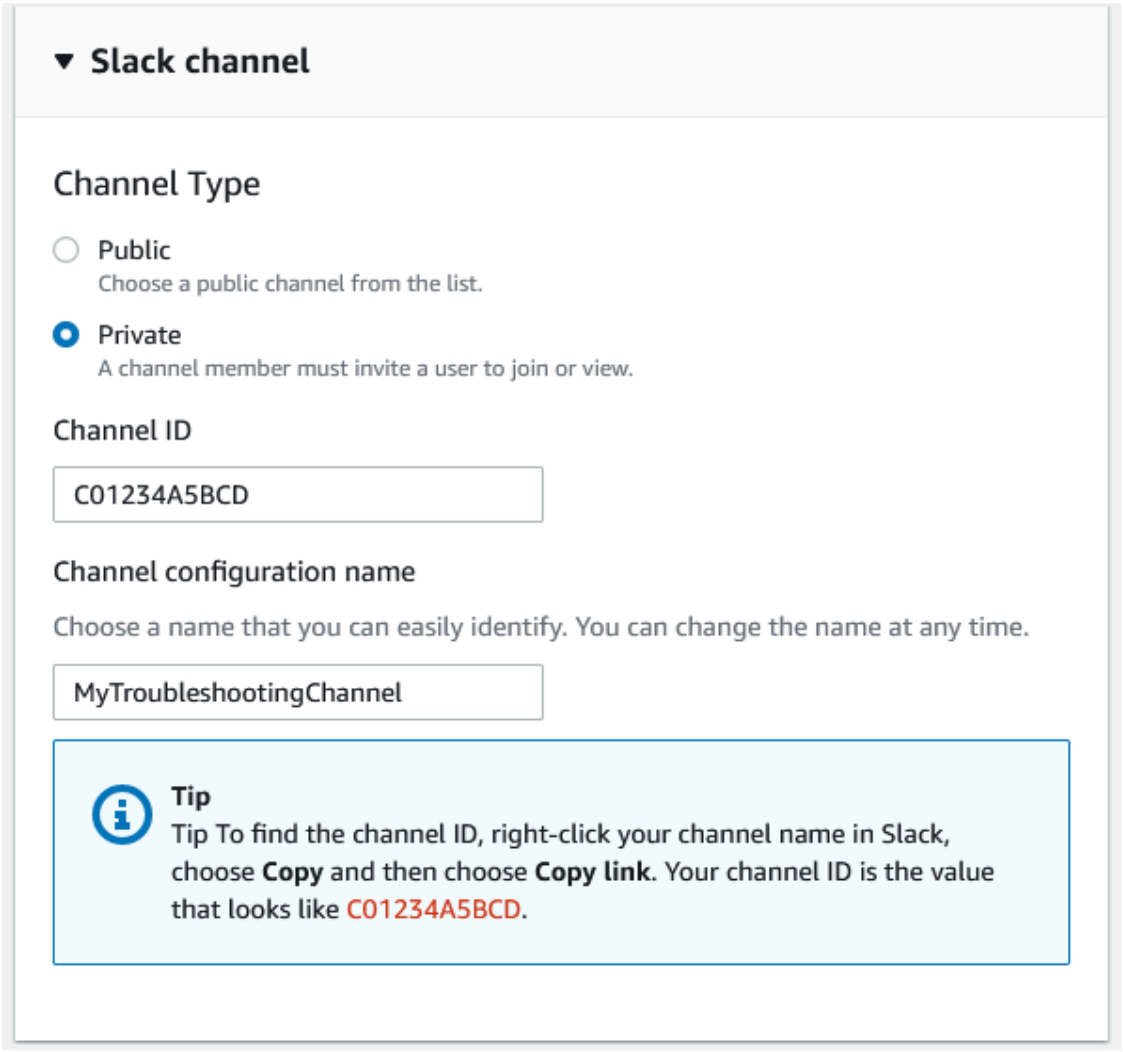


6. 在 Slack channel（Slack 通道）下，对于 Channel type（通道类型），请选择以下选项之一：
   - Public（公有）– 在 Public channel（公有通道）下，选择您邀请 AWS Support App 加入的 Slack 通道（步骤 2）。如果列表未显示您的通道，请选择刷新图标并重试。
   - Private（专用）– 在 Channel ID（通道 ID ）下，输入您邀请 AWS Support App 加入的 Slack 通道的 ID 或 URL。

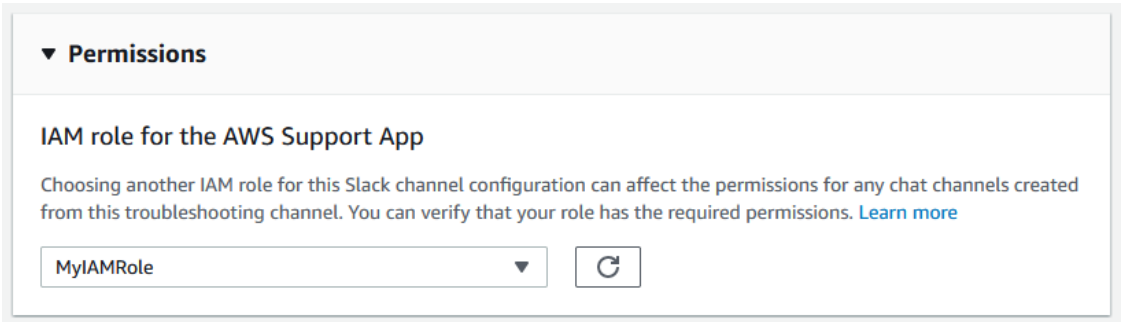
     Tip

     要查找通道 ID，请在 Slack 中打开通道名称的上下文（右键单击）菜单，然后依次选择 Copy（复制）、Copy link（复制链接）。通道 ID 是类似于 *C01234A5BCD* 的值。
7. 在 Channel configuration name（通道配置名称）下，输入一个可轻松识别 AWS Support App 的 Slack 通道配置的名称。该名称仅会在您的 AWS 账户 中显示，不会在 Slack 中显示。您可以稍后重命名通道配置。

   您的 Slack 通道类型可能类似于以下示例。



8. 在 Permissions（权限）下，对于 IAM role for the AAWS Support pp in Slack（Slack 中AWS Support App 的 I 列表仅显示将 AWS Support App 作为可信实体的角色。



   Note

   如果您尚未创建角色或列表未显示您的角色，请参阅 管理对 AWS Support App 的访问 (p. 155)。

9. 在 Notifications（通知）下，指定如何接收案例通知。

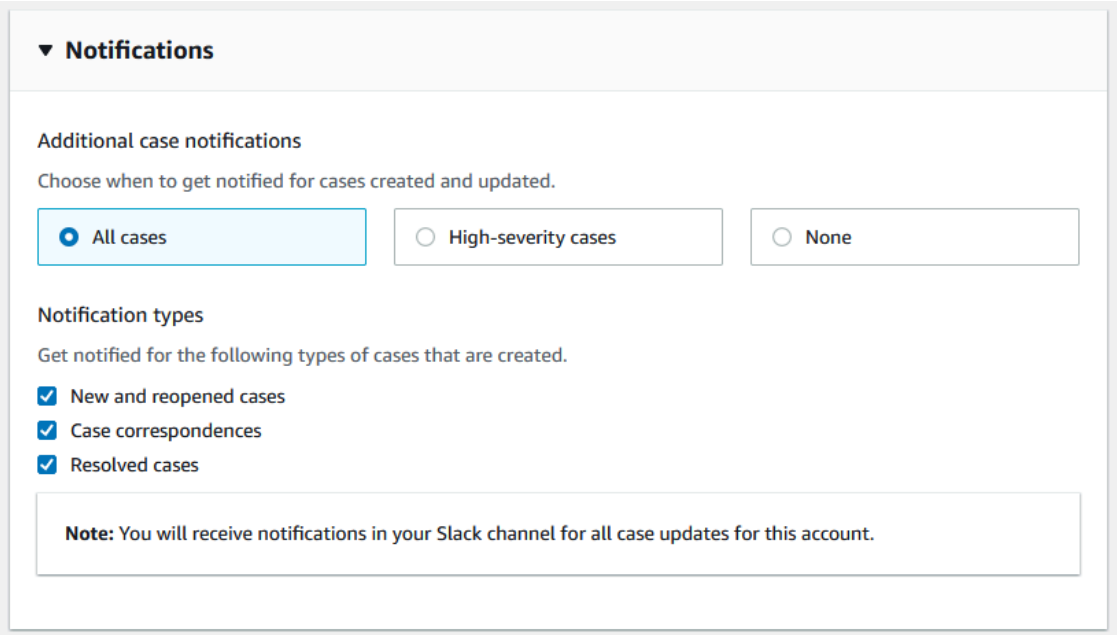
   - All cases（所有案例）– 接收所有案例更新通知。

- High-severity cases（高严重性案例）– 仅接收影响生产系统或更高级别系统的案例通知。有关更多信息，请参阅 选择严重性 (p. 3)。
- None（无）– 不接收案例更新通知。

10. （可选）如果您选择 All cases（所有案例）或 High-severity cases（高严重性案例），则必须至少选择下列选项之一：

    - New and reopened cases（新的案例和重新打开的案例）
    - Case correspondences（案例通信信息）
    - Resolved cases（已解决的案例）

    以下通道会接收 Slack 中所有案例更新通知。



11. 查看配置并选择 Add channel（添加通道）。Slack configuration（Slack 配置）页面会显示您的通道。

更新 Slack 通道配置

配置 Slack 通道后，您可以稍后对其进行更新，以更改 IAM 角色或案例通知。

更新 Slack 通道配置

1. 登录支持中心控制台，然后选择 Slack configuration（Slack 配置）。
2. 在 Channels（通道）下，选择所需的通道配置。
3. 在 ***channelName*** 页面上，您可以执行以下任务：
    - 选择 Rename（重命名）以更新通道配置名称。该名称仅会在您的 AWS 账户 中显示，不会在 Slack 中显示。
    - 选择 Delete（删除），以从 AWS Support App 中删除通道配置。请参阅 从 AWS Support App 中删除 Slack 通道配置 (p. 182)。
    - 选择 Open in Slack（在 Slack 中打开），以在浏览器中打开 Slack 通道。
    - 选择 Edit（编辑）以更改 IAM 角色或通知。

在 Slack 通道中创建支持案例

授权 Slack 工作区并添加 Slack 通道后，您可以在 Slack 通道中创建支持案例。

在 Slack 中创建支持案例

1. 在 Slack 通道中输入以下命令：

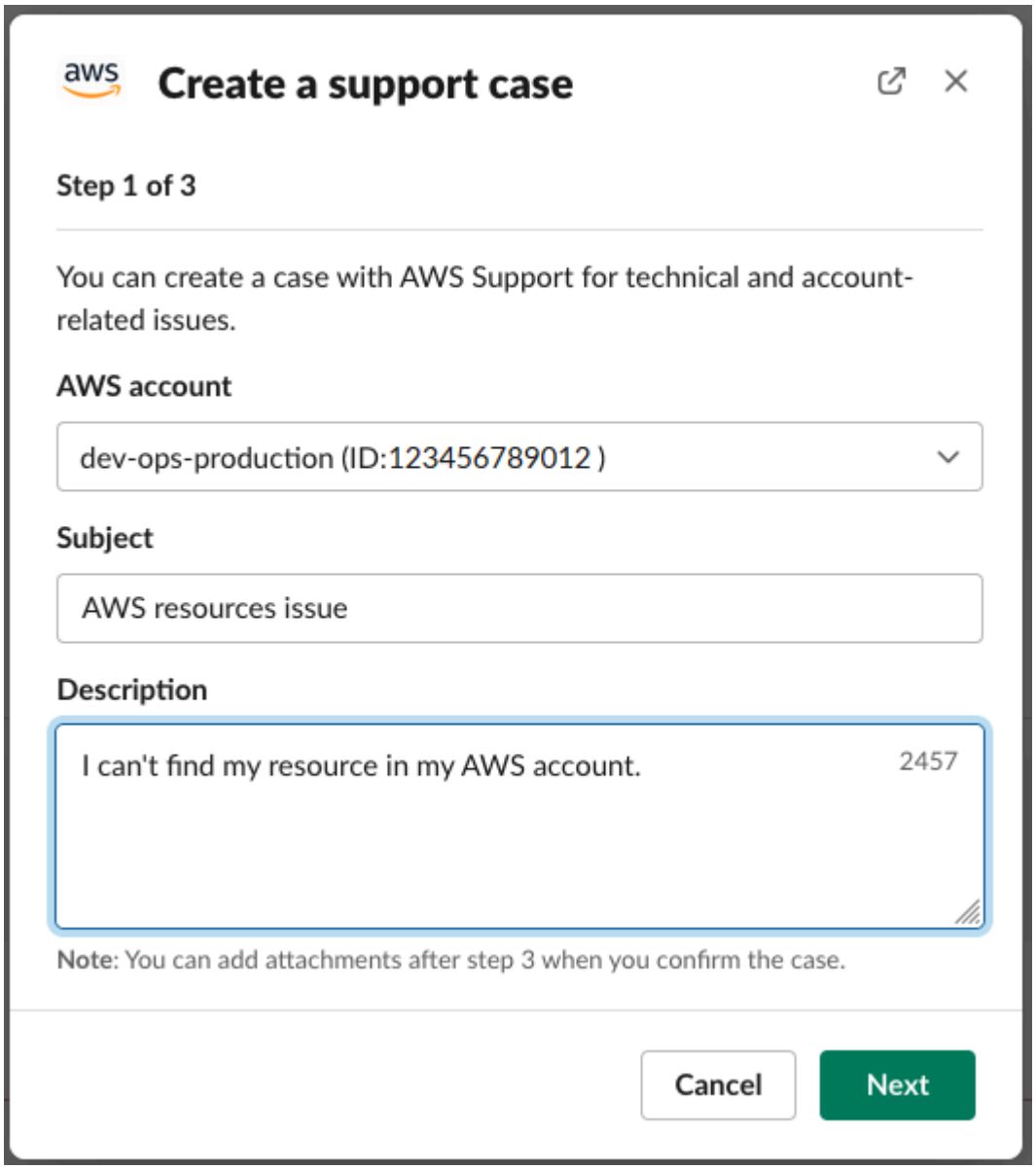
   ```
   /awssupport create
   ```

2. 在 Create a support case（创建支持案例）对话框中，执行以下操作：

   a. 如果您为此 Slack 通道配置了多个账户，请为 AWS 账户 选择账户 ID。如果您创建了账户名称，则该值会显示在账户 ID 旁边。有关更多信息，请参阅授权 Slack 工作区 (p. 159)：

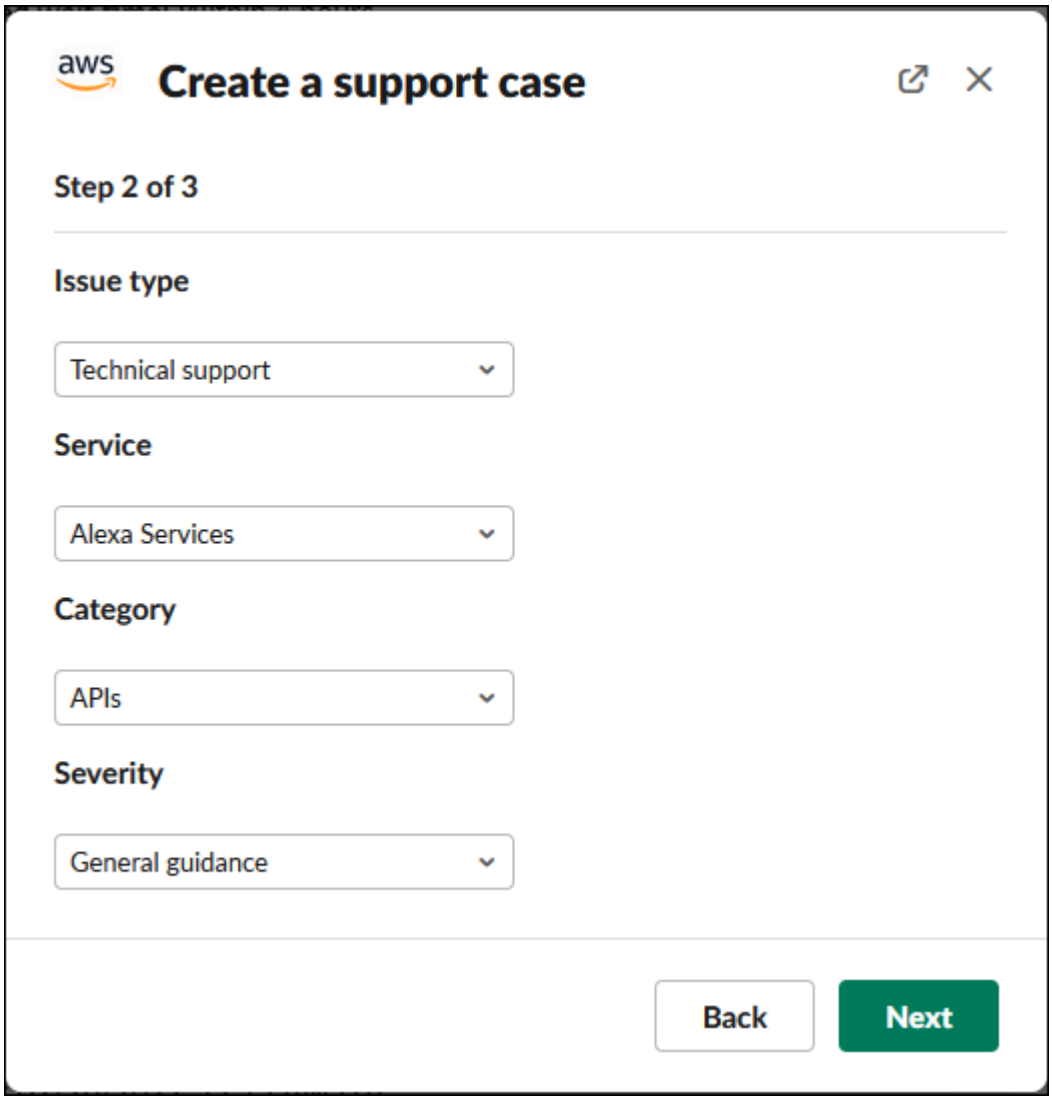
   b. 对于 Subject（主题），请输入支持案例的标题。

   c. 对于 Description（描述），请对支持案例进行描述。提供详细信息，例如 AWS 服务 的使用方式以及可尝试的问题排查步骤。



3. 选择下一步。
4. 在 Create a support case（创建支持案例）对话框中，指定以下选项：
   a. 选择 Issue type（问题类型）。
   b. 选择 Service（服务）。
   c. 选择 Category（类别）。
   d. 选择 Severity（严重性）。
   e. 查看案例详细信息并选择 Next（下一步）。

   以下示例显示了 Alexa 服务的技术支持案例。



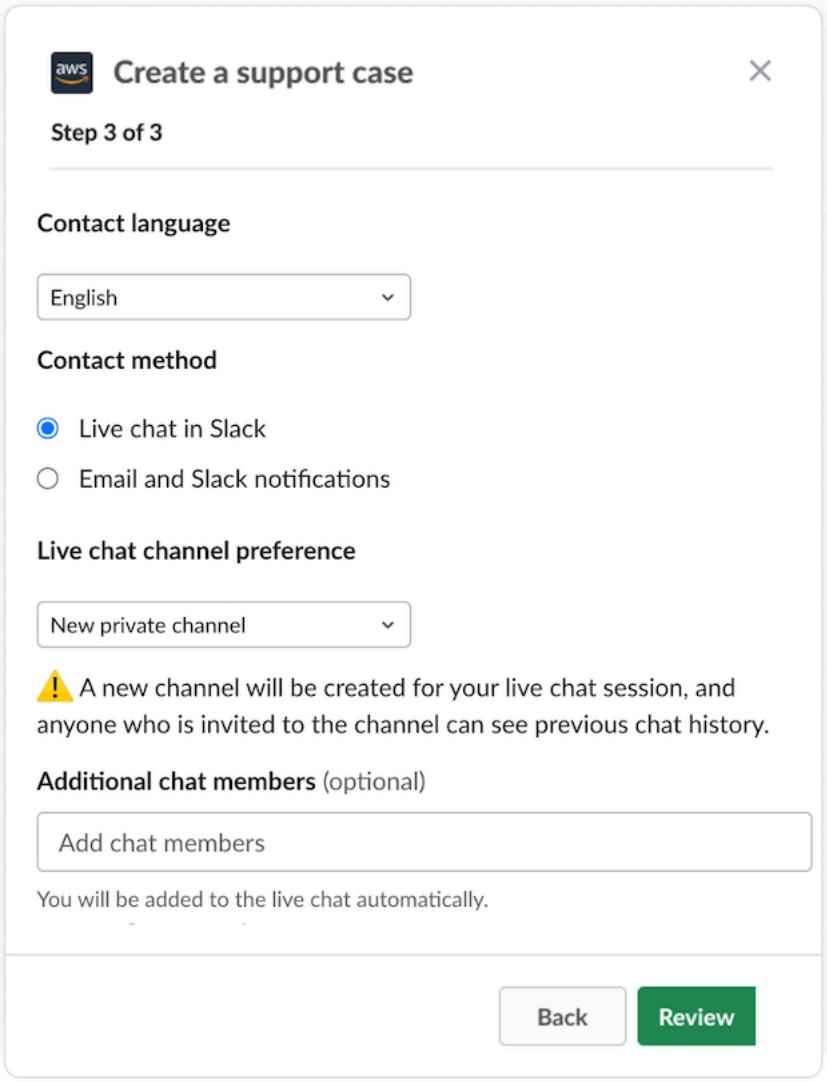
5. 对于 Contact language（联系语言），为您的支持案例选择首选语言。

   Note

   对于账户和账单案例，Slack 中的实时聊天暂不提供日语支持。

6. 对于 Contact method（联系方式），选择 Email and Slack notifications（电子邮件和 Slack 通知）或 Live chat in Slack（Slack 中的实时聊天）。

   以下示例显示了如何在 Slack 中选择实时聊天。



a. 如果您在 Slack 中选择实时聊天，请选择 “新建私人频道” 或 “当前频道” 作为您的实时聊天频道首选项。新的私人频道将创建一个单独的私人频道供你与AWS Support代理聊天，而当前频道将使用当前频道中的话题让你与AWS Support代理聊天。

b. （可选）如果您选择 Live chat in Slack（Slack 中的实时聊天），您可以输入其他 Slack 成员的姓名。对于新的私人频道，该AWS Support应用程序会自动将您和选定的成员添加到新频道。对于当前频道，当AWS Support代理加入时，AWS Support应用程序将自动标记您和聊天话题中的选定成员。

Important

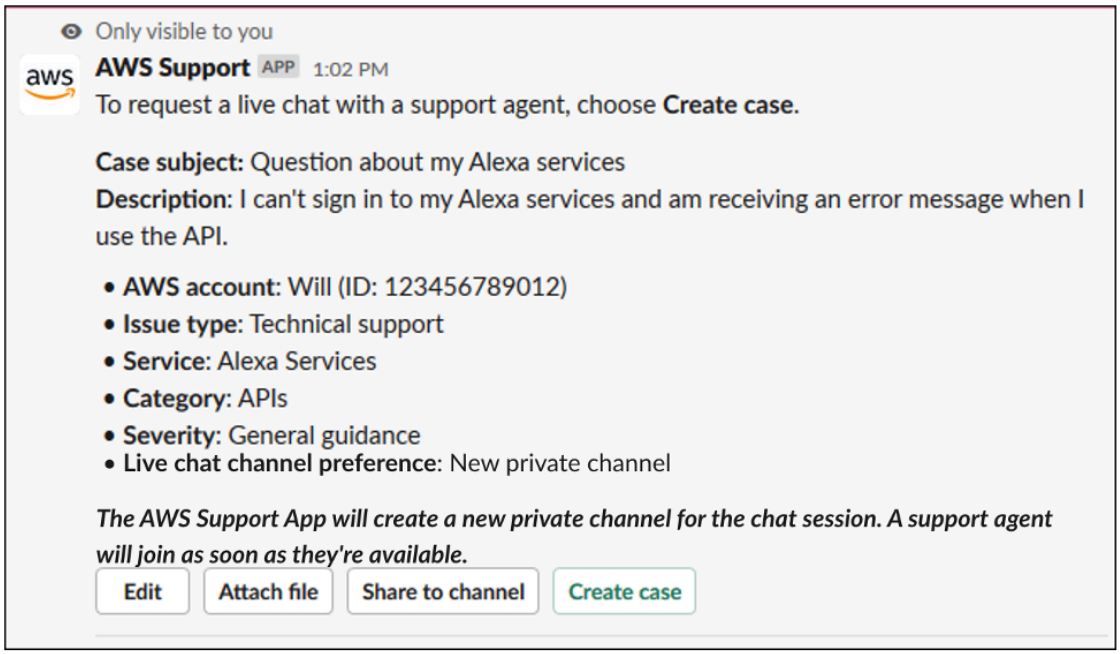
- 我们建议您只添加您希望其可以访问支持案例的聊天成员。
- 如果您为现有支持案例启动新的实时聊天会话，则AWS Support App 将使用与之前实时聊天相同的聊天通道。该AWS Support应用程序还使用与之前相同的实时聊天频道首选项。
- 只有从私人频道请求聊天时，“当前频道” 选项才可用。您只添加您希望其可以访问您希望其可以访问您希望其可以访问您希望其可以访问您希望其可以访问您希望其可以访问您希望其可以访问您希望其可以访问

7. （可选）对于 Additional contacts to notify（需要通知的其他联系人），请输入电子邮件地址以接收有关此支持案例更新的通知。您最多可添加 10 个电子邮件地址。
8. 选择 Review（审核）。
9. 在 Slack 通道中，查看案例详细信息。您可执行以下操作：
   - 选择 Edit（编辑）以更改案例详细信息。
   - 将文件添加到案例。为此，请按照以下步骤操作：
     a. 选择 Attach file（附加文件），选择 Slack 中的 + 图标，然后选择 Your computer（您的计算机）。
     b. 导航到您的文件并选择该文件。
     c. 在 Upload a file（上传文件）对话框中，输入 `@awssupport`，然后按发送消息  图标。

        注意

        - 您最多可以附加三个文件。每个文件最大可为 5 MB。
        - 如果将文件附加到支持案例，则须在 1 小时内提交案例。如果不附加，则须重新添加文件。
   - 选择 Share to channel（共享到通道），以与 Slack 通道中的其他人共享案例详细信息。在创建案例之前，您可以使用此选项与您的团队共享案例详细信息。
10. 查看案例详细信息，然后选择 Create case（创建案例）。

    以下示例显示了 Alexa 服务的技术支持案例。



    创建支持案例后，案例详细信息可能需要几分钟才能显示。
11. 当您的支持案例更新时，您可以选择 See details（查看详细信息）以查看案例信息。然后，您可执行以下操作：
    - 选择 Share to channel（共享到通道），以与 Slack 通道中的其他人共享案例详细信息。
    - 选择 Reply（回复）以添加通信。
    - 选择 Resolve case（解决案例）。

Note

如果您选择不在 Slack 中接收案例自动更新，可通过搜索支持案例查找 See details（查看详细信息）选项。

在 Slack 中回复支持案例

您可以为案例添加更新，例如案例详细信息和附件，并回复支持座席的回复。

Note

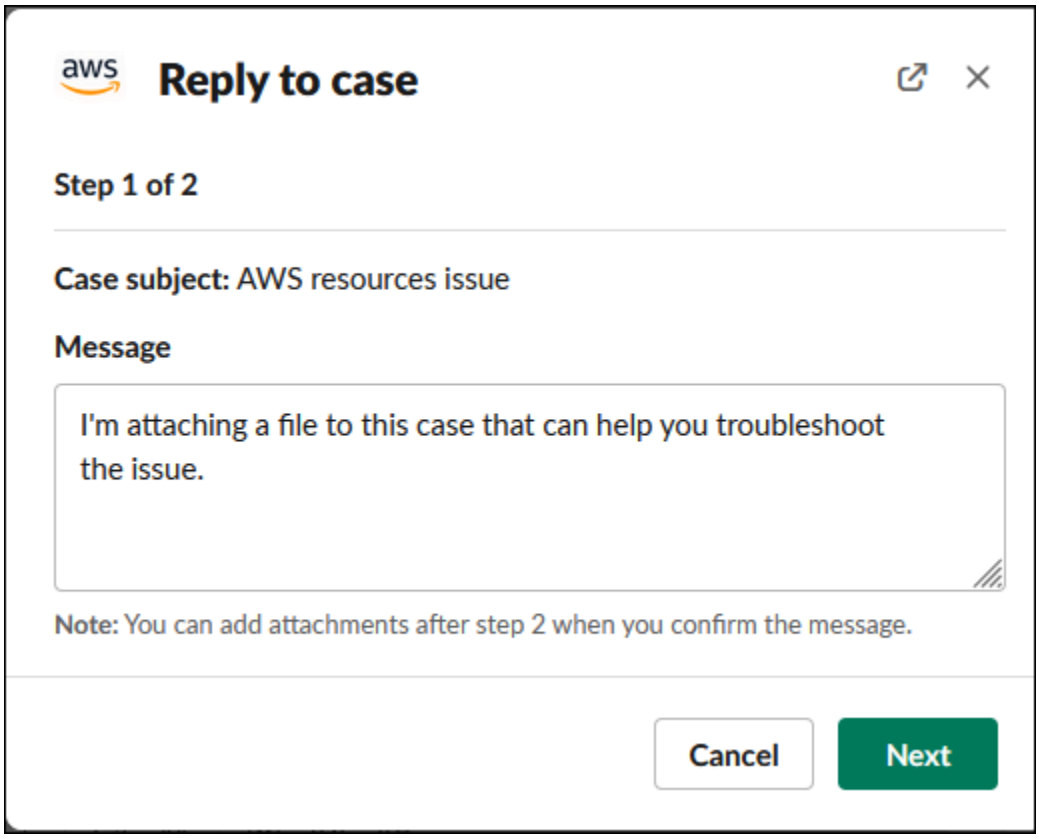
- 您还可以使用 AWS Support Center Console 回复支持座席。有关更多信息，请参阅更新、解决和重新打开您的案例 (p. 10)：
- 您无法为AWS Support应用程序创建通道中的案例添加通信信息。实时聊天通道仅会在实时聊天期间向座席发送消息。

在 Slack 中回复支持案例

1. 在您的 Slack 通道中，选择要响应的案例。您可以输入 `/awssupport search` 以查找您的支持案例。
2. 选择所需案例旁的 See details（查看详细信息）。
3. 在案例详细信息底部，选择 Reply（回复）。

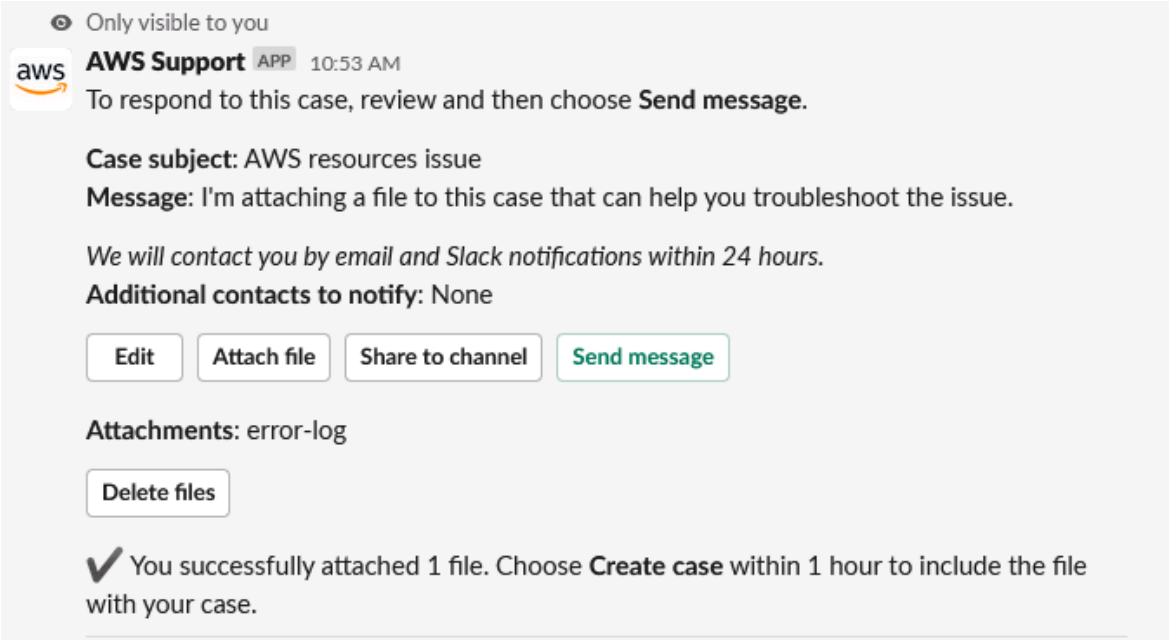


4. 在 Reply to case（回复案例）对话框中，在 Message（消息）字段中输入问题的简要描述。然后选择下一步。



5. 选择联系方式。可用的联系方式取决于您的案例类型和支持计划。
6. （可选）对于 Additional contacts to notify（需要通知的其他联系人），请输入您希望接收有关此支持案例更新通知的其他电子邮件地址。您最多可添加 10 个电子邮件地址。
7. 选择 Review（审核）。然后，您可以选择是否要编辑回复、附加文件或分享到通道。
8. 您准备好回复时，选择 Send message（发送消息）。
9. （可选）若要查看案例之前的通信信息，请选择 Previous correspondence（之前的通信信息）。若要查看短消息，请选择 Show full message（显示完整消息）。

Example ：在 Slack 中回复案例



加入与 AWS Support 的实时聊天会话

您为案例请求实时聊天时，您可以与支持座席选择您与支持座席选择与支持座席选择您与支持座席选择的实时聊天或者您与支持座席选择的实时聊天或者您与支持AWS Support座席选择。与支持座席以及您邀参加实时聊天的任何其他人与支持座席以及您邀请参加实时聊天的任何其他人通道。

Important

通过实时聊天加入频道的任何人都可以查看有关特定支持案例和聊天记录的详细信息。我们建议您只添加需要访问支持案例的用户。聊天频道或话题的任何成员也可以参与活跃的聊天。

Note

如果在实时聊天会话 这发生在聊天的之前、期间和之后，因此您可以使用聊天通道或聊天通道或线监控某个案例的所有更新。如果您选择新的聊天通道，请使用您邀请 App（您邀请AWS Support App）回复这些通信的配置通道。

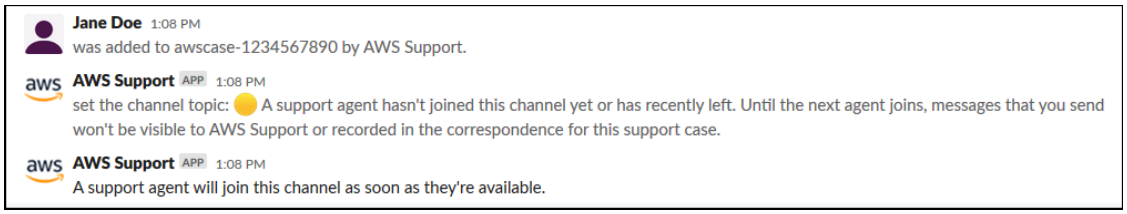
加入与的实时聊天加入与的实时聊天加入与的实时聊天加入与AWS Support的实时聊天的实时聊天

1. 在 Slack 应用程序中，导航到 AWS Support App 为您创建的通道。聊天通道包括您的支持案例 ID，例如 *awscase-1234567890*。

   Note

   AWS Support App 会将固定消息添加到实时聊天通道，其中包含有关支持案例的详细信息。从固定消息中，您可以结束聊天或解决案例。您可以在通道名称下找到该通道中的所有固定消息。

2. 支持座席加入该通道时，您可以与其聊聊您的支持案例。只有当支持座席加入该通道之后，座席才能看到该聊天中的消息，在此之前，这些消息也不会出现在您的案例通信信息中。



3. （可选）添加其他成员到聊天通道。默认情况下，聊天通道为专用。
4. 支持座席加入聊天后，聊天通道将处于活动状态，AWS Support App 将记录聊天。

您可以与座席聊聊您的支持案例，并将任何文件附件上传到该通道中。AWS Support App 会自动将您的文件和聊天日志保存到案例通信信息中。

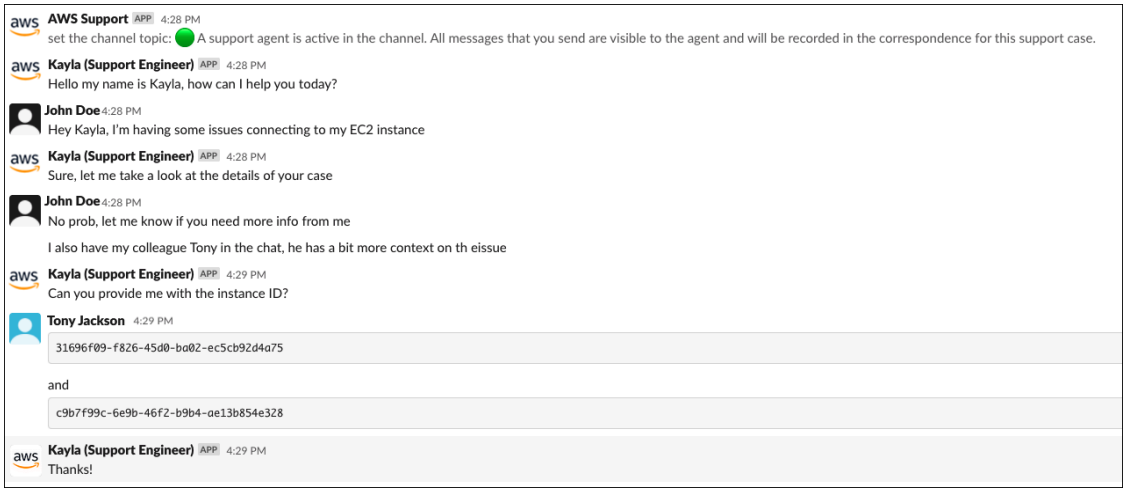
Note

您与支持座席聊天时，请注意 Slack 中 AWS Support App 的以下区别：

- 支持座席无法查看共享的消息或话题。若要共享消息或话题中的文本，请将该文本作为新消息输入。
- 如果您编辑或删除消息，座席仍可以看到原始消息。您必须再次输入新消息才能显示最新消息。

Example ：实时聊天会话

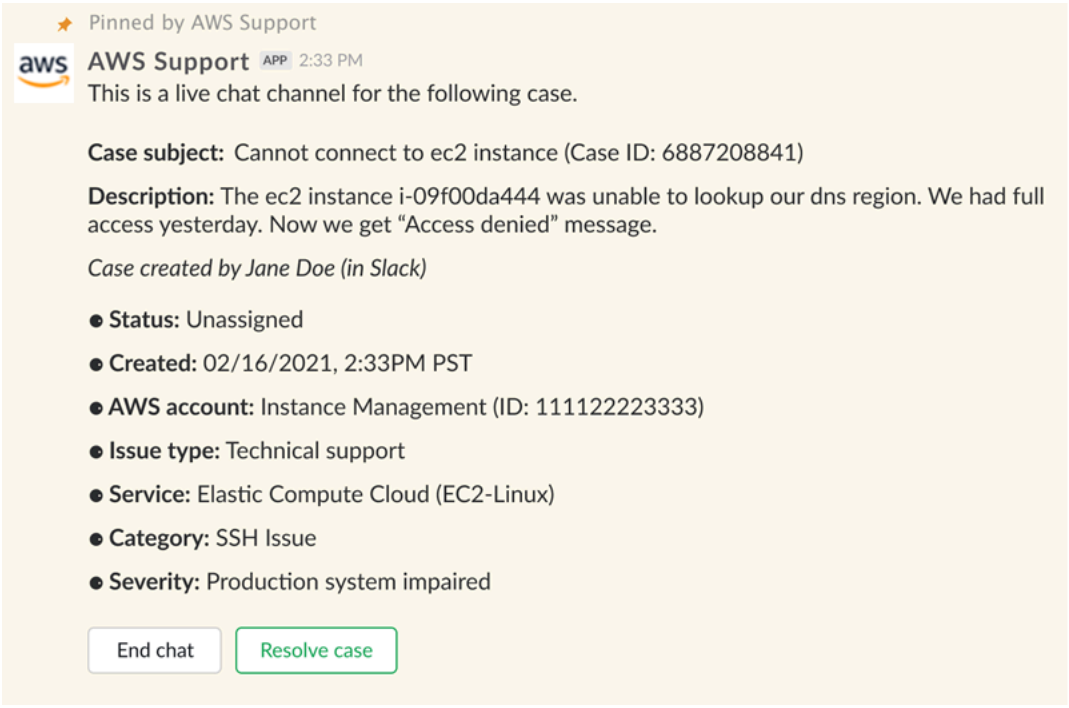
以下是与支持座席进行实时聊天会话以解决两个 Amazon Elastic Compute Cloud（Amazon EC2）实例连接问题的示例。



5. （可选）若要停止实时聊天，请选择 End chat（结束聊天）。支持座席离开通道，AWS Support App 停止记录实时聊天。您可以找到附加到此支持案例的案例通信信息的聊天记录。
6. 如果问题已解决，您可以从固定的消息中选择 Resolve case（解决案例）或者输入 `/awssupport resolve`。

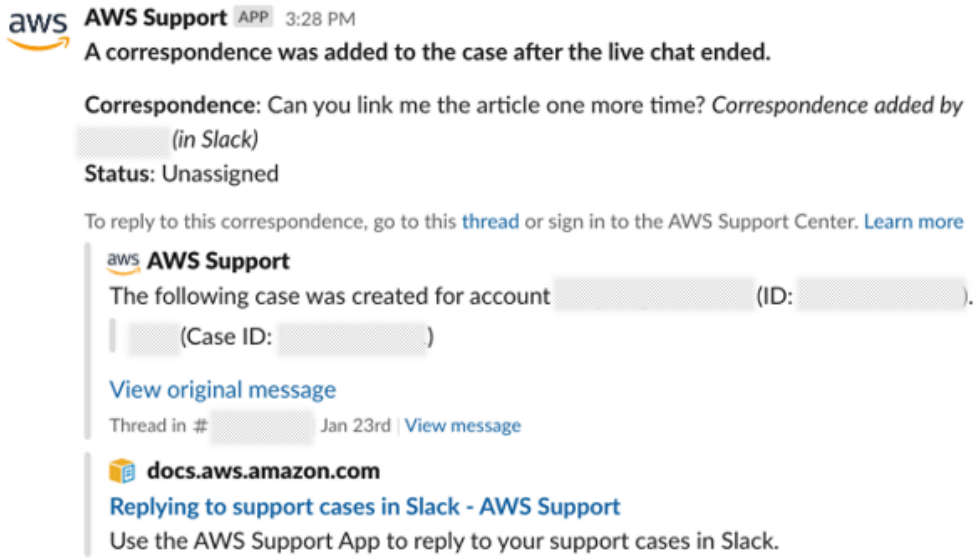
Example ：结束实时聊天

以下固定消息显示了有关 Amazon EC2 实例的案例详细信息。您可以在 Slack 通道名称下找到固定消息。



Example ：聊天通道中的通信信息通知

下面是在以下情况下收到通知的实时聊天通道的示例：其他协作者在聊天结束后添加了更新。



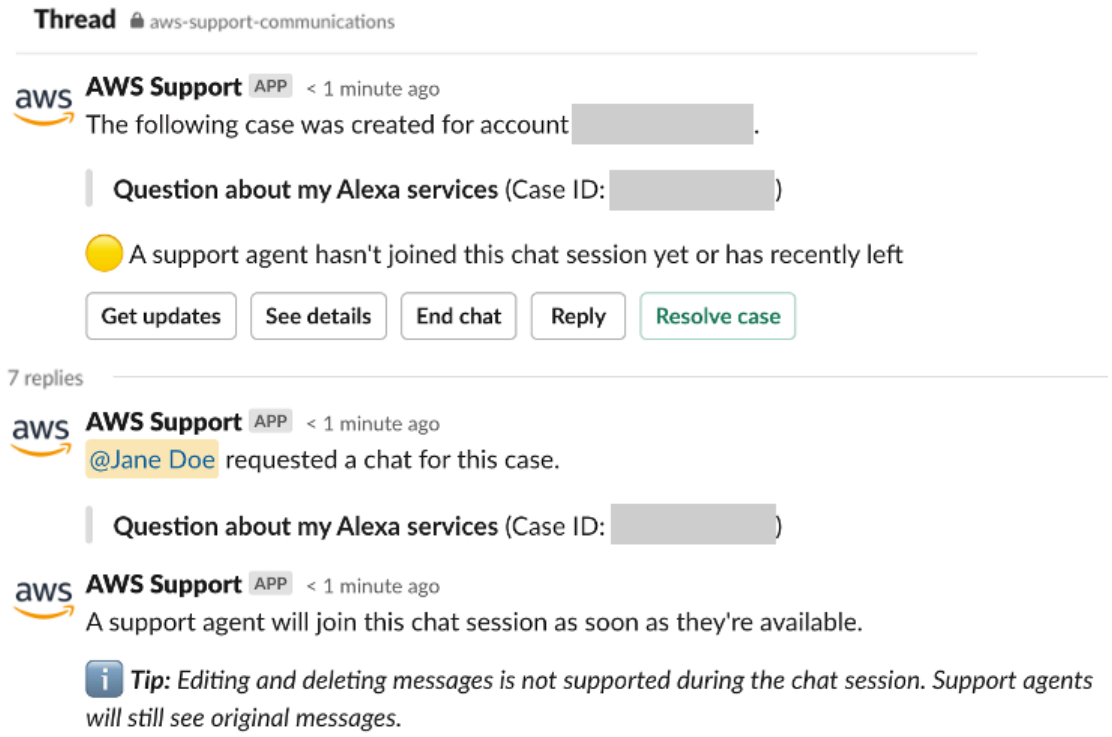
通知将指明聊天状态（已请求、正在进行或已结束），以及通信信息是由座席还是其他协作者添加的。Support App 还将尝试链接回发出此聊天请求的原始 Slack 话题或通道。您可以通过该通道或任何其他可以访问此案例的通道回复此案例。

加入与的实时聊天加入与的实时聊天加入与的实时聊天加入与AWS Support的实时聊天的实时聊天

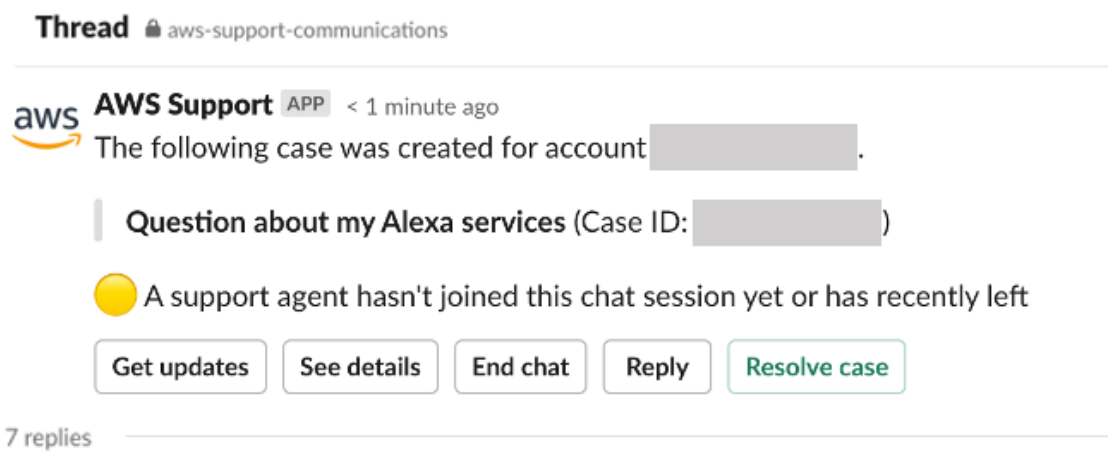
1. 在 Slack 应用程序中，导航到AWS Support App 用于聊天。在大多数情况下，这将是首次创建案例时开始的话题。
2. 支持座席加入该话，您可以与支持座席加入该聊天的实时聊天。只有当支持座席加入该聊天之后，座席才能看到该聊天中的消息，在此之前，这些消息也不会出现在您的案例通信信息中。

   Note

   即使聊天处于活动状态，也永远不会看到在聊天话题之外发送到此频道的消息。AWS Support



3. （可选）标记其他频道成员以在聊天话题中通知他们。
4. 支持座席加入聊天后，聊天将处于活动状态，AWS SupportApp 将记录聊天。与支持座席与支持座席与支持座席与支持座席与支持案例。AWS Support App 会自动将您的文件和聊天日志保存到案例通信信息中。
5. （可选）若要停止实时聊天，请从该话的实时聊天中选择 End（结束聊天）。支持座席离开该话，AWS Support App 停止记录实时聊天。您可以找到附加到此支持案例的案例通信信息的聊天记录。
6. 如果问题已解决，您可以从该话的实时消息中选择 Resolve（解决案例）。



在 Slack 中搜索支持案例

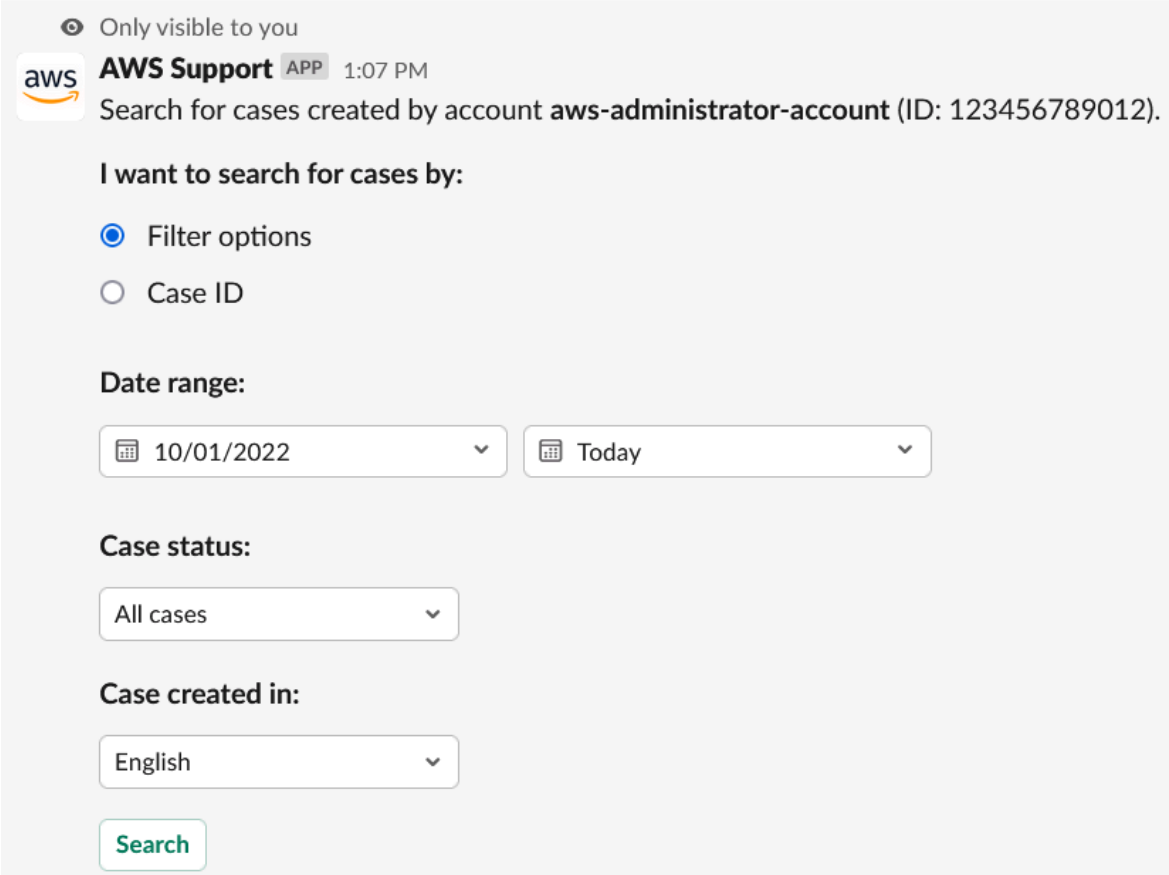
在 Slack 通道中，您可以从 AWS 账户 和其他配置了相同通道和工作区的账户中搜索支持案例。例如，如果您的账户（123456789012）和同事的账户（111122223333）在 AWS Support Center Console 中配置了相同的工作区和通道，您也可以使用 AWS Support App 搜索和更新彼此的支持案例。

要筛选您的搜索结果，可以使用以下选项：

- 账户 ID
- 案例 ID
- 案例状态
- 联系语言
- 日期范围

Example ：在 Slack 中搜索案例

以下示例显示了如何通过指定日期范围、案例状态和联系语言按 Filter options（筛选条件选项）搜索单个账户。



在 Slack 中搜索支持案例

1. 在 Slack 通道中输入以下命令：

   ```
   /awssupport search
   ```

2. 对于 I want to search for cases by: (我想通过以下方式搜索案例：) 选项，请选择以下选项之一：

   A. Filter options (筛选条件选项) ：您可以使用以下选项来筛选案例：

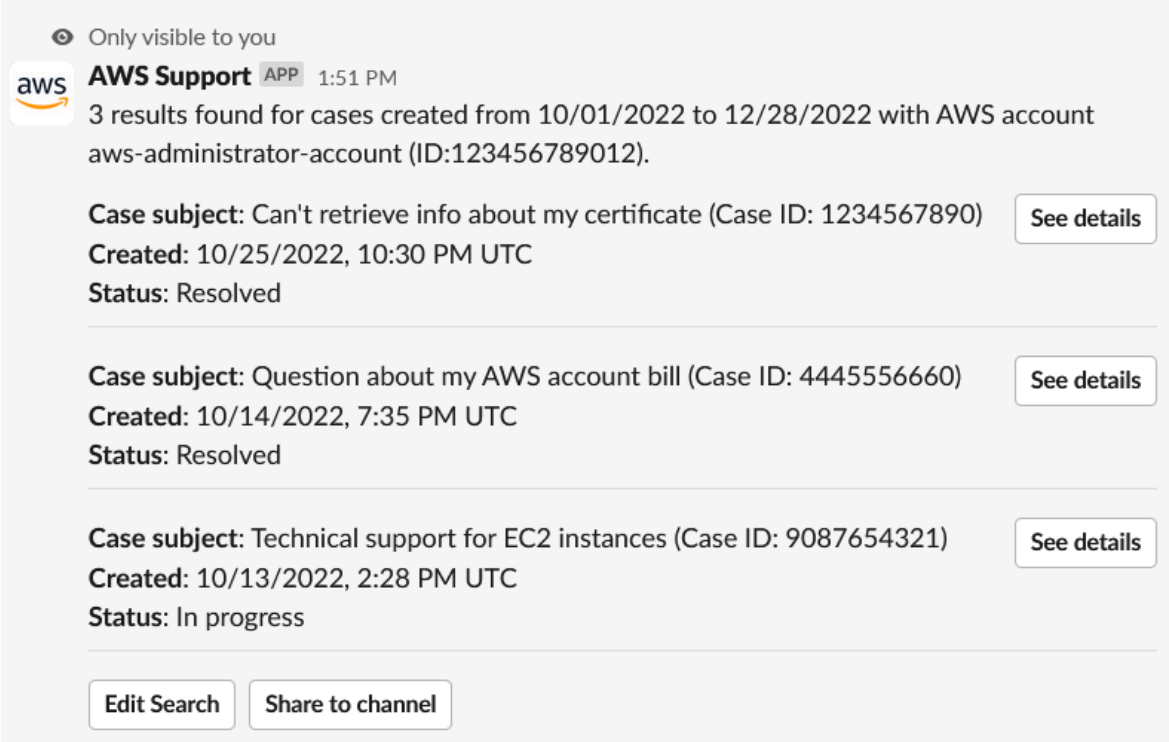
   - AWS 账户：仅当您在此通道中有多个账户时，才会显示此列表。
   - Date range (日期范围) ：案例的创建日期。
   - Case status (案例状态) ：当前案例状态，例如 All open cases (所有未决案例) 或 Resolved (已解决) 。
   - Case created in (案例创建语言) ：案例的联系语言。

   B. Case ID (案例 ID) ：输入案例 ID。一次只能输入一个案例 ID。如果您在通道中有多个账户，请选择 AWS 账户 来搜索案例。

3. 选择搜索。搜索结果会在 Slack 中显示。

使用您的搜索结果

以下示例从 AWS 账户 中返回三个支持案例。



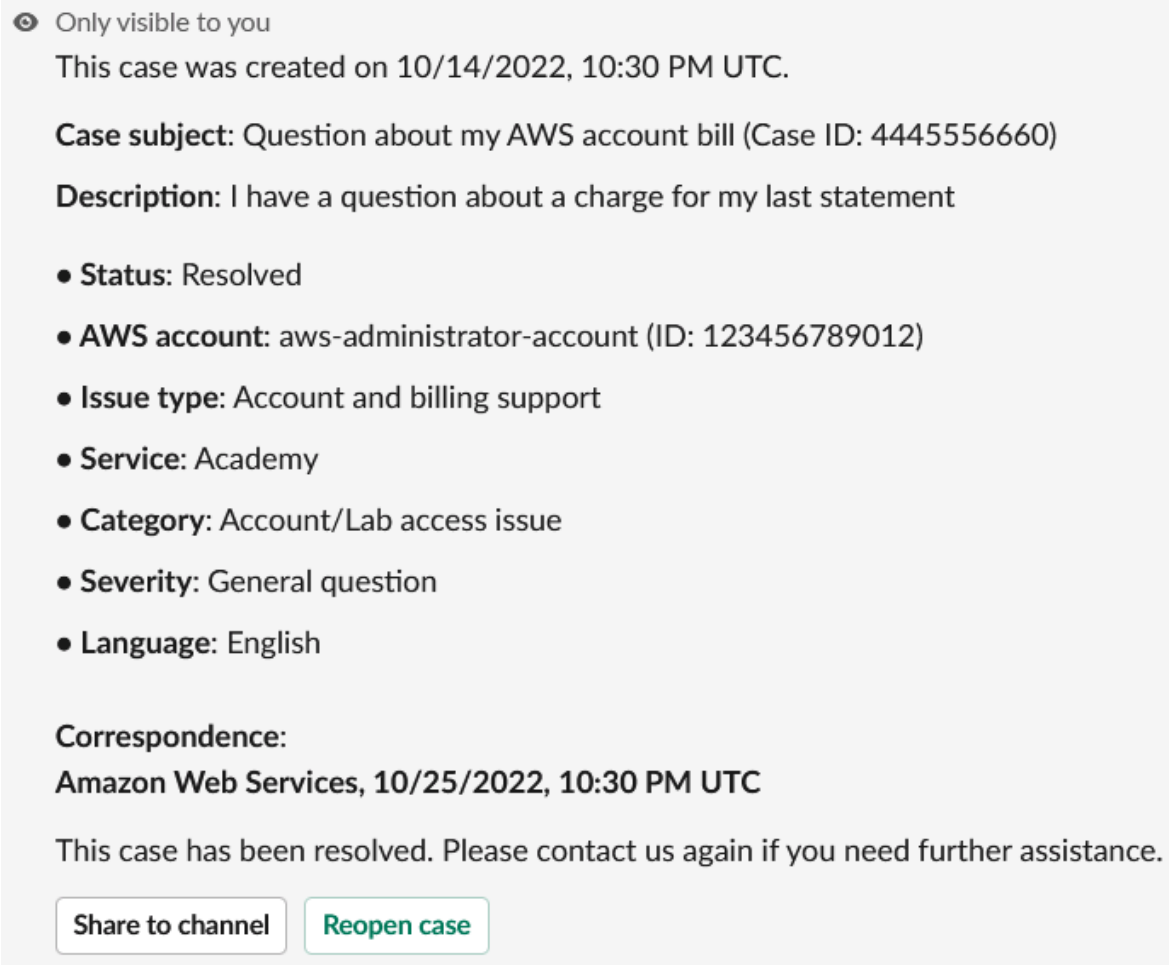
收到搜索结果后，您可以执行以下操作：

使用您的搜索结果

1. 选择 Edit Search（编辑搜索），更改您之前的筛选条件选项或案例 ID。
2. 选择 Share to channel（分享到通道）以与通道分享搜索结果。
3. 选择 See details（查看详细信息），查看有关案例的更多信息。您可以选择 Show full message（显示完整消息）查看其余的最新通信信息。
4. 如果您按 Filter options（筛选条件选项）进行搜索，搜索结果可能会返回多个案例。选择 Next 5 results（接下来的 5 个结果）或 Previous 5 results（之前的 5 个结果），查看接下来或之前的 5 个案例。

Example ：已解决的支持案例

以下示例显示了选择 See details（查看详细信息）后已解决的账户和账单问题支持案例。

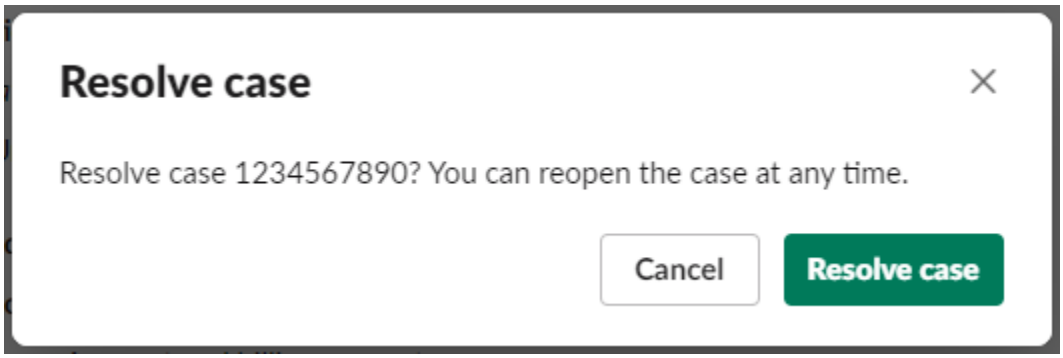


在 Slack 中解决支持案例

如果您不再需要支持案例，或者已修复了问题，则您可以直接在 Slack 中解决支持案例。这也解决了 AWS Support Center Console 中的案例。解决案例后，您可以稍后重新打开该案例。

在 Slack 中解决支持案例

1. 在您的 Slack 通道中，导航到支持案例。请参阅在 Slack 中搜索支持案例 (p. 176)。
2. 选择案例的 See details（查看详细信息）。
3. 选择 Resolve case（解决案例）。
4. 在 Resolve case（解决案例）对话框中，选择 Resolve case（解决案例）。您可以在 Slack 通道中或从支持中心控制台中重新打开案例。

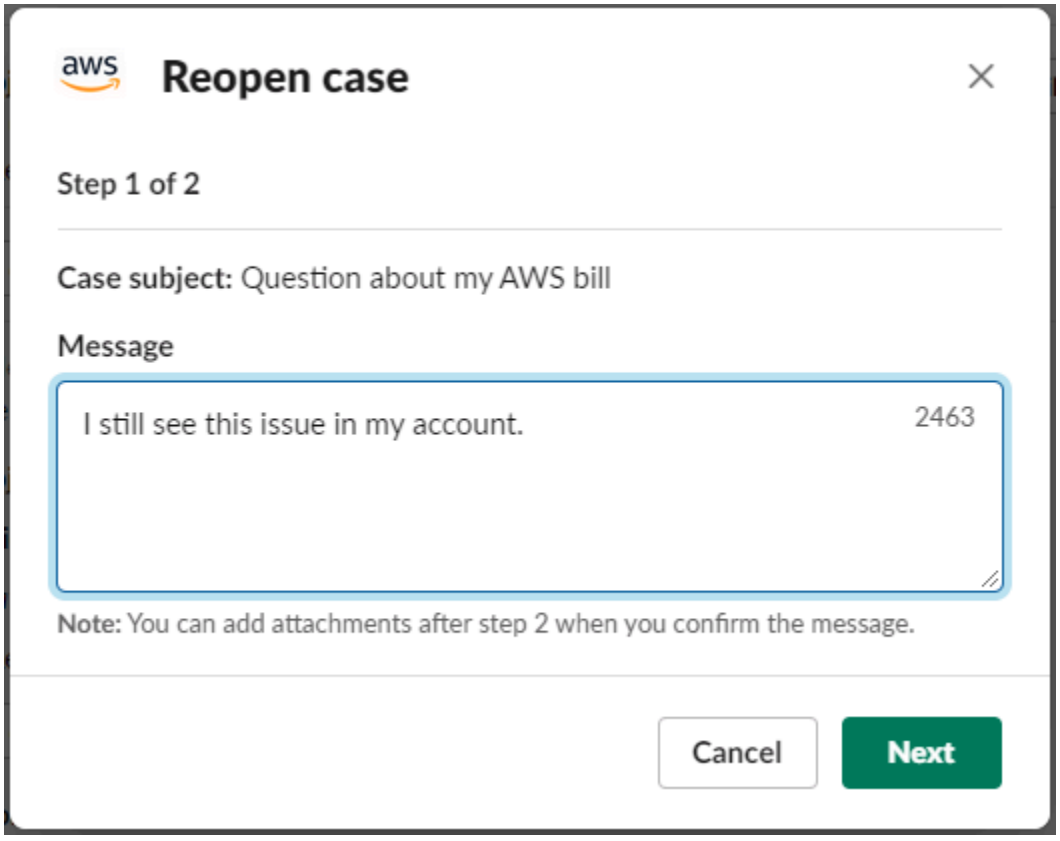


在 Slack 中重新打开支持案例

解决支持案例后，您可以从 Slack 中重新打开该案例。

在 Slack 中重新打开支持案例

1. 查找要在 Slack 中重新打开的支持案例。请参阅在 Slack 中搜索支持案例 (p. 176)。
2. 选择 See details（查看详细信息）。
3. 选择 Reopen case（重新打开案例）。
4. 在 Reopen case（重新打开案例）对话框中，在 Message（消息）字段中输入问题的简要描述。
5. 选择下一步。



6. （可选）输入其他联系人。

7. 选择 Review（审核）。
8. 查看案例的详细信息，然后选择 Send message（发送消息）。您的案例会重新打开。如果您请求与支持座席进行新的实时聊天，Slack 会使用与之前的实时聊天通道或聊天通道或聊天通道相同的聊天通道。如果您请求进行实时聊天但到目前为止还未进行过实时聊天，则会打开一个新的聊天通道。如果您请求进行实时聊天但到目前为止还未进行过实时聊天，则会使用当前通道中的话题。

请求增加服务限额

您可以从 Slack 通道为账户请求增加服务限额。

请求增加服务限额

1. 在 Slack 通道中输入以下命令：

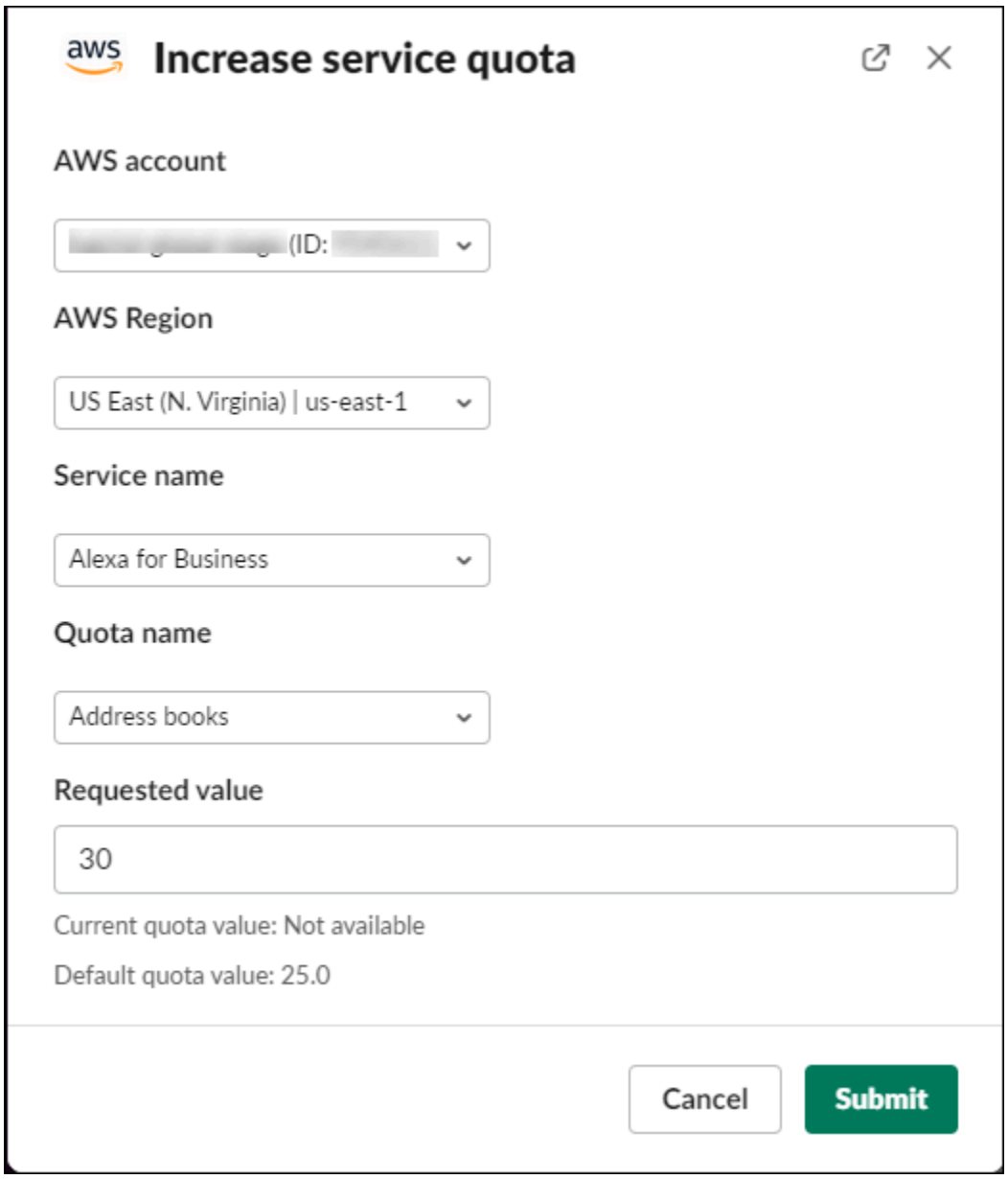
   ```
   /awssupport quota
   ```

2. 在 Increase service quota（增加服务限额）对话框中，输入以下信息：

   a. 选择 AWS 账户。
   b. 选择 AWS 区域。
   c. 选择 Service name（服务名称）。
   d. 选择 Quota name（限额名称）。
   e. 输入用于增加限额的 Requested value（请求的值）。您必须输入一个大于默认限额的值。

3. 选择 Submit（提交）。

Example ：适用于企业版 Alexa 的增加限额



您也可以在服务限额控制台中查看您的请求。有关更多信息，请参阅 Service Quotas 用户指南 中的请求增加配额。

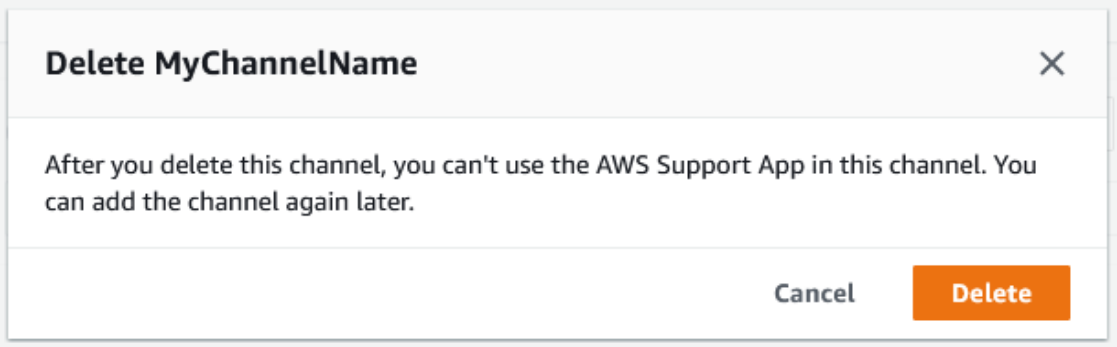
从 AWS Support App 中删除 Slack 通道配置

如果您不需要通道配置，可将其从 AWS Support App 中删除。此操作将仅从 AWS Support App 和 AWS Support Center Console 中删除通道。通道未从 Slack 中删除。

您最多可以为 AWS 账户 添加 20 个通道。如果您已达到此限额，必须先删除一个通道，然后才能添加另一个。

删除 Slack 通道配置

1. 登录支持中心工作台，然后选择 Slack configuration（Slack 配置）。
2. 在 Slack configuration（Slack 配置）页面上，Channels（通道）下，选择通道名称，然后选择 Delete（删除）。
3. 在 Delete channel name（删除通道名称）对话框中，选择 Delete（删除）。您之后可以再次将此通道添加到 AWS Support App。



从 AWS Support App 中删除 Slack 工作区配置

如果您不需要工作区配置，可将其从 AWS Support App 中删除。此操作将仅从 AWS Support App 和 AWS Support Center Console 中删除工作区。工作区不会从 Slack 中删除。

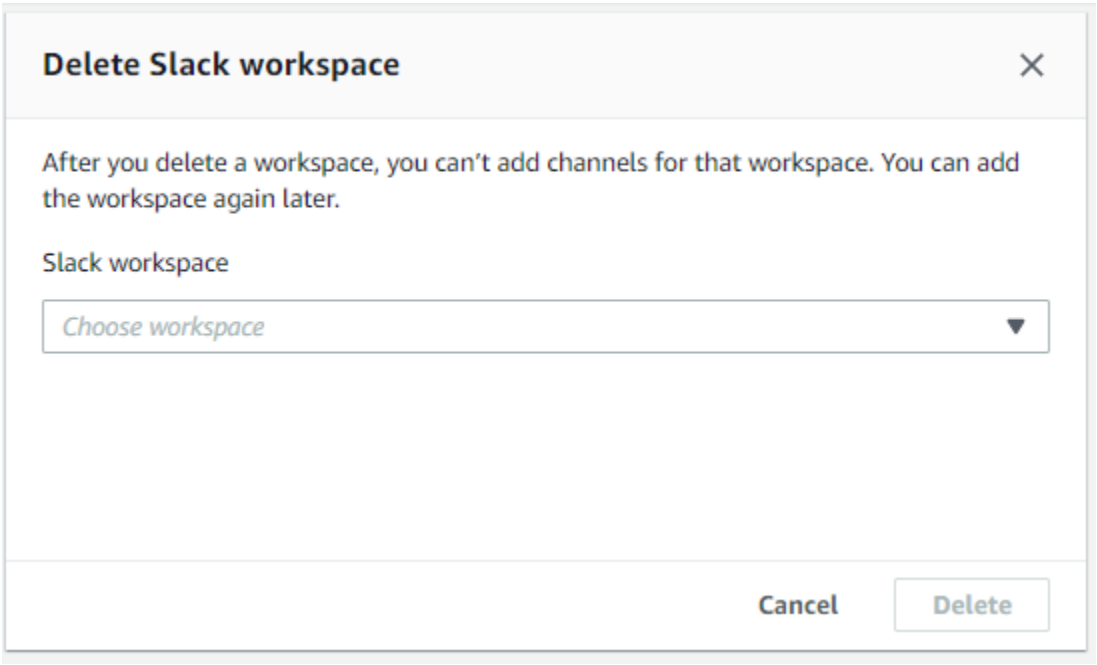
您最多可以为 AWS 账户 添加 5 个工作区。如果您已达到此限额，必须先删除一个 Slack 工作区，然后才能添加另一个。

Note

如果您将此工作区中的通道添加到 AWS Support App，则必须先删除这些通道，然后才能删除工作区。请参阅从 AWS Support App 中删除 Slack 通道配置 (p. 182)。

删除 Slack 工作区配置

1. 登录到 AWS Support Center Console，然后选择 Slack configuration（Slack 配置）。
2. 在 Slack 配置页面上，Slack workspaces（Slack 工作区）下，选择 Delete a workspace（删除工作区）。
3. 在 Delete Slack workspace（删除 Slack 工作区）对话框中，选择 Slack 工作区名称，然后选择 Delete（删除）。您之后可以再次将工作区添加到 AWS 账户。



Slack 中的 AWS Support App 命令

Slack 通道命令

您可以在邀请 AWS Support App 加入的 Slack 通道中输入以下命令。此 Slack 通道名称也会显示为 AWS Support Center Console 中的已配置通道。

`/awssupport create` 或者 `/awssupport create-case`

创建支持案例。

`/awssupport search` 或者 `/awssupport search-case`

搜索案例。您可以搜索 AWS 账户 中为 AWS Support App 配置了同一 Slack 通道的支持案例。

`/awssupport quota` 或者 `/awssupport service-quota-increase`

请求提升服务限额。

实时聊天通道命令

您可以在实时聊天通道中输入以下命令。这是AWS Support App 在您选择通话时为您创建的通道，这是 App 在您通话时为您创建的通道AWS Support。聊天通道包括您的支持案例 ID，例如 *awscase-1234567890*。

Note

使用当前频道中的话题进行实时聊天时，以下命令不可用。取而代之的是，使用初始话题消息上附加的按钮结束聊天、邀请新的代理人或解决案例。

`/awssupport endchat`

删除支持座席并结束实时聊天会话。

`/awssupport invite`

邀请新的支持座席加入此通道。

`/awssupport resolve`

解决支持案例。

在 AWS Support Center Console 中查看 AWS Support App 通信信息

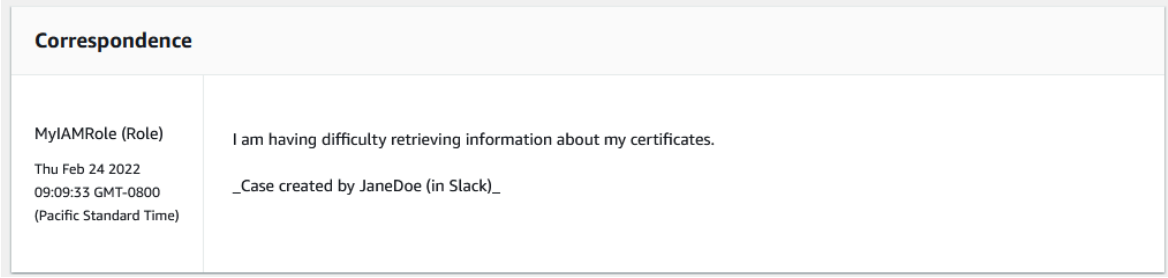
您在 Slack 通道中为账户创建、更新或解决支持案例时，也可以登录支持中心控制台查看案例。您可以查看案例通信信息以确定该案例是否已在 Slack 通道中更新，查看与支持座席的聊天记录，以及查找您从 Slack 上传的任何附件。

查看来自 Slack 的通信信息

1. 登录账户的 AWS Support Center Console。
2. 选择您的支持案例。
3. 在 Correspondence（通信信息）中，您可以查看是否在 Slack 通道中创建和更新该案例。

Example ：支持案例

在下列屏幕截图中，Jane Doe 在 Slack 中重新打开了一个支持案例。支持中心控制台的支持案例中将显示此通信信息。



使用 AWS CloudFormation 创建 Slack 中的 AWS Support App 资源

Slack 中的 AWS Support App 与 AWS CloudFormation 集成，后者是一项服务，可帮助您对 AWS 资源进行建模和设置，这样您只需花较少的时间来创建和管理资源与基础设施。您可以创建一个描述所需的全部 AWS资源（例如您的AccountAlias和SlackChannelConfiguration）的模板，然后将为您预置和配置这些资源。AWS CloudFormation

在您使用 AWS CloudFormation 时，可重复使用您的模板来不断地重复设置您的 AWS Support App 资源。描述您的资源一次，然后在多个 AWS 账户 和区域中反复预置相同的资源。

AWS Support App 和 AWS CloudFormation 模板

要为 AWS Support App 和相关服务预置和配置资源，您必须了解 AWS CloudFormation 模板。模板是 JSON 或 YAML 格式的文本文件。这些模板描述要在 AWS CloudFormation 堆栈中调配的资源。如果您不

熟悉 JSON 或 YAML，可以在 AWS CloudFormation Designer 的帮助下开始使用 AWS CloudFormation 模板。有关更多信息，请参阅 AWS CloudFormation 用户指南中的什么是 AWS CloudFormation Designer？。

AWS Support应用程序支持创建您的AccountAliasSlackChannelConfiguration和AWS CloudFormation。有关更多信息（包括和SlackChannelConfiguration资源的 JSON 和 YAML 模板示例），请参阅《AWS CloudFormation用户指南》中的 AWS SupportApp 资源类型参考。AccountAlias

为您的组织创建 Slack 配置资源

您可以使用CloudFormation模板来创建AWS Support App 所需的资源。如果您是组织的管理账户，则可以使用模板在 AWS Organizations 中为成员账户创建这些资源。

例如，您可以使用模板为组织中的所有账户创建相同的 Slack 工作区配置，随后使用单独的模板为特定 AWS 账户 或组织单位（OU）创建不同的 Slack 通道配置。您也可以使用模板来创建 Slack 工作区配置，以便成员账户为其 AWS 账户 配置所需的 Slack 通道。

您可以选择是否使用 CloudFormation 模板。如果不使用 CloudFormation 模板，则可以改为完成以下手动步骤：

- 在 AWS Support Center Console 中创建 AWS Support App 资源。
- 使用 AWS Support 创建支持案例，以授权多个账户 (p. 160)使用 AWS Support App。
- 调用 RegisterSlackWorkspaceForOrganization API 操作为您的账户注册 Slack 工作区。CloudFormation 堆栈会为您调用该 API 操作。

按照以下步骤将 CloudFormation 模板上传到您的组织。您可以使用 AWS Support App 资源类型参考页面中的示例模板。

该模板会告知 CloudFormation 创建以下资源：

- Slack 通道配置。
- Slack 工作区配置。
- 名为 `AWSSupportSlackAppCFNRole` 的 IAM 角色。附加 AWSSupportAppFullAccess AWS 托管策略。

目录

- 为 Slack 更新您的 CloudFormation 模板 (p. 186)
- 为管理账户创建堆栈 (p. 187)
- 为组织创建堆栈集 (p. 187)

为 Slack 更新您的 CloudFormation 模板

首先，请使用以下模板来创建堆栈。您必须将模板替换为 Slack 工作区和通道的有效值。

> **Note**
>
> 我们不建议使用该模板为您的组织创建 AccountAlias 资源。AccountAlias 资源在 AWS Support App 中唯一标识 AWS 账户。您的成员账户可以在支持中心控制台中输入账户名称。有关更多信息，请参阅授权 Slack 工作区 (p. 159)：

为 Slack 更新您的 CloudFormation 模板

1. 如果您是组织的管理账户，则必须手动为您的账户授权 Slack 工作区，然后您的成员账户才能使用CloudFormation来创建资源。如果尚未授权，请参阅 授权 Slack 工作区 (p. 159)。

2. 从 AWS Support App 资源类型参考页面中复制所需资源的 JSON 或 YAML 模板。
3. 在文本编辑器中，将模板粘贴到新文件中。
4. 在模板中，指定所需的参数。至少需要替换以下字段的值：

   - 带有 Slack 工作区 ID 的 `TeamId`
   - 带有 Slack 通道 ID 的 `ChannelId`
   - 带有用于标识 Slack 通道配置名称的 `ChannelName`

   Tip

   要查找工作区和通道 ID，请在浏览器中打开 Slack 通道。在 URL 中，您的工作区 ID 是第一个标识符，通道 ID 是第二个标识符。例如，在 https://app.slack.com/client/T012ABCDEFG/C01234A5BCD 中，T012ABCDEFG 是工作区 ID，C01234A5BCD 是通道 ID。
5. 将文件另存为 JSON 或 YAML 文件。

为管理账户创建堆栈

接下来，您必须在组织中为管理账户创建堆栈。此步骤会为您调用 RegisterSlackWorkspaceForOrganization API 操作并使用 Slack 授权工作区。

Note

我们建议您上传在上一步中为管理账户更新的 Slack 工作区配置模板。除非您还配置管理账户以使用 AWS Support App，否则无需上传 Slack 通道配置模板。

为管理账户创建堆栈

1. 使用组织的管理账户登录到AWS Management Console。
2. 打开 AWS CloudFormation 控制台，地址：https://console.aws.amazon.com/cloudformation。
3. 如果尚未设置，请在 Region selector（区域选择器）中，选择以下 AWS 区域 中的一个：

   - 欧洲地区（法兰克福）
   - 欧洲地区（爱尔兰）
   - 欧洲地区（伦敦）
   - 美国东部（弗吉尼亚州北部）
   - 美国东部（俄亥俄州）
   - 美国西部（俄勒冈州）
   - 亚太地区（新加坡）
   - 亚太地区（东京）
   - 加拿大（中部）
4. 按照步骤创建堆栈。有关更多信息，请参阅在 AWS CloudFormation 控制台上创建堆栈。

   CloudFormation 成功创建堆栈后，您可以使用相同的模板为组织创建堆栈集。

为组织创建堆栈集

接下来，对 Slack 工作区配置使用相同的模板，以创建具有 `service-managed` 权限的堆栈集。您可以使用堆栈集为整个组织创建堆栈，也可以指定所需的 OU。有关更多信息，请参阅创建堆栈集。

此过程还会为您调用 RegisterSlackWorkspaceForOrganization API 操作。此 API 操作会为成员账户使用 Slack 授权工作区。

为组织创建堆栈集

1. 使用组织的管理账户登录到AWS Management Console。
2. 打开 AWS CloudFormation 控制台，地址：https://console.aws.amazon.com/cloudformation。
3. 如果尚未设置，请在 Region selector（区域选择器）中，选择您在上一步中使用的相同 AWS 区域。
4. 在导航窗格中，选择 StackSets。
5. 选择 “创建”StackSet。
6. 在 Choose a template（选择模板）页面上，保留以下选项的默认选项：
   - 在 Permissions（权限）下，保留 Service-managed permissions（服务托管权限）。
   - 对于 Prerequisite - Prepare template（先决条件 – 准备模板），请保留 Template is ready（模板已就绪）。
7. 在 Specify template（指定模板）下，选择 Upload a template file（上传模板文件），然后选择 Choose file（选择文件）。
8. 选择文件，然后选择 Next（下一步）。
9. 在 Specify details（指定StackSet详细信息）页面上**`support-app-slack-workspace`**，输入堆栈名称，如描述并选择 Next（下一步）。
10. 在 Configure options（配置StackSet选项）页面上，保留默认选项，然后选择下一步。
11. 在 Set deployment options（设置部署选项）页面上，对于 Add stacks to stack set（将堆栈添加到堆栈集），保留默认的 Deploy new stacks（部署新堆栈）选项。
12. 对于 Deployment targets（部署目标），选择是否为整个组织或特定 OU 创建堆栈。如果选择 OU，请输入 OU ID。
13. 对于 Specify regions（指定区域），仅输入以下 AWS 区域 之一：
    - 欧洲地区（法兰克福）
    - 欧洲地区（爱尔兰）
    - 欧洲地区（伦敦）
    - 美国东部（弗吉尼亚州北部）
    - 美国东部（俄亥俄州）
    - 美国西部（俄勒冈州）
    - 亚太地区（新加坡）
    - 亚太地区（东京）
    - 加拿大（中部）

    备注:

    - 为了简化工作流，我们建议您使用在步骤 3 中选择的相同 AWS 区域 。
    - 选择多个 AWS 区域 可能会导致创建堆栈时发生冲突。
14. 对于 Deployment options（部署选项）和 Failure tolerance - optional（容错能力 – 可选）下，输入在 CloudFormation 停止操作之前堆栈可能失败的账户数。我们建议您输入要添加的账户数并减去一。例如，如果您指定的 OU 有 10 个成员账户，则输入 9。这意味着，即使 CloudFormation 操作失败 9 次，也至少有一个账户会成功。
15. 选择下一步。
16. 在 Review（审核）页面上，检查您的选择，然后选择 Submit（提交）。您可以在 Stack instances（堆栈实例）选项卡上检查堆栈状态。
17. （可选）重复此步骤以上传 Slack 通道配置的模板。示例模板还会创建 IAM 角色并附加 AWS 托管策略。该角色具有访问其他服务所需的权限。有关更多信息，请参阅管理对 AWS Support App 的访问 (p. 155)：

如果您不创建堆栈集来创建 Slack 通道配置，则您的成员账户可以手动配置 Slack 通道。有关更多信息，请参阅配置 Slack 通道 (p. 160)：

CloudFormation创建堆栈后，每个成员账户都可以登录Support 中心控制台并找到其配置的 Slack 工作区和通道。然后，他们可以将 AWS Support App 用于自己的 AWS 账户。请参阅在 Slack 通道中创建支持案例 (p. 165)。

Tip

如果您需要上传新模板，我们建议您使用之前指定的相同 AWS 区域。

了解有关 CloudFormation 的更多信息

要了解有关 CloudFormation 的更多信息，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation API 参考
- AWS CloudFormation 命令行界面用户指南

使用 Terraform 创建 AWS Support App 资源

您也可以使用 Terraform 为 AWS 账户 创建 AWS Support App 资源。Terraform 是一infrastructure-as-code款可用于云应用程序。您可以使用 Terraform 创建AWS Support App 资源，而不是将CloudFormation堆栈部署到账户。

安装 Terraform 后，您可以指定所需的 AWS Support App 资源。Terraform 会调用 RegisterSlackWorkspaceForOrganization API 操作为您注册 Slack 工作区，并创建资源。然后，您可以登录支持中心控制台并找到您配置的 Slack 工作区和通道。

注意

- 如果您是组织的管理账户，则必须手动为您的账户授权 Slack 工作区，然后您的成员账户才能使用 Terraform 来创建资源。如果尚未授权，请参阅 授权 Slack 工作区 (p. 159)。
- 与CloudFormation堆栈集不同，您不能使用 Terraform 为组织中的 OU 创建AWS Support App 资源。
- 您还可以在 AWS CloudTrail 中找到来自 Terraform 的更新的事件历史记录。这些事件的 `eventSource` 将是 `cloudcontrolapi.amazonaws.com` 和 `supportapp.amazonaws.com`。有关更多信息，请参阅使用 AWS CloudTrail 记录 Slack API 调用中的 AWS Support App (p. 316)：

了解更多信息

要了解有关 Terraform 的更多信息，请参阅以下主题：

- Terraform installation (Terraform 安装)
- Terraform 教程：为构建基础架构AWS
- `awscc_support_app_account_alias`
- `awscc_supportapp_slack_workspace_configuration`
- `awscc_supportapp_slack_channel_configuration`

AWS Support 中的安全性

AWS 十分重视云安全性。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是AWS和您的共同责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为 AWS 合规性计划的一部分，第三方审计人员将定期测试和验证安全措施的有效性。要了解适用于 AWS Support 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性 - 您的责任由您使用的 AWS 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 AWS Support 时应用责任共担模型 以下主题说明如何配置 AWS Support 以实现您的安全性和合规性目标。您还会了解如何使用其他 Amazon Web Services 以帮助您监控和保护 AWS Support 资源。

主题

- AWS Support 中的数据保护 (p. 190)
- AWS Support 案例的安全性 (p. 191)
- 适用于 AWS Support 的 Identity and Access Management (p. 191)
- 事件响应 (p. 235)
- AWS Support 和 AWS Trusted Advisor 中的日志记录和监控 (p. 235)
- AWS Support 的合规性验证 (p. 236)
- AWS Support 中的故障恢复能力 (p. 236)
- AWS Support 中的基础设施安全性 (p. 236)
- AWS Support 中的配置和漏洞分析 (p. 237)

AWS Support 中的数据保护

AWS责任共担模式适用于 AWS Support 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS Cloud 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center (successor to AWS Single Sign-On) 或 AWS Identity and Access Management (IAM) 设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务 中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。

- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如 Name（名称）字段）。这包括使用控制台、API、AWS CLI 或 AWS SDK 处理 AWS Support 或其他 AWS 服务时。您在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

AWS Support 案例的安全性

您创建支持案例时，您拥有支持案例中包含的信息。AWS 未经您的许可无法访问 AWS 账户 数据。AWS 不会与第三方共享您的信息。

创建支持案例时，请注意以下几点：

- AWS Support 使用在 `AWSServiceRoleForSupport` 服务相关角色中定义的权限以调用其他 AWS 服务 为您解决客户问题。有关更多信息，请参阅使用服务相关角色AWS Support和AWS托管策略：AWSSupportServiceRolePolicy。
- 您可以查看在 AWS 账户 中发生的对 AWS Support 的 API 调用。例如，您的账户中有人创建或解决支持案例时，您可以查看日志信息。有关更多信息，请参阅使用 AWS CloudTrail 记录 AWS Support API 调用。
- 您可以使用 AWS Support API 调用 `DescribeCases` API。此 API 返回支持案例信息，例如案例 ID、创建和解决日期以及与支持座席的通信信息。创建案例后，您最多可以查看 12 个月内的案例详细信息。有关更多信息，请参阅《AWS Support API 参考》中的 DescribeCases。
- 您的支持案例遵循 AWS Support 的合规性验证。
- 创建支持案例时，AWS 无法访问您的账户。如有必要，支持座席使用屏幕共享工具远程查看您的屏幕，同时识别并解决问题。此工具仅用于查看。AWS Support 在屏幕共享会话期间无法为您执行操作。您必须同意与支持座席共享屏幕。有关更多信息，请参阅 AWS Support 常见问题。
- 您可以更改 AWS Support 计划以获取账户所需的帮助。有关更多信息，请参阅比较 AWS Support Plans 和更改您的 AWS Support 计划。

适用于 AWS Support 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一项 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）来使用 AWS Support 资源。IAM 是一项无需额外费用即可使用的 AWS 服务。

主题

- 受众 (p. 192)
- 使用身份进行身份验证 (p. 192)
- 使用策略管理访问 (p. 193)
- AWS Support 如何与 IAM 协同工作 (p. 194)
- AWS Support 基于身份的策略示例 (p. 196)
- 使用服务相关角色 (p. 197)
- AWS适用于 AWS Support 的托管策略 (p. 201)
- 管理对 AWS Support 中心的访问 (p. 221)

- 管理对 AWS Support 计划的访问权限 (p. 224)
- 管理对 AWS Trusted Advisor 的访问 (p. 226)
- 对 AWS Support 身份和访问进行故障排除 (p. 234)

受众

使用 AWS Identity and Access Management (IAM) 的方式因您可以在 AWS Support 中执行的操作而异。

服务用户 – 如果使用 AWS Support 服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多 AWS Support 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问 AWS Support 中的功能，请参阅 对 AWS Support 身份和访问进行故障排除 (p. 234)。

服务管理员 – 如果您在公司负责管理 AWS Support 资源，则您可能具有 AWS Support 的完全访问权限。您有责任确定您的服务用户应访问哪些 AWS Support 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 AWS Support 搭配使用的更多信息，请参阅AWS Support 如何与 IAM 协同工作 (p. 194)。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 AWS Support 的访问权限的详细信息。要查看您可在 IAM 中使用的 AWS Support 基于身份的策略示例，请参阅 AWS Support 基于身份的策略示例 (p. 196)。

使用身份进行身份验证

身份验证是您使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 AWS）。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWS IAM Identity Center (successor to AWS Single Sign-On)(IAM Identity Center) 用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接代入角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录到 AWS 的更多信息，请参阅《AWS 登录 用户指南》中的 如何登录到您的 AWS 账户。

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包 (SDK) 和命令行界面（CLI），以便使用您的凭证对您的请求进行加密签名。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行对请求签名的更多信息，请参阅《AWS 一般参考》中的 签名版本 4 签名流程。

无论使用何种身份验证方法，您可能需要提供其他安全信息。例如，AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center (successor to AWS Single Sign-On) 用户指南》中的 多重身份验证 和《IAM 用户指南》中的 在 AWS 中使用多重身份验证（MFA）。

AWS 账户根用户

当您创建 AWS 账户时，最初使用的是一个对账户中所有 AWS 服务和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 AWS Account Management 参考指南中的需要根用户凭证的任务。

IAM 用户和组

IAM 用户是AWS 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景

需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 对于需要长期凭证的使用场景定期轮换访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

IAM 角色

IAM 角色是AWS 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 AWS Management Console 中暂时代入 IAM 角色。您可以调用 AWS CLI 或 AWS API 操作或使用自定义 URL 以担任角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）– 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center (successor to AWS Single Sign-On) 用户指南》中的 权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 – 某些 AWS 服务使用其它 AWS 服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 主体权限 – 当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其它相关操作，请参阅服务授权参考中的 AWS Support 的操作、资源和条件键。
  - 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的 创建向 AWS 服务 委派权限的角色。
  - 服务相关角色 – 服务相关角色是与 AWS 服务关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 AWS 账户 中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的 使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

使用策略管理访问

您将创建策略并将其附加到 AWS 身份或资源，以控制 AWS 中的访问。策略是 AWS 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，AWS 将评估这些策

略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南 中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM policy。然后，管理员可以向角色添加 IAM policy，并且用户可以代入角色。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 AWS Management Console、AWS CLI 或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的 创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管式策略是可以附加到AWS 账户中的多个用户、组和角色的独立策略。托管式策略包括 AWS 托管式策略和客户托管式策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南 中的在托管式策略与内联策略之间进行选择。

其它策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 AWS Organizations 中的最大权限。AWS Organizations 服务可以分组和集中管理您的企业拥有的多个 AWS 账户 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体（包括每个 AWS 账户根用户）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 AWS 如何确定在涉及多种策略类型时是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

AWS Support 如何与 IAM 协同工作

在使用 IAM 管理对 AWS Support 的访问之前，您应了解哪些 IAM 功能可与 AWS Support 结合使用。要大致了解 AWS Support 和其他 AWS 服务如何与 IAM 一起使用，请参阅 IAM 用户指南中的与 IAM 一起使用的 AWS 服务。

有关如何使用 IAM 管理对 AWS Support 的访问的信息，请参阅管理对 AWS Support 的访问。

主题

- AWS Support 基于身份的策略 (p. 195)

- AWS Support IAM 角色 (p. 195)

AWS Support 基于身份的策略

使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源，以及指定在什么条件下允许或拒绝操作。AWS Support 支持特定的操作。要了解您在 JSON 策略中使用的元素，请参阅 IAM 用户指南 中的 IAM JSON 策略元素参考。

操作

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行相关操作的权限。

AWS Support 中的策略操作在操作前使用以下前缀：`support:`。例如，要授予某人使用 Amazon EC2 `RunInstances` API 操作运行 Amazon EC2 实例的权限，您应将 `ec2:RunInstances` 操作纳入其策略。策略语句必须包括 `Action` 或 `NotAction` 元素。AWS Support 定义了自己的一组操作，这些操作描述了可使用该服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，包括以下操作：

```
"Action": "ec2:Describe*"
```

要查看 AWS Support 操作列表，请参阅 IAM 用户指南中的 AWS Support 定义的操作。

示例

要查看 AWS Support 基于身份的策略的示例，请参阅 AWS Support 基于身份的策略示例 (p. 196)。

AWS Support IAM 角色

IAM 角色是 AWS 账户中具有特定权限的实体。

将临时凭证用于 AWS Support

您可以使用临时凭证进行联合身份登录，担任 IAM 角色或担任跨账户角色。您可以通过调用AssumeRole或等 AWS STS API 操作来获取临时安全证书GetFederationToken。

AWS Support 支持使用临时凭证。

服务相关角色

服务相关角色允许 AWS 服务访问其它服务中的资源以代表您完成操作。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

AWS Support 支持服务相关角色。有关创建或管理 AWS Support 服务相关角色的详细信息，请参阅 将服务相关角色用于 AWS Support (p. 197)。

服务角色

此功能允许服务代表您担任服务角色。此角色允许服务访问其它服务中的资源以代表您完成操作。服务角色显示在您的 IAM 账户中，并归该账户所有。这意味着，IAM 管理员可以更改该角色的权限。但是，这样做可能会中断服务的功能。

AWS Support 支持服务角色。

AWS Support 基于身份的策略示例

预设情况下，IAM 用户和角色没有创建或修改 AWS Support 资源的权限。它们还无法使用 AWS Management Console、AWS CLI 或 AWS API 执行任务。IAM 管理员必须创建 IAM policy，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅 IAM 用户指南中的在 JSON 选项卡上创建策略。

主题

- 策略最佳实践 (p. 196)
- 使用 AWS Support 控制台 (p. 196)
- 允许用户查看他们自己的权限 (p. 197)

策略最佳实践

基于身份的策略非常强大。它们确定某个人是否可以创建、访问或删除您账户中的 AWS Support 资源。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管式策略 – 要快速开始使用 AWS Support，请使用 AWS 托管式策略，为您的员工提供他们所需的权限。这些策略已在您的账户中提供，并由 AWS 维护和更新。有关更多信息，请参阅 IAM 用户指南中的开始使用 AWS 托管式策略中的权限。
- 授予最低权限 – 创建自定义策略时，仅授予执行任务所需的许可。最开始只授予最低权限，然后根据需要授予其它权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说更为安全。有关更多信息，请参阅《IAM 用户指南》中的授予最低权限。
- 为敏感操作启用 MFA – 为增强安全性，要求 IAM 用户使用多重身份验证 (MFA) 来访问敏感资源或 API 操作。要了解更多信息，请参阅 IAM 用户指南中的在 AWS 中使用多重身份验证 (MFA)。
- 使用策略条件来增强安全性 – 在切实可行的范围内，定义基于身份的策略在哪些情况下允许访问资源。例如，您可编写条件来指定请求必须来自允许的 IP 地址范围。您也可以编写条件，以便仅允许指定日期或时间范围内的请求，或者要求使用 SSL 或 MFA。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

使用 AWS Support 控制台

要访问 AWS Support 控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的 AWS 账户中的 AWS Support 资源的详细信息。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体（IAM 用户或角色）正常运行控制台。

要确保这些实体仍可使用 AWS Support 控制台，也可向实体附加以下 AWS 托管策略。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

对于只需要调用 AWS CLI 或 AWS API 的用户，无需为其提供最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 AWS CLI 或 AWS API 所需的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

使用服务相关角色

AWS Support 和 AWS Trusted Advisor 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 AWS Support 和 Trusted Advisor 直接关联的独特 IAM 角色。在每个案例中，服务相关角色是预定义的角色。此角色包含 AWS Support 或 Trusted Advisor 代表您调用其他 AWS 服务所需的一切权限。以下主题说明了服务相关角色的功能以及如何在 AWS Support 和 Trusted Advisor 中使用这些角色。

主题

- 将服务相关角色用于 AWS Support (p. 197)
- 将服务相关角色用于 Trusted Advisor (p. 199)

将服务相关角色用于 AWS Support

AWS Support 工具通过 API 调用来收集有关 AWS 资源的信息，以提供客户服务和技术支持。为了提高支持活动的透明度和可审核性，AWS Support 现在使用 AWS Identity and Access Management (IAM) 服务相关角色。

`AWSServiceRoleForSupport` 服务相关角色是直接链接到 AWS Support 的独特 IAM 角色。此服务相关角色是预定义的，并包含 AWS Support 代表您调用其他 AWS 服务所需的权限。

AWSServiceRoleForSupport 服务相关角色信任 support.amazonaws.com 服务来代入角色。

为提供这些服务，该角色的预定义权限会向 AWS Support 授予对资源元数据而不是客户数据的访问权限。只有 AWS Support 工具可以代入此角色，此角色存在于您的 AWS 账户中。

我们会编辑可能包含客户数据的字段。例如，对于 AWS Step Functions API 调GetExecutionHistory用的Input和Output字段是不可见的AWS Support。我们使用 AWS KMS keys 加密敏感字段。这些字段在 API 响应中进行了编辑，对 AWS Support 座席不可见。

> Note
>
> AWS Trusted Advisor 使用单独的 IAM 服务相关角色来访问您账户的 AWS 资源，以提供最佳实践建议和检查。有关更多信息，请参阅将服务相关角色用于 Trusted Advisor (p. 199)：

AWSServiceRoleForSupport 服务相关角色通过 AWS CloudTrail 使所有 AWS Support API 调用均对客户可见。这样便于监控和审核要求，因为您可以透明地了解 AWS Support 代表您执行的操作。有关 CloudTrail 的信息，请参阅 AWS CloudTrail 用户指南。

AWS Support 的服务相关角色权限

此角色使用 AWSSupportServiceRolePolicy AWS 托管式策略。此托管策略已附加到角色，并授予角色代表您完成操作的权限。

这些操作可能包括以下内容：

- 账单、管理、支持和其他客户服务 – AWS 客户服务使用托管策略授予的权限来执行很多服务以作为支持计划的一部分。其中包括调查和解答账户和账单问题、为账户提供管理支持、增加服务配额和提供额外的客户支持。
- 您的 AWS 账户的服务属性和使用数据的处理 – AWS Support 可能会使用托管策略授予的权限来访问您的 AWS 账户的服务属性和使用数据。此策略允许 AWS Support 为您的账户提供账单、管理和技术支持。服务属性包括账户的资源标识符、元数据标签、角色和权限。使用率数据包括使用策略、使用情况统计数据和分析。
- 维护账户及其资源的运行状况 – AWS Support 使用自动化工具执行与操作和技术支持相关的操作。

有关允许的服务和操作的更多信息，请参阅 IAM 控制台中的 AWSSupportServiceRolePolicy 策略。

> Note
>
> AWS Support 每月自动更新一次 AWSSupportServiceRolePolicy 策略，以添加新 AWS 服务和操作的权限。

有关更多信息，请参阅AWS适用于 AWS Support 的托管策略 (p. 201)：

为 AWS Support 创建服务相关角色

您无需手动创建 AWSServiceRoleForSupport 角色。当您创建 AWS 账户时，将自动为您创建和配置此角色。

> Important
>
> 如果您在 AWS Support 开始支持服务相关角色之前使用该服务，则 AWS 会在您的账户中创建 AWSServiceRoleForSupport 角色。有关更多信息，请参阅我的 IAM 账户中出现新角色。

为 AWS Support 编辑和删除服务相关角色

您可以使用 IAM 编辑 AWSServiceRoleForSupport 服务相关角色的描述。有关更多信息，请参阅 IAM 用户指南中的编辑服务相关角色。

AWSServiceRoleForSupport 角色对于 AWS Support 为您的账户提供管理、运营和技术支持是必需的。因此，无法通过 IAM 控制台、API 或 AWS Command Line Interface (AWS CLI) 删除此角色。这将保护您的 AWS 账户，因为您不会无意中删除管理支持服务所需的权限。

有关 AWSServiceRoleForSupport 角色或其使用的更多信息，请联系 AWS Support。

将服务相关角色用于 Trusted Advisor

AWS Trusted Advisor 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 AWS Trusted Advisor 直接关联的独特 IAM 角色。服务相关角色由 Trusted Advisor 预定义，并具有该服务代表您调用其他 AWS 服务所需的一切权限。Trusted Advisor 使用此角色检查您在 AWS 上的使用情况并提供用于改善 AWS 环境的建议。例如，Trusted Advisor 通过分析您的 Amazon Elastic Compute Cloud (Amazon EC2) 实例使用来帮助您降低成本、提高性能、增强容错能力，并提高安全性。

> Note
>
> AWS Support 使用单独的 IAM 服务相关角色来访问账户的资源，以提供账单、管理和支持服务。有关更多信息，请参阅将服务相关角色用于 AWS Support (p. 197)：

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的 AWS 服务。查找在 Service-linked role（服务相关角色）列的值为 Yes（是）的服务。选择 Yes（是）与查看该服务的服务相关角色文档的链接。

主题

- Trusted Advisor 的服务相关角色权限 (p. 199)
- 管理服务相关角色的权限 (p. 199)
- 为 Trusted Advisor 创建服务相关角色 (p. 200)
- 为 Trusted Advisor 编辑服务相关角色 (p. 201)
- 删除 Trusted Advisor 的服务相关角色 (p. 201)

Trusted Advisor 的服务相关角色权限

Trusted Advisor 使用两个服务相关角色：

- AWSServiceRoleForTrustedAdvisor— 此角色信任该Trusted Advisor服务代入代表您访问AWS服务的角色。角色权限策略允许 Trusted Advisor 对所有的 AWS 资源的只读访问权限。此角色可简化开始使用 AWS 账户的过程，因为您不必为 Trusted Advisor 添加必要的权限。在开设一个 AWS 账户时，Trusted Advisor 会为您创建此角色。定义的权限包括信任策略和权限策略。不能将该权限策略附加到任何其他 IAM 实体。

  有关附加策略的更多信息，请参阅 AWSTrustedAdvisorServiceRolePolicy (p. 216)。
- AWSServiceRoleForTrustedAdvisorReporting – 此角色信任 Trusted Advisor 服务来担任组织视图功能的角色。此角色启用 Trusted Advisor 作为您的 AWS Organizations 组织的可信服务。Trusted Advisor 将在您启用组织视图时为您创建此角色。

  有关附加策略的更多信息，请参阅 AWSTrustedAdvisorReportingServiceRolePolicy (p. 218)。

  您可以使用组织视图为组织中的所有账户的 Trusted Advisor 检查结果创建报告。有关此功能的更多信息，请参阅AWS Trusted Advisor 的组织视图 (p. 29)。

管理服务相关角色的权限

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。以下示例使用 AWSServiceRoleForTrustedAdvisor 服务相关角色。

Example ：允许 IAM 实体创建 **AWSServiceRoleForTrustedAdvisor** 服务相关角色

仅当 Trusted Advisor 账户被禁用、服务相关角色被删除并且用户必须重新创建角色来重新启用 Trusted Advisor 时，才需执行此步骤。

将以下语句添加到 IAM 实体的权限策略可创建服务相关角色。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example ：允许 IAM 实体编辑 **AWSServiceRoleForTrustedAdvisor** 服务相关角色的描述

您只能编辑 AWSServiceRoleForTrustedAdvisor 角色的描述。您可以将以下语句添加到 IAM 实体的权限策略来编辑服务相关角色的描述。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example ：允许 IAM 实体删除 **AWSServiceRoleForTrustedAdvisor** 服务相关角色

您可以将以下语句添加到 IAM 实体的权限策略来删除服务相关角色。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

您也可以使用AWS托管策略（例如 AdministratorAccess）来提供对的完全访问权限Trusted Advisor。

为 Trusted Advisor 创建服务相关角色

无需手动创建 AWSServiceRoleForTrustedAdvisor 服务相关角色。开设 AWS 账户时，Trusted Advisor 将为您创建服务相关角色。

> **Important**
>
> 如果您在 Trusted Advisor 服务开始支持服务相关角色之前使用该服务，则 Trusted Advisor 会在您的账户中创建 AWSServiceRoleForTrustedAdvisor 角色。要了解更多信息，请参阅 IAM 用户指南中的我的 IAM 账户中出现新角色。

如果您的账户没有 AWSServiceRoleForTrustedAdvisor 服务相关角色，Trusted Advisor 将无法按预期工作。如果您的账户中有人将 Trusted Advisor 禁用然后又删除服务相关角色，可能会出现上述情况。在这种情况下，您可以使用 IAM 创建 AWSServiceRoleForTrustedAdvisor 服务相关角色，然后重新启用 Trusted Advisor。

启用 Trusted Advisor（控制台）

1. 使用 IAM 控制台、AWS CLI 或 IAM API 为 Trusted Advisor 创建服务相关角色。有关更多信息，请参阅创建服务相关角色。
2. 登录到 AWS Management Console，然后导航到位于 https://console.aws.amazon.com/trustedadvisor 的 Trusted Advisor 控制台。

   禁用的 Trusted Advisor 状态横幅显示在控制台中。
3. 从状态横幅中选择 Enable Trusted Advisor Role（启用 Trusted Advisor 角色）。如果未检测到所需的 `AWSServiceRoleForTrustedAdvisor`，则已禁用状态横幅仍将显示。

为 Trusted Advisor 编辑服务相关角色

由于多个实体可能引用该角色，因此无法更改服务相关角色的名称。不过，您可以使用 IAM 控制台、AWS CLI 或 IAM API 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 Trusted Advisor 的服务相关角色

如果您不需要使用 Trusted Advisor 的功能或服务，您可以删除 `AWSServiceRoleForTrustedAdvisor` 角色。您必须禁用 Trusted Advisor，然后才能删除此服务相关角色。这样可以防止您删除 Trusted Advisor 操作所需的权限。当您禁用 Trusted Advisor 时，将禁用所有服务功能，包括脱机处理和通知。此外，如果为成员账户禁用 Trusted Advisor，则单独的付款人账户也会受到影响，这意味着您将不会收到确定成本节省方法的 Trusted Advisor 检查。您无法访问 Trusted Advisor 控制台。对 Trusted Advisor 的 API 调用将返回访问被拒绝错误。

您必须在 `AWSServiceRoleForTrustedAdvisor` 账户中重新创建服务相关角色，然后才能重新启用 Trusted Advisor。

在删除 `AWSServiceRoleForTrustedAdvisor` 服务相关角色之前，您必须先在控制台中禁用 Trusted Advisor。

要禁用 Trusted Advisor

1. 登录到 AWS Management Console 并导航到位于 https://console.aws.amazon.com/trustedadvisor 的 Trusted Advisor 控制台。
2. 在导航窗格中，选择 Preferences。
3. 在服务相关角色权限部分中，选择禁用 Trusted Advisor。
4. 在确认对话框中，通过选择 OK（确定）来确认您要禁用 Trusted Advisor。

禁用 Trusted Advisor 后，所有 Trusted Advisor 功能都将被禁用，Trusted Advisor 控制台将只显示已禁用状态横幅。

然后，您可以使用 IAM 控制台、AWS CLI 或 IAM API 删除名为 `AWSServiceRoleForTrustedAdvisor` 的 Trusted Advisor 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。

AWS适用于 AWS Support 的托管策略

要向用户、组和角色添加权限，与自己编写策略相比，使用 AWS 托管策略更简单。创建仅为团队提供所需权限的 IAM 客户托管策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管式策略。这些策略涵盖常见使用案例，可在您的 AWS 账户 中使用。有关 AWS 托管式策略的更多信息，请参阅 IAM 用户指南中的AWS 托管式策略。

AWS 服务 负责维护和更新 AWS 托管式策略。您无法更改 AWS 托管式策略中的权限。服务偶尔会向 AWS 托管式策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启

动新功能或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管式策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，AWS 还支持跨多种服务的工作职能的托管式策略。例如，`ViewOnlyAccess` AWS 托管式策略提供对许多 AWS 服务 服务和资源的只读访问权限。当服务启动新功能时，AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 AWS 托管策略。

主题

- AWS适用于 AWS Support 的托管策略 (p. 202)
- 用于 Slack 中 AWS Support App 的 AWS 托管策略 (p. 211)
- AWS适用于 AWS Trusted Advisor 的托管策略 (p. 213)
- 适用于 AWS Support Plans 的 AWS 托管策略 (p. 220)

AWS适用于 AWS Support 的托管策略

AWS Support 具有以下托管式策略。

目录

- AWS 托管策略：AWSSupportServiceRolePolicy (p. 202)
- 对 AWS 托管式策略的 AWS Support 更新 (p. 202)
- AWSSupportServiceRolePolicy 的权限更改 (p. 210)

AWS 托管策略：AWSSupportServiceRolePolicy

AWS Support 使用 AWSSupportServiceRolePolicy AWS 托管策略。此托管策略附加到 `AWSServiceRoleForSupport` 服务相关角色。该策略允许服务相关角色代表您完成操作。您不能将此策略附加到您的 IAM 实体。有关更多信息，请参阅AWS Support 的服务相关角色权限 (p. 198)：

有关对策略的更改列表，请参阅 对 AWS 托管式策略的 AWS Support 更新 (p. 202) 和 AWSSupportServiceRolePolicy 的权限更改 (p. 210)。

对 AWS 托管式策略的 AWS Support 更新

查看有关 AWS Support 和 Trusted Advisor 的 AWS 托管式策略更新的详细信息（从这些服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅 文档历史记录 (p. 345) 页面上的 RSS 源。

下表介绍了自 2022 年 2 月 17 日以来对 AWS Support 托管式策略的重要更新。

AWS Support

更改	说明	日期
AWSSupportServiceRolePolicy (p. 202) – 对现有策略的更新	为以下服务添加了 141 个新权限，用于执行有助于解决与账单、管理和技术支持相关的客户问题的操作： • Lambda — 用于解决与 Lambda 服务相关的问题。 • 亚马逊 Lex — 解决与亚马逊 Lex 服务有关的问题。	2023 年 6 月 26 日

更改	说明	日期
	• AWS传输-调试与传输服务相关的问题。 • AWS Amplify— 调试与 Amplify 服务相关的问题。 • 亚马逊 EventBridge Pipes — 用于解决与 Pipes 相关的权限和账单问题。 • 亚马逊 EventBridge-调试与亚马逊有关的问题 EventBridge • 亚马逊CloudWatch日志-解决与亚马逊CloudWatch日志有关的问题。 • AWS Systems Manager— 解决与系统管理器有关的问题。 • 亚马逊 CloudWatch —调试与相关的问题CloudWatch. • 亚马逊 ElastiCache-解决与亚马逊有关的问题ElastiCache。 • 亚马逊雅典娜—调试与雅典娜有关的问题。 • AWS Elastic Disaster Recovery — 解决与 Elastic 灾难恢复相关的问题。 • 亚马逊 CloudWatch-对亚马逊的配置进行故障排除CloudWatch。 • 亚马逊 EC2 — 用于调试与 EC2 服务相关的问题。 • AWS Certificate Manager— 解决与证书管理器有关的问题。 • 亚马逊EventBridge调度程序-解决与EventBridge调度程序有关的问题。 • 亚马逊OpenSearch服务—解决与以下相关的问题OpenSearch. • 亚马逊EventBridge架构-调试与EventBridge架构相关的问题。 • AWS用户通知-解决与用户通知有关的问题。 • 亚马逊CloudWatch应用程序见解-解决与CloudWatch应用程序见解有关的问题。 • 亚马逊 DynamoDB — 解决与 DynamoDB 相关的问题。 • 亚马逊 DocumentDB 弹性集群 — 解决与 DocumentDB 弹性集群相关的问题	

更改	说明	日期
AWSSupportServiceRolePolicy (p. 232) – 对现有策略的更新	为以下服务添加了 53 个新权限，用于执行有助于解决与账单、管理和技术支持相关的客户问题的操作： • 自动扩展-解决与自动扩展服务相关的问题。 • 亚马逊 CloudWatch-解决与亚马逊有关的问题CloudWatch。 • AWS Compute Optimizer— 解决与计算优化器有关的问题。 • 亚马逊 CloudWatch Evidently — 解决与 Evidenly 有关的问题。 • EC2 映像生成器-解决与映像生成器服务相关的问题。 • AWS IoT TwinMaker— 解决与相关的问题AWS IoT TwinMaker。 • 亚马逊CloudWatch日志-解决与亚马逊CloudWatch日志有关的问题。 • Amazon Pinpoint：解决与 Amazon Pinpoint 相关的问题。 • AWSOAM 链接-调试与 OAM 资源相关的问题。 • AWS Outposts— 解决与相关的问题AWS Outposts。 • 亚马逊 RDS — 用于调试与亚马逊 RDS 相关的问题。 • AWS 资源探索器— 解决与资源浏览器有关的问题。 • 亚马逊 CloudWatch RUM — 对 RUM 服务资源的配置进行故障排除。 • 亚马逊 SNS — 解决与亚马逊 SNS 相关的问题。 • 亚马逊 S CloudWatch ynthetics — 解决与 S CloudWatch ynthetics 有关的问题。	2023年5月2日

更改	说明	日期
AWSSupportServiceRolePolicy (p. 232) – 对现有策略的更新	为以下服务添加了 52 个新权限，用于执行有助于解决与账单、管理和技术支持相关的客户问题的操作： • AWS Backup gateway— 解决与备份网关有关的问题。 • 亚马逊 S3 — 调试与亚马逊 S3 有关的问题。 • AWS Application Migration Service— 解决与应用程序迁移服务有关的问题。 • AWS无尘室—调试与AWS洁净室有关的问题； • AWS Systems Managerfor SAP — 解决与 AWS Systems Manager SAP 相关的问题。 • 亚马逊 VPC Lattice — 调试与亚马逊 VPC Lattice 相关的问题。	2023 年 3 月 16 日

更改	说明	日期
AWSSupportServiceRolePolicy (p. 212) – 对现有策略的更新	为以下服务增加了 220 项新权限，以执行有助于解决与账单、管理和技术支持相关的客户问题的操作： • Amazon Athena：允许 AWS Support 开发可用于帮助客户解决与 Athena 相关的查询的工具。 • Amazon Chime：解决与 Amazon Chime 相关的问题。 • 亚马逊CloudWatch互联网监视器-调试与互联网监视器有关的问题。 • Amazon Comprehend：解决与 Amazon Comprehend 相关的问题。 • Amazon Elastic Compute Cloud：用于调试与 Transit Gateway Connect 和组播功能相关的问题。 • 亚马逊EventBridge管道-用于解决与EventBridge管道有关的问题。 • Amazon Interactive Video Service：允许 AWS Support 查询 Amazon IVS 资源以解决客户问题。 • Amazon FSx：允许 AWS Support 开发支持导入和导出 Amazon FSx 数据存储库的工具。 • 亚马逊 GameLift-解决与亚马逊有关的问题GameLift。 • AWS Glue：解决与 AWS Glue 数据质量相关的问题。 • Amazon Kinesis Video Streams：解决与 Kinesis Video Streams 相关的问题。 • Amazon Managed Service for Prometheus：解决与 Amazon Managed Service for Prometheus 相关的问题。 • Amazon Managed Streaming for Apache Kafka：解决与 Amazon MSK Connect 相关的问题。 • AWS Network Manager：解决与 Network Manager 相关的问题。	2023 年 1 月 10 日

更改	说明	日期
	• Amazon Nimble Studio：调试与 Nimble Studio 相关的问题。 • Amazon Personalize：调试与 Amazon Personalize 相关的问题。 • Amazon Pinpoint：解决与 Amazon Pinpoint 相关的问题。 • Amazon Omics：解决与 Omics 相关的问题。 • Amazon Transcribe：调试与 Amazon Transcribe 相关的问题。	
AWSSupportServiceRolePolicy (p. 212) – 对现有策略的更新	为以下服务增加了 47 项新权限，以执行有助于解决与账单、管理和技术支持相关的客户问题的操作： • AWS Application Migration Service - 解决复制和启动问题。 • AWS CloudFormation 挂钩 - 启用 AWS Support 以开发可以有助于解决问题的自动化工具。 • Amazon Elastic Kubernetes Service - 解决与 Amazon EKS 相关的问题。 • AWS IoT FleetWise - 解决与 AWS IoT FleetWise 相关的问题。 • AWS Mainframe Modernization - 调试与大型机现代化相关的问题。 • AWS Outposts - 帮助 AWS Support 获取专属主机和资产的列表。 • AWS Private 5G - 解决与 Private 5G 相关的问题。 • AWS Tiros - 调试与 Tiros 相关的问题。	2022 年 10 月 4 日

更改	说明	日期
AWSSupportServiceRolePolicy (p. 212) – 对现有策略的更新	为以下服务增加了 46 项新权限，以执行有助于解决与账单、管理和技术支持相关的客户问题的操作： • Amazon Managed Streaming for Apache Kafka - 解决与 Amazon MSK 相关的问题。 • AWS DataSync— 解决与相关的问题DataSync。 • AWS Elastic Disaster Recovery - 解决复制和启动问题。 • 亚马逊 GameSparks —解决与以下相关的问题GameSparks. • AWS IoT TwinMaker - 调试与 AWS IoT TwinMaker 相关的问题。 • AWS Lambda - 查看函数 URL 的配置以解决问题。 • Amazon Lookout for Equipment - 解决与 Lookout for Equipment 相关的问题。 • Amazon Route 53 和 Amazon Route 53 Resolver - 获取解析器配置，以便 AWS Support 可以检查 VPC 的 DNS 解析行为。	2022 年 8 月 17 日
AWSSupportServiceRolePolicy (p. 212) – 对现有策略的更新	为以下服务增加了新权限，以执行有助于解决与账单、管理和技术支持相关的客户问题的操作： • 亚马逊CloudWatch日志-帮助解决与CloudWatch日志相关的问题。 • Amazon Interactive Video Service – 帮助 AWS Support 检查现有的 Amazon IVS 资源，了解有关欺诈或账户遭盗用的支持案例。 • Amazon Inspector – 对 Amazon Inspector 相关问题进行问题排查。 删除了亚马逊等服务的权限 WorkLink。亚马逊WorkLink于 2022 年 4 月 19 日被弃用。	2022 年 6 月 23 日

更改	说明	日期
AWSSupportServiceRolePolicy (p. 212) – 对现有策略的更新	为以下服务增加了 25 项新权限，以执行有助于解决与账单、管理和技术支持相关的客户问题的操作： • AWS Amplify UI Builder – 排查与组件和主题生成相关的问题。 • 亚马逊 AppStream-通过检索最近推出的功能的资源来解决问题。 • AWS Backup – 排查与备份作业相关的问题。 • AWS CloudFormation – 诊断与 IAM、扩展和版本控制相关的问题。 • Amazon Kinesis – 排查与 Kinesis 相关的问题。 • AWS Transfer Family – 排查与 Transfer Family 相关的问题。	2022 年 4 月 27 日

AWSSupportServiceRolePolicy (p. 212) – 对现有策略的更新	为以下服务添加了 54 项新权限，以执行有助于解决与账单、管理和技术支持相关的客户问题的操作：
	• Amazon Elastic Compute Cloud
	  • 解决与客户和 AWS 管理的前缀列表相关的问题。
	  • 解决与 Amazon VPC IP 地址管理器 (IPAM) 相关的问题。
	• AWS 网络管理器 – 解决与网络管理器相关的问题。
	• Savings Plans – 获取有关未完成 Savings Plan 承诺的元数据。
	• AWS Serverless Application Repository – 作为研究和解决支持案例的一部分，改进和支持响应操作。
	• 亚马逊 WorkSpaces Web — 用于调试和解决 WorkSpaces Web 服务问题。
		2022 年 3 月 14 日

更改	说明	日期
AWSSupportServiceRolePolicy (p. 212) – 对现有策略的更新	为以下服务添加了 74 项新权限，以执行有助于解决与账单、管理和技术支持相关的客户问题的操作： • AWS Application Migration Service - 在应用程序迁移服务中支持无代理复制。 • AWS CloudFormation - 对 IAM、扩展和版本控制相关问题执行诊断。 • 亚马逊CloudWatch日志-用于验证资源策略。 • Amazon EC2 回收站 - 获取有关回收站保留规则的元数据。 • AWS Elastic Disaster Recovery - 解决客户账户中的复制问题和启动问题。 • Amazon FSx - 查看 Amazon FSx 快照的描述。 • Amazon Lightsail - 查看 Lightsail 存储桶的元数据和配置详细信息。 • Amazon Macie - 查看 Macie 配置，例如分类任务、自定义数据标识符、正则表达式和结果。 • Simple Storage Service (Amazon S3) - 收集 Simple Storage Service (Amazon S3) 存储桶的元数据和配置。 • AWS Storage Gateway - 查看有关客户自动创建磁带策略的元数据。 • Elastic Load Balancing - 查看使用 Service Quotas 控制台时的资源限制的说明。 有关更多信息，请参阅AWSSupportServiceRolePolicy 的权限更改 (p. 210)：	2022 年 2 月 17 日
已发布的更改日志	AWS Support 托管策略的更改日志。	2022 年 2 月 17 日

AWSSupportServiceRolePolicy 的权限更改

添加到 `AWSSupportServiceRolePolicy` 的大多数权限允许 AWS Support 使用相同名称调用 API 操作。但是，某些 API 操作需要具有不同名称的权限。

下表仅列出了需要具有不同名称的权限的 API 操作。下表介绍了这些从 2022 年 2 月 17 日开始的差异。

日期	API 操作名称	所需的策略权限
2022 年 2 月 17 日添加了权限	s3.GetBucketAnalyticsConfiguration s3.ListBucketAnalyticsConfiguration	s3:GetAnalyticsConfiguration
	s3.GetBucketNotificationConfiguration	s3:GetBucketNotification
	s3.GetBucketEncryption	s3:GetEncryptionConfiguration
	s3.GetBucketIntelligentTieringConfiguration s3.ListBucketIntelligentTieringConfiguration	s3:GetIntelligentTieringConfiguratio
	s3.GetBucketInventoryConfiguration s3.ListBucketInventoryConfiguration	s3:GetInventoryConfiguration
	s3.GetBucketLifecycleConfiguration	s3:GetLifecycleConfiguration
	s3.GetBucketMetricsConfiguration s3.ListBucketMetricsConfiguration	s3:GetMetricsConfiguration
	s3.GetBucketReplication	s3:GetReplicationConfiguration
	s3.HeadBucket s3.ListObjects	s3:ListBucket
	s3.ListBuckets	s3:ListAllMyBuckets
	s3.ListMultipartUploads	s3:ListBucketMultipartUploads
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts

用于 Slack 中 AWS Support App 的 AWS 托管策略

> **Note**
>
> 要在 AWS Support Center Console 中访问和查看支持案例，请参阅 管理对 AWS Support 中心的访问 (p. 221)。

AWS Support App 具有以下托管策略。

目录

- AWS托管策略：AWSSupportAppFullAccess (p. 211)
- AWS 托管策略：AWSSupportAppReadOnlyAccess (p. 212)
- 有关 AWS 托管策略的 AWS Support App 更新 (p. 213)

AWS托管策略：AWSSupportAppFullAccess

您可以使用 AWSSupportAppFullAccess 托管策略授予 IAM 角色访问 Slack 通道配置的权限。您还能将 AWSSupportAppFullAccess 策略附加到您的 IAM 实体。

有关更多信息，请参阅Slack 中的 AWS Support App (p. 153)：

此策略授予允许实体为 AWS Support App 执行 AWS Support、服务限额和 IAM 操作的权限。

权限详细信息

此策略包含以下权限：

- servicequotas - 描述您现有的服务限额和请求，并增加账户的服务限额。
- support - 创建、更新和解决您的支持案例。更新和描述有关案例的信息，例如文件附件、通信信息和严重性级别。启动与支持座席的实时聊天会话。
- iam - 创建用于服务限额的服务相关角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicequotas:GetRequestedServiceQuotaChange",
                "servicequotas:GetServiceQuota",
                "servicequotas:RequestServiceQuotaIncrease",
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeSeverityLevels",
                "support:InitiateChatForCase",
                "support:ResolveCase"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "servicequotas.amazonaws.com"}
            }
        }
    ]
}
```

有关更多信息，请参阅管理对 AWS Support App 的访问 (p. 155)：

AWS 托管策略：AWSSupportAppReadOnlyAccess

AWSSupportAppReadOnlyAccess 策略授予允许实体执行只读 AWS Support App 操作的权限。有关更多信息，请参阅Slack 中的 AWS Support App (p. 153)：

权限详细信息

此策略包含以下权限：

- support - 描述支持案例的详细信息以及添加到支持案例中的通信。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeCases",
                "support:DescribeCommunications"
            ],
            "Resource": "*"
        }
    ]
}
```

有关 AWS 托管策略的 AWS Support App 更新

查看有关 AWS Support App 的 AWS 托管策略更新详细信息（从该服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅 文档历史记录 (p. 345) 页面上的 RSS 源。

下表介绍了自 2022 年 8 月 17 日以来对 AWS Support App 托管策略的重要更新。

AWS Support 应用

更改	说明	日期
AWSSupportAppFullAccess (p. 211) 和 AWSSupportAppReadOnlyAccess (p. 211) 适用于 AWS Support App 的新 AWS 托管策略	您可以将这些策略用于您为 Slack 通道配置的 IAM 角色。 有关更多信息，请参阅管理对 AWS Support App 的访问 (p. 155)：	2022 年 8 月 19 日
已发布的更改日志	AWS Support App 托管策略的更改日志。	2022 年 8 月 19 日

AWS适用于 AWS Trusted Advisor 的托管策略

Trusted Advisor 具有以下 AWS 托管策略。

目录

- AWS托管策略：AWSTrustedAdvisorPriorityFullAccess (p. 213)
- AWS托管策略：AWSTrustedAdvisorPriorityReadOnlyAccess (p. 215)
- AWS 托管策略：AWSTrustedAdvisorServiceRolePolicy (p. 216)
- AWS 托管策略：AWSTrustedAdvisorReportingServiceRolePolicy (p. 218)
- 对 AWS 托管式策略的 Trusted Advisor 更新 (p. 219)

AWS托管策略：AWSTrustedAdvisorPriorityFullAccess

AWSTrustedAdvisorPriorityFullAccess 策略授予对 Trusted Advisor Priority 的完全访问权限。此策略还允许用户将 Trusted Advisor 添加为具有 AWS Organizations 受信任服务，并为 Trusted Advisor Priority 指定委派管理员帐户。

权限详细信息

在第一条语句中，此策略包含 trustedadvisor 的以下权限：

- 描述您的账户和组织。
- 描述 Trusted Advisor Priority 的已识别风险。这些权限允许您下载和更新风险状态。
- 描述 Trusted Advisor Priority 电子邮件通知的配置。这些权限允许您配置电子邮件通知，并为委派管理员禁用这些通知。
- 设置 Trusted Advisor 以便您的账户可以启用 AWS Organizations。

在第二条语句中，此策略包含 organizations 的以下权限：

- 描述您的 Trusted Advisor 账户和组织。
- 列出您为了使用 Organizations 以启用的 AWS 服务。

在第三条语句中，此策略包含 organizations 的以下权限：

- 列出 Trusted Advisor Priority 的委派管理员。
- 启用和禁用 Organizations 的受信任访问。

在第四条语句中，此策略包含 iam 的以下权限：

- 创建 AWSServiceRoleForTrustedAdvisorReporting 服务相关角色。

在第五条语句中，此策略包含 organizations 的以下权限：

- 允许您注册和注销 Trusted Advisor Priority 的委派管理员。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeRisk*",
                "trustedadvisor:DownloadRisk",
                "trustedadvisor:UpdateRiskStatus",
                "trustedadvisor:DescribeNotificationConfigurations",
                "trustedadvisor:UpdateNotificationConfigurations",
                "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
                "trustedadvisor:SetOrganizationAccess"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:RegisterDelegatedAdministrator",
                "organizations:DeregisterDelegatedAdministrator"
            ],
            "Resource": "arn:aws:organizations::*:*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

AWS托管策略：AWSTrustedAdvisorPriorityReadOnlyAccess

AWSTrustedAdvisorPriorityReadOnlyAccess 策略授予 Trusted Advisor Priority 包括查看委派管理员帐户在内的权限。

权限详细信息

在第一条语句中，此策略包含 `trustedadvisor` 的以下权限：

- 描述您的 Trusted Advisor 账户和组织。
- 描述 Trusted Advisor Priority 的已识别风险并允许您下载这些风险。
- 描述 Trusted Advisor Priority 电子邮件通知的配置。

在第二条和第三条语句中，此策略包含 `organizations` 的以下权限：

- 使用 Organizations 描述您的组织。
- 列出您为了使用 Organizations 以启用的 AWS 服务。
- 列出 Trusted Advisor Priority 的委派管理员

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeRisk*",
                "trustedadvisor:DownloadRisk",
                "trustedadvisor:DescribeNotificationConfigurations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

AWS 托管策略：AWSTrustedAdvisorServiceRolePolicy

此策略附加到 AWSServiceRoleForTrustedAdvisor 服务相关角色。此角色允许服务相关角色为您执行操作。您不能将 AWSTrustedAdvisorServiceRolePolicy 附加到您的 AWS Identity and Access Management（IAM）实体。有关更多信息，请参阅将服务相关角色用于 Trusted Advisor (p. 199)：

此策略授予管理权限，允许服务相关角色访问 AWS 服务。这些权限允许 Trusted Advisor 的检查来评估您的账户。

权限详细信息

此策略包含以下权限。

- Auto Scaling – 描述 Amazon EC2 Auto Scaling 账户配额和资源
- cloudformation— 描述 AWS CloudFormation (CloudFormation) 账户配额和堆栈
- cloudfront— 描述亚马逊CloudFront发行版

- cloudtrail— 描述 AWS CloudTrail (CloudTrail) 路线
- dynamodb – 描述 Amazon DynamoDB 账户配额和资源
- ec2 – 描述 Amazon Elastic Compute Cloud (Amazon EC2) 账户配额和资源
- elasticloadbalancing - 描述弹性负载均衡（ELB）账户配额和资源
- iam – 获取 IAM 资源，如证书、密码策略和证书
- kinesis – 描述 Amazon Kinesis (Kinesis) 账户配额
- rds – 描述 Amazon Relational Database Service (Amazon RDS) 资源
- redshift – 描述 Amazon Redshift 资源
- route53 – 描述 Amazon Route 53 账户配额和资源
- s3 – 描述 Amazon Simple Storage Service (Amazon S3) 资源
- ses – 获取 Amazon Simple Email Service (Amazon SES) 发送配额
- sqs – 列出 Amazon Simple Queue Service (Amazon SQS) 队列
- cloudwatch— 获取亚马逊CloudWatch活动（CloudWatch事件）指标统计数据
- ce – 获取 Cost Explorer 服务 (Cost Explorer) 建议

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
```

```
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "kinesis:DescribeLimits",
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:ListQueues",
                "cloudwatch:GetMetricStatistics",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略：AWSTrustedAdvisorReportingServiceRolePolicy

此策略附加到 AWSServiceRoleForTrustedAdvisorReporting 服务相关角色，使 Trusted Advisor 能够执行组织视图功能的操作。您不能将 AWSTrustedAdvisorReportingServiceRolePolicy 附加到您的 IAM 实体。有关更多信息，请参阅将服务相关角色用于 Trusted Advisor (p. 199)：

此策略授予管理权限，允许服务相关角色执行 AWS Organizations 操作。

权限详细信息

此策略包含以下权限。

- organizations – 描述您的组织并列出服务访问权限、账户、父级、子级和组织单位

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

对 AWS 托管式策略的 Trusted Advisor 更新

查看有关 AWS Support 和 Trusted Advisor 的 AWS 托管策略更新的详细信息（从这些服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅 文档历史记录 (p. 345) 页面上的 RSS 源。

下表介绍了自 2021 年 8 月 10 日以来对 Trusted Advisor 托管式策略的重要更新。

Trusted Advisor

更改	说明	日期
AWSTrustedAdvisorReportingServiceRolePolicy (p. 218) 附加到Trusted AdvisorAWSServiceRoleForTrustedAdvisorReporting服务相关角色的托管策略的第 2 版	将Trusted AdvisorAWSServiceRoleForTrustedAdvisorReporting服务相关角色的AWS托管策略升级到 v2。v2 将再添加一个 IAM 操作 organizations:ListDelegatedAdministrators	2023年2月28日
AWSTrustedAdvisorPriorityFullAccess (p. 214) 和 AWSTrustedAdvisorPriorityReadOnlyAccess (p. 215) 用于 Trusted Advisor 的新 AWS 托管策略	Trusted Advisor 添加了两个新的托管策略，您可以使用这些策略来控制对 Trusted Advisor Priority 的访问权限。	2022 年 8 月 17 日
AWSTrusted AdvisorServiceRolePolicy (p. 213) – 对现有策略的更新	Trusted Advisor 添加了新的操作来授予 DescribeTargetGroups 和	2021 年 8 月 10 日

更改	说明	日期
	`GetAccountPublicAccessBlock` 权限。 Auto Scaling 组运行状况检查需要 `DescribeTargetGroup` 权限，以检索附加到 Auto Scaling 组的非经典负载均衡器。 Amazon S3 存储桶权限检查需要 `GetAccountPublicAccessBlock` 权限以检索 AWS 账户 的阻止公有访问设置。	
已发布的更改日志	Trusted Advisor 托管策略的更改日志。	2021 年 8 月 10 日

适用于 AWS Support Plans 的 AWS 托管策略

AWS Support Plans 具有以下托管策略。

目录

- AWS托管策略：AWSSupportPlansFullAccess (p. 220)
- AWS托管策略：AWSSupportPlansReadOnlyAccess (p. 221)
- 对 AWS 托管策略的 AWS Support 计划更新 (p. 221)

AWS托管策略：AWSSupportPlansFullAccess

AWS Support Plans 使用 AWSSupportPlansFullAccess AWS 托管策略。IAM 实体使用此策略为您完成以下 Support Plans 操作：

- 查看 AWS 账户 的支持计划
- 查看有关更改支持计划请求状态的详细信息
- 更改 AWS 账户 的支持计划
- 为您创建支持计划时间表 AWS 账户

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule"
            ],
            "Resource": "*"
        }
    ]
}
```

有关策略更改的列表，请参阅 对 AWS 托管策略的 AWS Support 计划更新 (p. 221)。

AWS托管策略：AWSSupportPlansReadOnlyAccess

AWS Support Plans 使用 AWSSupportPlansReadOnlyAccess AWS 托管策略。IAM 实体使用此策略为您完成以下只读 Support Plans 操作：

- 查看 AWS 账户 的支持计划
- 查看有关更改支持计划请求状态的详细信息

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

有关策略更改的列表，请参阅 对 AWS 托管策略的 AWS Support 计划更新 (p. 221)。

对 AWS 托管策略的 AWS Support 计划更新

查看有关 Support Plans AWS 托管策略更新的详细信息（从这些服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅 文档历史记录 (p. 345) 页面上的 RSS 源。

下表介绍了自 2022 年 9 月 29 日以来对 Support Plans 托管策略的重要更新。

AWS Support

更改	说明	日期
AWSSupportPlansFullAccess (p. 220) – 对现有策略的更新	向AWSSupportPlansFullAccess托管策略添加CreateSupportPlanSchedule操作。	2023 年 5 月 8 日
已发布的更改日志	Support Plans 托管策略的更改日志。	2022 年 9 月 29 日

管理对 AWS Support 中心的访问

您必须具有访问支持中心和创建支持案例 (p. 1)的权限。

您可以使用以下选项之一访问支持中心：

- 使用与您的 AWS 账户关联的电子邮件地址和密码。此身份称作 AWS 账户根用户。
- 使用 AWS Identity and Access Management (IAM)。

如果您拥有商业、Enterprise On-Ramp 或企业 Support 计划，则还可以使用 AWS Support API (p. 15) 以编程方式访问 AWS Support 和 Trusted Advisor 操作。有关详细信息，请参阅 AWS Support API 参考。

Note

如果无法登录到支持中心，则可以使用 Contact Us（联系我们）页面。您可以使用此页面获取有关账单和账户问题的帮助。

拥有AWS账户

您可以使用您的 AWS 账户电子邮件地址和密码登录 AWS Management Console 并访问支持中心。此身份称作 AWS 账户根用户。但是，我们强烈建议您不要使用根用户来执行日常任务，即使是管理任务。相反，我们建议您使用 IAM，它允许您控制哪些人可以在您的账户中执行某些任务。

AWS支持行动

可以在控制台中执行以下 AWS Support 操作。还可以在 IAM policy 中指定这些 AWS Support 操作以允许或拒绝特定操作。

Note

如果您拒绝 IAM 政策中的以下任何操作，则在创建支持案例或与支持案例互动时，可能会导致支持中心出现意外行为。

操作	描述
`DescribeSupportLevel`	授予返回AWS账户标识符支持级别的权限。Cent AWS Support er 在内部使用它来确定您的支持级别。
`InitiateCallForCase`	授予在 AWS Support 中心上发起调用的权限。Cent AWS Support er 在内部使用它来代表你发起呼叫。
`InitiateChatForCase`	授予在 Cent AWS Support er 上发起聊天的权限。Cent AWS Support er 在内部使用它来代表你开始聊天。
`RateCaseCommunication`	授予对AWS Support案例沟通进行评分的权限。
`DescribeCaseAttributes`	授予允许辅助服务读取AWS Support案例属性的权限。Cent AWS Support er 在内部使用它来获取案例上的属性标签。
`DescribeIssueTypes`	授予返回AWS Support案例问题类型的权限。Cent AWS Support er 在内部使用它来获取您的账户的可用问题类型。
`SearchForCases`	授予返回与给定输入匹配的AWS Support案例列表的权限。Cent AWS Support er 在内部使用它来查找搜索到的案例。
`PutCaseAttributes`	授予允许辅助服务向 AWS Support 案例添加属性的权限。Cent AWS Support er 内部使用它来为您的AWS Support案例添加操作标签。

IAM

默认情况下，IAM 用户无法访问支持中心。您可以使用 IAM 创建各个用户或组。然后，您将 IAM policy 附加到这些实体，以便它们有权执行操作和访问资源，例如打开支持中心案例和使用 AWS Support API。

创建 IAM 用户以后，您可以为这些用户提供单独的密码和账户特定的登录页面。然后，他们可以登录到 AWS 账户并在支持中心工作。已获取 AWS Support 访问权限的 IAM 用户可以看到为该账户创建的所有案例。

有关更多信息，请参阅 IAM 用户指南中的 IAM 用户如何登录您的 AWS 账户。

授予权限的最简单方法是将 AWS 托管策略 AWSSupportAccess 附加到用户、组或角色。AWS Support 允许使用操作级权限来控制对特定 AWS Support 操作的访问。AWS Support 不提供资源级访问，因此 `Resource` 元素始终设置为 `*`。您无法允许或拒绝对特定支持案例的访问。

Example ：允许对所有 AWS Support 操作的访问

AWS托管策略向 IAM 用户AWSSupportAccess授予访问权限AWS Support。具有此策略的 IAM 用户可以访问所有 AWS Support 操作和资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["support:*"],
            "Resource": "*"
        }
    ]
}
```

有关如何将 `AWSSupportAccess` 策略附加到您的实体的更多信息，请参阅 IAM 用户指南中的添加 IAM 身份权限（控制台）。

Example：允许访问除操作之外的所有ResolveCase操作

您也可以在 IAM 中创建客户托管策略来指定允许或拒绝哪些操作。以下策略语句允许 IAM 用户在 AWS Support 中执行除解决案例之外的所有操作。

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
   },
   {
       "Effect": "Deny",
       "Action": "support:ResolveCase",
       "Resource": "*"
    }]
}
```

有关如何创建客户托管式 IAM policy 的更多信息，请参阅《IAM 用户指南》中的创建 IAM policy（控制台）。

如果用户或组已有策略，则您可向该策略添加 AWS Support 特定的策略语句。

Important

- 如果您无法在支持中心中查看案例，请确保您拥有所需的权限。您可能需要联系您的 IAM 管理员。有关更多信息，请参阅适用于 AWS Support 的 Identity and Access Management (p. 191)：

对 AWS Trusted Advisor 的访问权限

在 AWS Management Console中，单独的 `trustedadvisor` IAM 命名空间控制对 Trusted Advisor 的访问。在 AWS Support API 中，`support` IAM 命名空间控制对 Trusted Advisor 的访问。有关更多信息，请参阅管理对 AWS Trusted Advisor 的访问 (p. 226)：

管理对 AWS Support 计划的访问权限

主题

- Support Plans 控制台的权限 (p. 224)
- Support Plans 操作 (p. 224)
- Support Plans 的示例 IAM policy (p. 224)
- 问题排查 (p. 225)

Support Plans 控制台的权限

要访问 Support Plans 控制台，用户必须拥有一组最低权限。这些权限必须允许用户列出和查看有关 AWS 账户 中 Support Plans 资源的详细信息。

使用 `supportplans` 命名空间创建 AWS Identity and Access Management（IAM）policy。您可以使用此策略来指定操作和资源的权限。

创建策略时，可以指定服务的命名空间来允许或拒绝操作。Support Plans 的命名空间为 `supportplans`。

您可以使用 AWS 托管策略并将其附加到您的 IAM 实体。有关更多信息，请参阅适用于 AWS Support Plans 的 AWS 托管策略 (p. 220)：

Support Plans 操作

可以在控制台中执行以下 Support Plans 操作。还可以在 IAM policy 中指定这些 Support Plans 操作以允许或拒绝特定操作。

操作	描述
`GetSupportPlan`	授予查看有关此 AWS 账户 当前 Support Plans 详细信息的权限。
`GetSupportPlanUpdateStatus`	授予查看有关更新 Support Plans 请求状态的详细信息的权限。
`StartSupportPlanUpdate`	授予启动请求以更新此 AWS 账户 支持计划的权限。
`CreateSupportPlanSchedule`	授予为此创建支持计划时间表的权限AWS 账户。

Support Plans 的示例 IAM policy

您可以使用以下示例策略来管理对 Support Plans 的访问。

对 Support Plans 的完全访问

以下策略允许用户对 Support Plans 进行完全访问。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:*",
            "Resource": "*"
        }
    ]
}
```

对 Support Plans 的只读访问

以下策略允许用户对 Support Plans 进行只读访问。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:Get*",
            "Resource": "*"
        }
    ]
}
```

拒绝对 Support Plans 的访问

以下策略不允许用户访问 Support Plans。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "supportplans:*",
            "Resource": "*"
        }
    ]
}
```

问题排查

请参阅以下主题以管理对 Support 计划的访问。

尝试查看或更改支持计划时，Support 计划控制台显示缺少 GetSupportPlan 权限

IAM 用户必须具有访问 Support 计划控制台所需的权限。您可以更新 IAM policy 以包含缺少的权限，也可以使用 AWSSupportPlansFullAccess 或 AWSSupportPlansReadOnlyAccess 等 AWS 托管策略。有关更多信息，请参阅适用于 AWS Support Plans 的 AWS 托管策略 (p. 220)：

如果您无权更新 IAM policy，请联系 AWS 账户管理员。

相关信息

有关更多信息，请参阅 IAM 用户指南中的以下主题：

- 使用 IAM policy simulator 测试 IAM policy

- 排查访问被拒绝错误消息

具有正确的 Support 计划权限，但仍然显示相同的错误信息

如果您的 AWS 账户 是属于 AWS Organizations 的成员账户，则可能需要更新服务控制策略（SCP）。SCP 是一种管理组织权限的策略。

由于 Support 计划是一项全球服务，因此限制 AWS 区域的策略可能会阻止成员账户查看或更改其支持计划。要为您的组织允许全球服务，例如 IAM 和 Support 计划，必须将该服务添加到任何适用的 SCP 的排除列表中。这意味组织中的账户可以访问这些服务，即使 SCP 拒绝指定的 AWS 区域。

要将 Support 计划添加为例外，请在 SCP 的 "NotAction" 列表中输入 "supportplans:*"。

```
"supportplans:*",
```

您的 SCP 可能显示为以下策略代码段。

Example ：允许 Support 计划在组织中进行访问的 SCP

```
{ "Version":  "2012-10-17",
   "Statement": [
     { "Sid":  "GRREGIONDENY",
       "Effect":  "Deny",
       "NotAction": [
         "aws-portal:*",
         "budgets:*",
         "chime:*"
         "iam:*",
         "supportplans:*",
         ....
```

如果您有成员账户但无法更新 SCP，请联系 AWS 账户 管理员。管理账户可能需要更新 SCP，以便所有成员账户都可以访问 Support 计划。

AWS Control Tower 的注意事项

- 如果您的组织将 AWS Control Tower 与 SCP 结合使用，则可以更新根据请求的 AWS 区域 拒绝访问 AWS控制（通常称为区域拒绝控制）。
- 如果您将适用于 AWS Control Tower 的 SCP 更新为允许 supportplans，则修复偏差将删除您对 SCP 的更新。有关更多信息，请参阅检测并解决 AWS Control Tower 中的偏差。

相关信息

有关更多信息，请参阅以下主题：

- 《AWS Organizations 用户指南》中的服务控制策略（SCP）。
- 《AWS Control Tower 用户指南》中的配置区域拒绝控制
- 根据《AWS Control Tower 用户指南》中要求的 AWS 区域 拒绝访问 AWS

管理对 AWS Trusted Advisor 的访问

您可以从 AWS Management Console访问 AWS Trusted Advisor。所有 AWS 账户 都有权访问特色级核心 Trusted Advisor 检查。如果您拥有商业、Enterprise On-Ramp 或企业 Support 计划，则可以访问所有检查。有关更多信息，请参阅 AWS Trusted Advisor 检查引用 (p. 65)。

您可以使用 AWS Identity and Access Management (IAM) 控制对 Trusted Advisor 的访问权限。

主题

- Trusted Advisor 控制台的权限 (p. 224)
- Trusted Advisor 操作 (p. 227)
- IAM policy 示例 (p. 230)
- 另请参阅 (p. 234)

Trusted Advisor 控制台的权限

要访问 Trusted Advisor 控制台，用户必须拥有一组最低的权限。这些权限必须允许用户列出和查看有关您的 AWS 账户 中的 Trusted Advisor 资源的详细信息。

可以使用以下选项来控制对 Trusted Advisor 的访问：

- 使用 Trusted Advisor 控制台的标签筛选条件功能。用户或角色必须具有与标签关联的权限。

  可以使用 AWS 托管策略或自定义策略来按标签分配权限。有关更多信息，请参阅 使用标签控制对 IAM 用户和角色的访问。
- 使用 `trustedadvisor` 命名空间创建 IAM policy。您可以使用此策略来指定操作和资源的权限。

创建策略时，可以指定服务的命名空间来允许或拒绝操作。Trusted Advisor 的命名空间为 `trustedadvisor`。但是，不能使用 `trustedadvisor` 命名空间来允许或拒绝 AWS Support API 中的 Trusted Advisor API 操作。相反，您必须使用 AWS Support 的 `support` 命名空间。

> **Note**
>
> 如果您具有 AWS Support API 的权限，则 Trusted Advisor 中的 AWS Management Console 小组件将显示 Trusted Advisor 结果的摘要视图。要在 Trusted Advisor 控制台中查看结果，您必须具有 `trustedadvisor` 命名空间的权限。

Trusted Advisor 操作

可以在控制台中执行以下 Trusted Advisor 操作。还可以在 IAM policy 中指定这些 Trusted Advisor 操作以允许或拒绝特定操作。

操作	描述
`DescribeAccount`	授予权限以查看 AWS Support 计划和各种 Trusted Advisor 首选项。
`DescribeAccountAccess`	授予权限以查看 AWS 账户 是否启用或禁用了 Trusted Advisor。
`DescribeCheckItems`	授予权限以查看检查项目的详细信息。
`DescribeCheckRefreshStatuses`	授予权限以查看 Trusted Advisor 检查的刷新状态。
`DescribeCheckSummaries`	授予权限以查看 Trusted Advisor 检查摘要。
`DescribeChecks`	授予权限以查看 Trusted Advisor 检查的详细信息。
`DescribeNotificationPreferences`	授予权限以查看 AWS 账户的通知首选项。
`ExcludeCheckItems`	授予权限以排除 Trusted Advisor 检查的建议。
`IncludeCheckItems`	授予权限以包含 Trusted Advisor 检查的建议。

操作	描述
RefreshCheck	授予权限以刷新 Trusted Advisor 检查。
SetAccountAccess	授予权限以便为账户启用或禁用 Trusted Advisor。
UpdateNotificationPreferences	授予权限以更新 Trusted Advisor 的通知首选项。
DescribeCheckStatusHistoryChanges	授予查看过去 30 天内检查结果和更改状态的权限。

组织视图的 Trusted Advisor 操作

以下 Trusted Advisor 操作用于组织视图功能。有关更多信息，请参阅AWS Trusted Advisor 的组织视图 (p. 29)：

操作	描述
DescribeOrganization	授予权限以查看 AWS 账户 是否满足启用组织视图功能的要求。
DescribeOrganizationAccounts	授予权限以查看组织中的关联 AWS 账户。
DescribeReports	授予权限以查看组织视图报告的详细信息（例如，报告名称、运行时间、创建日期、状态和格式）。
DescribeServiceMetadata	授予权限以查看有关组织视图报告的信息（例如，AWS 区域、检查类别、检查名称和资源状态）。
GenerateReport	授予权限以便为组织中的 Trusted Advisor 检查创建报告。
ListAccountsForParent	授予在 Trusted Advisor 控制台中查看 AWS 组织中由根或组织单位 (OU) 包含的所有账户的权限。
ListOrganizationalUnitsForParent	授予在 Trusted Advisor 控制台中查看父组织单位或根中所有组织单位 (OU) 的权限。
ListRoots	授予在 Trusted Advisor 控制台中查看 AWS 组织中定义的所有根的权限。
SetOrganizationAccess	授予权限以便为 Trusted Advisor 启用组织视图功能。

Trusted Advisor Priority 操作

如果您为账户启用了 Trusted Advisor Priority，则您可以在控制台中执行以下 Trusted Advisor 操作。还可以在 IAM policy 中添加这些 Trusted Advisor 操作以允许或拒绝特定操作。有关更多信息，请参阅Trusted Advisor Priority 的 IAM policy 示例 (p. 232)：

> Note
>
> Trusted Advisor Priority 中出现的风险是您的技术客户经理 (TAM) 为您的账户确定的建议。系统会自动为您创建来自服务的建议，例如 Trusted Advisor 检查。来自 TAM 的建议是手动为您创建的。接下来，您的 TAM 会发送这些建议，以便它们出现在您账户的 Trusted Advisor Priority 中。

有关更多信息，请参阅AWS Trusted Advisor Priority 入门 (p. 52)：

操作	描述
DescribeRisks	授予权限以查看 Trusted Advisor Priority 中的风险。
DescribeRisk	授予权限以查看 Trusted Advisor Priority 中的风险详细信息。
DescribeRiskResources	授予权限以查看 Trusted Advisor Priority 中受影响的风险资源。
DownloadRisk	授予权限以下载包含 Trusted Advisor Priority 中风险详细信息的文件。
UpdateRiskStatus	授予权限以更新 Trusted Advisor Priority 中的风险状态。
DescribeNotificationConfigurations	授予权限以获取 Trusted Advisor Priority 的电子邮件通知首选项。
UpdateNotificationConfigurations	授予权限以创建或更新 Trusted Advisor Priority 的电子邮件通知首选项。
DeleteNotificationConfigurationForDelegatedAdmin	授予组织管理账户权限，以允许其从 Trusted Advisor Priority 的委派管理员账户中删除电子邮件通知首选项。

Trusted Advisor参与行动

如果您为账户启用了 Eng Trusted Advisor age，则可以在控制台中执行以下Trusted Advisor操作。还可以在 IAM policy 中添加这些 Trusted Advisor 操作以允许或拒绝特定操作。有关更多信息，请参阅 Trusted Advisor参与的 IAM 政策示例 (p. 232)。

有关更多信息，请参阅开始使用 EngAWS Trusted Advisor age（预览版） (p. 59)：

操作	描述
CreateEngagement	授予在 Engage 中创建Trusted Advisor互动的权限。
CreateEngagementAttachment	授予在 Engage 中创建Trusted Advisor参与附件的权限。
CreateEngagementCommunication	授予在 Eng Trusted Advisor age 中创建互动交流的权限。
GetEngagement	授予在 Trusted Advisor Engage 中查看参与的权限。
GetEngagementAttachment	授予在 Engage 中查看Trusted Advisor参与附件的权限。
GetEngagementType	授予在 Engage 中查看特定Trusted Advisor参与类型的权限。
ListEngagementCommunications	授予在 Engage 中查看Trusted Advisor参与的所有通信的权限。

操作	描述
ListEngagements	授予查看 Engage 中所有Trusted Advisor参与的权限。
ListEngagementTypes	授予在 Engage 中查看所有Trusted Advisor参与类型的权限。
UpdateEngagementStatus	授予在 Engage 中更新Trusted Advisor参与状态的权限。

IAM policy 示例

以下策略介绍如何允许和拒绝对 Trusted Advisor 的访问。您可以使用下面的策略之一来在 IAM 控制台中创建客户托管策略。例如，您可以复制示例策略，然后将其粘贴到 IAM 控制台的 JSON 选项卡中。然后，将策略附加您的 IAM 用户、组或角色。

有关如何创建 IAM policy 的更多信息，请参阅 IAM 用户指南中的创建 IAM policy（控制台）。

示例

- 对 Trusted Advisor 的完全访问权限 (p. 230)
- 对 Trusted Advisor 的只读访问权限 (p. 230)
- 拒绝对 Trusted Advisor 的访问 (p. 231)
- 允许和拒绝特定操作 (p. 231)
- 控制对 Trusted Advisor 的 AWS Support API 操作的访问 (p. 231)
- Trusted Advisor Priority 的 IAM policy 示例 (p. 232)
- Trusted Advisor参与的 IAM 政策示例 (p. 232)

对 Trusted Advisor 的完全访问权限

以下策略允许用户在 Trusted Advisor 控制台中查看和执行针对所有 Trusted Advisor 检查的所有操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

对 Trusted Advisor 的只读访问权限

以下策略允许用户对 Trusted Advisor 控制台进行只读访问。用户无法进行任何更改，例如刷新检查或更改通知首选项。

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

```
                "trustedadvisor:Get*",
                "trustedadvisor:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

拒绝对 Trusted Advisor 的访问

以下策略不允许用户在 Trusted Advisor 控制台中查看或执行针对 Trusted Advisor 检查的操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

允许和拒绝特定操作

以下策略允许用户在 Trusted Advisor 控制台中查看所有 Trusted Advisor 检查，但不允许用户刷新任何检查。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:RefreshCheck",
            "Resource": "*"
        }
    ]
}
```

控制对 Trusted Advisor 的 AWS Support API 操作的访问

在 AWS Management Console中，单独的 `trustedadvisor` IAM 命名空间控制对 Trusted Advisor 的访问。不能使用 `trustedadvisor` 命名空间来允许或拒绝 AWS Support API 中的 Trusted Advisor API 操作。相反，可以使用 `support` 命名空间。您必须具有对 AWS Support API 的权限才能以编程方式调用 Trusted Advisor。

例如，如果您想调用该RefreshTrustedAdvisorCheck操作，则必须在策略中拥有此操作的权限。

Example ：仅允许 Trusted Advisor API 操作

以下策略允许用户访问 Trusted Advisor 的 AWS Support API 操作，而不允许用户访问其余的 AWS Support API 操作。例如，用户可以使用 API 查看和刷新检查。它们无法创建、查看、更新或解析 AWS Support 案例。

您可以使用此策略以编程方式调用 Trusted Advisor API 操作，但您无法使用此策略在 Trusted Advisor 控制台中查看或刷新检查。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
            "Resource": "*"
        }
    ]
}
```

有关 IAM 如何使用 AWS Support 和 Trusted Advisor 的更多信息，请参阅 操作 (p. 195)。

Trusted Advisor Priority 的 IAM policy 示例

您可以使用以下 AWS 托管策略来控制对 Trusted Advisor Priority 的访问。有关更多信息，请参阅 AWS适用于 AWS Trusted Advisor 的托管策略 (p. 213) 和 AWS Trusted Advisor Priority 入门 (p. 52)。

Trusted Advisor参与的 IAM 政策示例

> **Note**
>
> Trusted AdvisorEngage 处于预览版中，目前没有任何AWS托管策略。您可以使用下面的策略之一来在 IAM 控制台中创建客户托管策略。

在 Eng Trusted Advisor age 中授予读写权限的策略示例：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

在 Eng Trusted Advisor age 中授予只读访问权限的策略示例：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*"
            ],
            "Resource": "*"
        }
    ]
}
```

在 Eng Trusted Advisor age 中授予读写访问权限以及启用对以下内容的可信访问权限的策略示例Trusted Advisor：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:CreateEngagement*",
                "trustedadvisor:DescribeAccount*",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:GetEngagement*",
                "trustedadvisor:ListEngagement*",
                "trustedadvisor:SetOrganizationAccess",
                "trustedadvisor:UpdateEngagement*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": [
                        "reporting.trustedadvisor.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/
reporting.trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisorReporting",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "reporting.trustedadvisor.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

另请参阅

有关 Trusted Advisor 权限的更多信息，请参阅以下资源：

- IAM 用户指南中的由 AWS Trusted Advisor 定义的操作。
- 控制对 Trusted Advisor 控制台的访问

对 AWS Support 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 AWS Support 和 IAM 时可能遇到的常见问题。

主题

- 我无权执行 iam：PassRole (p. 234)
- 我想要查看我的访问密钥 (p. 234)
- 我是管理员并希望允许其他人访问 AWS Support (p. 235)
- 我希望允许我的 AWS 账户之外的人员访问我的 AWS Support 资源 (p. 235)

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 AWS Support。

有些 AWS 服务允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 AWS Support 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 AWS 管理员。管理员是向您提供登录凭证的人。

我想要查看我的访问密钥

在创建 IAM 用户访问密钥后，您可以随时查看您的访问密钥 ID。但是，您无法再查看您的秘密访问密钥。如果您丢失了私有密钥，则必须创建一个新的访问密钥对。

访问密钥包含两部分：访问密钥 ID（例如 `AKIAIOSFODNN7EXAMPLE`）和秘密访问密钥（例如 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`）。与用户名和密码一样，您必须同时使用访问密钥 ID 和秘密访问密钥对请求执行身份验证。像对用户名和密码一样，安全地管理访问密钥。

> **Important**
>
> 请不要向第三方提供访问密钥，即便是为了帮助找到您的规范用户 ID 也不行。如果您这样做，可能会向某人提供对您的账户的永久访问权限。

当您创建访问密钥对时，系统会提示您将访问密钥 ID 和秘密访问密钥保存在一个安全位置。秘密访问密钥仅在您创建它时可用。如果丢失了您的秘密访问密钥，您必须为 IAM 用户添加新的访问密钥。您最多可拥有

两个访问密钥。如果您已有两个密钥，则必须删除一个密钥对，然后再创建新的密钥。要查看说明，请参阅 IAM 用户指南中的管理访问密钥。

我是管理员并希望允许其他人访问 AWS Support

要允许其他人访问 AWS Support，您必须为需要访问权限的人员或应用程序创建一个 IAM 实体（用户或角色）。它们将使用该实体的凭证访问 AWS。然后，您必须将策略附加到实体，以便在 AWS Support 中向其授予正确的权限。

要立即开始使用，请参阅 IAM 用户指南中的创建您的第一个 IAM 委派用户和组。

我希望允许我的 AWS 账户之外的人员访问我的 AWS Support 资源

您可以创建一个角色，以便其它账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 AWS Support 是否支持这些功能，请参阅 AWS Support 如何与 IAM 协同工作 (p. 194)。
- 要了解如何为您拥有的 AWS 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的为您拥有的另一个 AWS 账户 中的 IAM 用户提供访问权限。
- 要了解如何为第三方AWS 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的为第三方拥有的AWS 账户提供访问权限。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅 IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

事件响应

AWS Support 的事件响应是一项 AWS 责任。AWS 拥有正式的、已归档的策略和程序来管理事件响应。有关更多信息，请参阅“AWS 安全事件响应简介”白皮书。

使用以下选项可自行获知操作性问题：

- 具有广泛影响的 AWS 操作性问题将在 AWS Service Health Dashboard 上发布。例如，影响非账户特定的服务或区域的事件。
- 在 AWS Health Dashboard 中查看单个账户的操作性问题。例如，影响账户中的服务或资源的事件。有关更多信息，请参阅 AWS Health 用户指南中的 AWS Health Dashboard 入门。

AWS Support 和 AWS Trusted Advisor 中的日志记录和监控

监控是保持 AWS Support 和 AWS Trusted Advisor 以及您的其他 AWS 解决方案的可靠性、可用性和性能的重要方面。AWS 提供了以下监控工具来监控 AWS Support 和 AWS Trusted Advisor、在出现错误时进行报告，并适时采取措施。

- 亚马逊实时CloudWatch监控您的AWS资源和您运行AWS的应用程序。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以

CloudWatch跟踪您的亚马逊弹性计算云 (Amazon EC2) 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅亚马逊CloudWatch用户指南。

- Amazon EventBridge 提供近乎实时的系统事件流，用于描述AWS资源变化。EventBridge 支持自动事件驱动型计算，因为您可以编写规则，以监控某些事件和在这些事件发生时在其他 AWS 服务中触发自动操作。有关更多信息，请参阅亚马逊EventBridge用户指南。
- AWS CloudTrail 捕获由您的 AWS 账户或代表该账户发出的 API 调用和相关事件，并将日志文件传送到您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 AWS CloudTrail 用户指南。

有关更多信息，请参阅 AWS Support 的监控和日志记录 (p. 311) 和 AWS Trusted Advisor 的监控和日志记录 (p. 327)。

AWS Support 的合规性验证

要了解某个 AWS 服务 是否在特定合规性计划范围内，请参阅 合规性计划范围内的 AWS 服务，然后选择您感兴趣的合规性计划。有关常规信息，请参阅AWS合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅在 AWS Artifact 中下载报告、。

您使用 AWS 服务 的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署以安全性和合规性为重点的基准环境的步骤。
- Amazon Web Services 上的 HIPAA 安全性和合规性架构设计– 该白皮书介绍了公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。

  Note

  并非所有 AWS 服务都符合 HIPAA 要求。有关更多信息，请参阅符合 HIPAA 要求的服务参考。
- AWS合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- AWS Config 开发人员指南中的使用规则评估资源 – 此 AWS Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub – 此 AWS 服务 向您提供 AWS 中安全状态的全面视图。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- AWS Audit Manager – 此 AWS 服务可帮助您持续审计您的 AWS 使用情况，以简化管理风险以及与相关法规和行业标准的合规性的方式。

AWS Support 中的故障恢复能力

AWS全球基础设施围绕AWS区域和可用区构建。AWS区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅 AWS 全球基础设施。

AWS Support 中的基础设施安全性

作为一项托管式服务，AWS Support 由 Amazon Web Services：安全流程概览白皮书中所述的AWS全球网络安全程序提供保护。

您可以使用 AWS 发布的 API 调用通过网络访问 AWS Support。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

AWS Support 中的配置和漏洞分析

对于 AWS Trusted Advisor，AWS 负责处理来宾操作系统 (OS) 和数据库补丁、防火墙配置和灾难恢复等基本安全任务。

配置和 IT 控制是AWS和您（我们的客户）之间的共同责任。有关更多信息，请参阅AWS责任共担模型。

使用 AWS 开发工具包的 AWS Support 代码示例

以下代码示例显示如何将 AWS Support 与 AWS 软件开发工具包（SDK）一起使用。

操作是大型程序的代码摘录，必须在上下文中运行。虽然操作向您展示了如何调用单个服务函数，但您可以在其相关场景和跨服务示例中查看操作的上下文。

场景是展示如何通过在同一服务中调用多个函数来完成特定任务的代码示例。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

开始使用

Hello AWS Support

以下代码示例显示如何开始使用 AWS Support。

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
using Amazon.AWSSupport;
using Microsoft.Extensions.DependencyInjection;
using Microsoft.Extensions.Hosting;

public static class HelloSupport
{
    static async Task Main(string[] args)
    {
        // Use the AWS .NET Core Setup package to set up dependency injection for
 the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default profile.
        // You must have one of the following AWS Support plans: Business,
 Enterprise On-Ramp, or Enterprise. Otherwise, an exception will be thrown.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>()
            ).Build();

        // Now the client is available for injection.
        var supportClient = host.Services.GetRequiredService<IAmazonAWSSupport>();

        // You can use await and any of the async methods to get a response.
        var response = await supportClient.DescribeServicesAsync();
        Console.WriteLine($"\tHello AWS Support! There are
 {response.Services.Count} services available.");
    }
```

```
}
```

- 有关 API 的详细信息，请参阅 DescribeServicesAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
/**
 * Before running this Java (v2) code example, set up your development environment,
 including your credentials.
 *
 * For more information, see the following documentation topic:
 *
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
 *
 *  In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:
 *
 *  https://aws.amazon.com/premiumsupport/plans/
 *
 *  This Java example performs the following task:
 *
 * 1. Gets and displays available services.
 *
 *
 * NOTE: To see multiple operations, see SupportScenario.
 */

public class HelloSupport {

    public static void main(String[] args) {
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
            .region(region)
            .build();

        System.out.println("***** Step 1. Get and display available services.");
        displayServices(supportClient);
      }

   // Return a List that contains a Service name and Category name.
    public static void displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                .language("en")
                .build();

            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service: services) {
                if (index== 11)
                    break;
```

```
                System.out.println("The Service name is: "+service.name());

                // Display the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat: categories) {
                    System.out.println("The category name is: "+cat.name());
                }
                index++ ;
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
}
```

- 有关 API 的详细信息，请参阅 DescribeServicesAWS SDK for Java 2.xAPI 参考文档。

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

调用 `main()` 运行该示例。

```
import {
  DescribeServicesCommand,
  SupportClient,
} from "@aws-sdk/client-support";

// Change the value of 'region' to your preferred AWS Region.
const client = new SupportClient({ region: "us-east-1" });

const getServiceCount = async () => {
  try {
    const { services } = await client.send(new DescribeServicesCommand({}));
    return services.length;
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature."
      );
    } else {
      throw err;
    }
  }
};

export const main = async () => {
  try {
    const count = await getServiceCount();
    console.log(`Hello, AWS Support! There are ${count} services available.`);
  } catch (err) {
    console.error("Failed to get service count: ", err.message);
  }
};
```

- 有关 API 的详细信息，请参阅 DescribeServicesAWS SDK for JavaScriptAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:
https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html

In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following task:

1. Gets and displays available services.
 */

suspend fun main() {
    displaySomeServices()
}

// Return a List that contains a Service name and Category name.
suspend fun displaySomeServices() {
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is: " + service.name)

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                index++
            }
        }
    }
}
```

- 有关 API 详细信息，请参阅DescribeServices《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
import logging
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)

def hello_support(support_client):
    """
    Use the AWS SDK for Python (Boto3) to create an AWS Support client and count
    the available services in your account.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param support_client: A Boto3 Support Client object.
    """
    try:
        print("Hello, AWS Support! Let's count the available Support services:")
        response = support_client.describe_services()
        print(f"There are {len(response['services'])} services available.")
    except ClientError as err:
        if err.response['Error']['Code'] == 'SubscriptionRequiredException':
            logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                        "plan to use the AWS Support API. \n\tPlease upgrade your
 subscription to run these "
                        "examples.")
        else:
            logger.error(
                "Couldn't count services. Here's why: %s: %s",
                err.response['Error']['Code'], err.response['Error']['Message'])
            raise

if __name__ == '__main__':
    hello_support(boto3.client('support'))
```

- 有关 API 详细信息，请参阅DescribeServices《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

代码示例

- 使用 AWS 开发工具包的 AWS Support 操作 (p. 243)
  - 使用 AWS SDK 向案例添加 AWS Support 通信 (p. 243)
  - 使用 AWS SDK 向集合添加 AWS Support 附件 (p. 247)
  - 使用 AWS SDK 创建 AWS Support 案例 (p. 250)
  - 使用 AWS SDK 描述 AWS Support 案例的附件 (p. 254)
  - 使用 AWS SDK 描述 AWS Support 案例 (p. 257)
  - 使用 AWS SDK 描述案例的 AWS Support 通信 (p. 261)

- 使用 AWS SDK 描述支持案例的可用 AWS 服务 (p. 265)
- 使用 AWS SDK 描述 AWS Support 严重性级别 (p. 268)
- 使用 AWS SDK 解析 AWS Support 案例 (p. 271)
- 使用 AWS 开发工具包的 AWS Support 场景 (p. 274)
  - 使用 AWS SDK 开始处理 AWS Support 案例 (p. 274)

使用 AWS 开发工具包的 AWS Support 操作

以下代码示例演示了如何使用 AWS 开发工具包来执行各个 AWS Support 操作。这些摘录调用 AWS Support API，是大型程序的代码摘录，必须在上下文中运行。每个示例都包含一个链接GitHub，其中包含了有关设置和运行代码的说明。

以下示例仅包括最常用的操作。有关完整列表，请参阅 AWS Support API 参考。

示例

- 使用 AWS SDK 向案例添加 AWS Support 通信 (p. 243)
- 使用 AWS SDK 向集合添加 AWS Support 附件 (p. 247)
- 使用 AWS SDK 创建 AWS Support 案例 (p. 250)
- 使用 AWS SDK 描述 AWS Support 案例的附件 (p. 254)
- 使用 AWS SDK 描述 AWS Support 案例 (p. 257)
- 使用 AWS SDK 描述案例的 AWS Support 通信 (p. 261)
- 使用 AWS SDK 描述支持案例的可用 AWS 服务 (p. 265)
- 使用 AWS SDK 描述 AWS Support 严重性级别 (p. 268)
- 使用 AWS SDK 解析 AWS Support 案例 (p. 271)

使用 AWS SDK 向案例添加 AWS Support 通信

以下代码示例显示如何将带附件的 AWS Support 通信添加到支持案例。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 开始使用案例 (p. 274)

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</param>
    /// <returns>True if successful.</returns>
```

```
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }
```

- 有关 API 的详细信息，请参阅 AddCommunicationToCaseAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
        try {
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                .caseId(caseId)
                .attachmentSetId(attachmentSetId)
                .communicationBody("Please refer to attachment for details.")
                .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication to
an AWS Support case");
            else
                System.out.println("There was an error adding the communication to
an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- 有关 API 的详细信息，请参阅 AddCommunicationToCaseAWS SDK for Java 2.xAPI 参考文档。

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
import { AddCommunicationToCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  let attachmentSetId;

  try {
    // Add a communication to a case.
    const response = await client.send(
      new AddCommunicationToCaseCommand({
        communicationBody: "Adding an attachment.",
        // Set value to an existing support case id.
        caseId: "CASE_ID",
        // Optional. Set value to an existing attachment set id to add attachments
 to the case.
        attachmentSetId,
      })
    );
    console.log(response);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 有关 API 的详细信息，请参阅 AddCommunicationToCaseAWS SDK for JavaScriptAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
suspend fun addAttachSupportCase(caseIdVal: String?, attachmentSetIdVal: String?) {
    val caseRequest = AddCommunicationToCaseRequest {
        caseId = caseIdVal
        attachmentSetId = attachmentSetIdVal
        communicationBody = "Please refer to attachment for details."
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS Support
 case")
        } else {
            println("There was an error adding the communication to an AWS Support
 case")
        }
    }
}
```

- 有关 API 详细信息，请参阅AddCommunicationToCase《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client('support')
        return cls(support_client)

    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
 support case.",
                attachmentSetId=attachment_set_id
            )
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
```

- 有关 API 详细信息，请参阅AddCommunicationToCase《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

使用 AWS SDK 向集合添加 AWS Support 附件

以下代码示例显示如何将 AWS Support 附件添加到附件集。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 开始使用案例 (p. 274)

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does not
exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates a
new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
   public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
   {
       var response = await _amazonSupport.AddAttachmentsToSetAsync(
           new AddAttachmentsToSetRequest
           {
               AttachmentSetId = attachmentSetId,
               Attachments = new List<Attachment>
               {
                   new Attachment
                   {
                       Data = data,
                       FileName = fileName
                   }
               }
           });
       return response.AttachmentSetId;
   }
```

- 有关 API 的详细信息，请参阅 AddAttachmentsToSetAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
   public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
       try {
```

```
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                .fileName(myFile.getName())
                .data(sourceBytes)
                .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                .attachments(attachment)
                .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();

        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- 有关 API 的详细信息，请参阅 AddAttachmentsToSetAWS SDK for Java 2.xAPI 参考文档。

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
import { AddAttachmentsToSetCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new attachment set or add attachments to an existing set.
    // Provide an 'attachmentSetId' value to add attachments to an existing set.
    // Use AddCommunicationToCase or CreateCase to associate an attachment set with
 a support case.
    const response = await client.send(
      new AddAttachmentsToSetCommand({
        // You can add up to three attachments per set. The size limit is 5 MB per
 attachment.
        attachments: [
          {
            fileName: "example.txt",
            data: new TextEncoder().encode("some example text"),
          },
        ],
      })
    );
    // Use this ID in AddCommunicationToCase or CreateCase.
    console.log(response.attachmentSetId);
    return response;
  } catch (err) {
    console.error(err);
```

```
  }
};
```

- 有关 API 的详细信息，请参阅 AddAttachmentsToSetAWS SDK for JavaScriptAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal = Attachment {
        fileName = myFile.name
        data = sourceBytes
    }

    val setRequest = AddAttachmentsToSetRequest {
        attachments = listOf(attachmentVal)
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

- 有关 API 详细信息，请参阅AddAttachmentsToSet《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
```

```
        support_client = boto3.client('support')
        return cls(support_client)

    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does not
 exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        'fileName': 'attachment_file.txt',
                        'data': b"This is a sample file for attachment to a support
 case."
                    }
                ])
            new_set_id = response['attachmentSetId']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return new_set_id
```

- 有关 API 详细信息，请参阅AddAttachmentsToSet《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

使用 AWS SDK 创建 AWS Support 案例

以下代码示例显示如何创建新的 AWS Support 案例。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 开始使用案例 (p. 274)

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

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

```
   /// Create a new support case.
   /// </summary>
   /// <param name="serviceCode">Service code for the new case.</param>
   /// <param name="categoryCode">Category for the new case.</param>
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the new
case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
   /// <returns>The caseId of the new support case.</returns>
   public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
       string body, string language = "en", string? attachmentSetId = null, string
issueType = "customer-service")
   {
       var response = await _amazonSupport.CreateCaseAsync(
           new CreateCaseRequest()
           {
               ServiceCode = serviceCode,
               CategoryCode = categoryCode,
               SeverityCode = severityCode,
               Subject = subject,
               Language = language,
               AttachmentSetId = attachmentSetId,
               IssueType = issueType,
               CommunicationBody = body
           });
       return response.CaseId;
   }
```

- 有关 API 的详细信息，请参阅 CreateCaseAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
   public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
       try {
           String serviceCode = sevCatList.get(0);
           String caseCat = sevCatList.get(1);
           CreateCaseRequest caseRequest = CreateCaseRequest.builder()
               .categoryCode(caseCat.toLowerCase())
               .serviceCode(serviceCode.toLowerCase())
               .severityCode(sevLevel.toLowerCase())
               .communicationBody("Test issue with "+serviceCode.toLowerCase())
               .subject("Test case, please ignore")
               .language("en")
               .issueType("technical")
               .build();

           CreateCaseResponse response = supportClient.createCase(caseRequest);
           return response.caseId();
```

```
        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- 有关 API 的详细信息，请参阅 CreateCaseAWS SDK for Java 2.xAPI 参考文档。

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
import { CreateCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Create a new case and log the case id.
    // Important: This creates a real support case in your account.
    const response = await client.send(
      new CreateCaseCommand({
        // The subject line of the case.
        subject: "IGNORE: Test case",
        // Use DescribeServices to find available service codes for each service.
        serviceCode: "service-quicksight-end-user",
        // Use DescribeSecurityLevels to find available severity codes for your
 support plan.
        severityCode: "low",
        // Use DescribeServices to find available category codes for each service.
        categoryCode: "end-user-support",
        // The main description of the support case.
        communicationBody: "This is a test. Please ignore."
      })
    );
    console.log(response.caseId);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 有关 API 的详细信息，请参阅 CreateCaseAWS SDK for JavaScriptAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
suspend fun createSupportCase(sevCatListVal: List<String>, sevLevelVal: String):
 String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest = CreateCaseRequest {
        categoryCode = caseCategory.lowercase(Locale.getDefault())
        serviceCode = serCode.lowercase(Locale.getDefault())
        severityCode = sevLevelVal.lowercase(Locale.getDefault())
        communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
        subject = "Test case, please ignore"
        language = "en"
        issueType = "technical"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```

- 有关 API 详细信息，请参阅CreateCase《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client('support')
        return cls(support_client)

    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject='Example case for testing, ignore.',
                serviceCode=service['code'],
                severityCode=severity['code'],
```

```
                categoryCode=category['code'],
                communicationBody='Example support case body.',
                language='en',
                issueType='customer-service'
            )
            case_id = response['caseId']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return case_id
```

- 有关 API 详细信息，请参阅CreateCase《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

使用 AWS SDK 描述 AWS Support 案例的附件

以下代码示例显示如何描述 AWS Support 案例的附件。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 开始使用案例 (p. 274)

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
   /// <summary>
   /// Get description of a specific attachment.
   /// </summary>
   /// <param name="attachmentId">Id of the attachment, usually fetched by
 describing the communications of a case.</param>
   /// <returns>The attachment object.</returns>
   public async Task<Attachment> DescribeAttachment(string attachmentId)
   {
       var response = await _amazonSupport.DescribeAttachmentAsync(
           new DescribeAttachmentRequest()
           {
               AttachmentId = attachmentId
           });
       return response.Attachment;
   }
```

```
```

- 有关 API 的详细信息，请参阅 DescribeAttachmentAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
   public static void describeAttachment(SupportClient supportClient,String
attachId) {
       try {
           DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
               .attachmentId(attachId)
               .build();

           DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
           System.out.println("The name of the file is
"+response.attachment().fileName());

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
   }
```

- 有关 API 的详细信息，请参阅 DescribeAttachmentAWS SDK for Java 2.xAPI 参考文档。

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
import { DescribeAttachmentCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the metadata and content of an attachment.
    const response = await client.send(
      new DescribeAttachmentCommand({
        // Set value to an existing attachment id.
        // Use DescribeCommunications or DescribeCases to find an attachment id.
        attachmentId: "ATTACHMENT_ID",
      })
    );
    console.log(response.attachment?.fileName);
    return response;
  } catch (err) {
    console.error(err);
```

```
  }
};
```

- 有关 API 的详细信息，请参阅 DescribeAttachmentAWS SDK for JavaScriptAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest = DescribeAttachmentRequest {
        attachmentId = attachId
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

- 有关 API 详细信息，请参阅DescribeAttachment《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client('support')
        return cls(support_client)

    def describe_attachment(self, attachment_id):
        """
        Get information about an attachment by its attachmentID.
```

```
        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response['attachment']['fileName']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return attached_file
```

- 有关 API 详细信息，请参阅DescribeAttachment《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

使用 AWS SDK 描述 AWS Support 案例

以下代码示例显示如何描述 AWS Support 案例。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 开始使用案例 (p. 274)

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication. Defaults
 to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases. Defaults
 to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
```

```
   /// <param name="language">Optional language support for your case.
   /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
   /// <returns>A list of CaseDetails.</returns>
   public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
string? displayId = null, bool includeCommunication = true,
       bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
beforeTime = null,
       string language = "en")
   {
       var results = new List<CaseDetails>();
       var paginateCases = _amazonSupport.Paginators.DescribeCases(
           new DescribeCasesRequest()
           {
               CaseIdList = caseIds,
               DisplayId = displayId,
               IncludeCommunications = includeCommunication,
               IncludeResolvedCases = includeResolvedCases,
               AfterTime = afterTime?.ToString("s"),
               BeforeTime = beforeTime?.ToString("s"),
               Language = language
           });
       // Get the entire list using the paginator.
       await foreach (var cases in paginateCases.Cases)
       {
           results.Add(cases);
       }
       return results;
   }
```

- 有关 API 的详细信息，请参阅 DescribeCasesAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
   public static void getOpenCase(SupportClient supportClient) {
       try {
           // Specify the start and end time.
           Instant now = Instant.now();
           java.time.LocalDate.now();
           Instant yesterday = now.minus(1, ChronoUnit.DAYS);

           DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
               .maxResults(20)
               .afterTime(yesterday.toString())
               .beforeTime(now.toString())
               .build();

           DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
           List<CaseDetails> cases = response.cases();
           for (CaseDetails sinCase: cases) {
               System.out.println("The case status is "+sinCase.status());
               System.out.println("The case Id is "+sinCase.caseId());
               System.out.println("The case subject is "+sinCase.subject());
           }
```

```
        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- 有关 API 的详细信息，请参阅 DescribeCasesAWS SDK for Java 2.xAPI 参考文档。

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
import { DescribeCasesCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all of the unresolved cases in your account.
    // Filter or expand results by providing parameters to the
 DescribeCasesCommand. Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecasescommandinput.html
    const response = await client.send(new DescribeCasesCommand({}));
    const caseIds = response.cases.map((supportCase) => supportCase.caseId);
    console.log(caseIds);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 有关 API 的详细信息，请参阅 DescribeCasesAWS SDK for JavaScriptAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 20
```

```
        afterTime = yesterday.toString()
        beforeTime = now.toString()
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}
```

- 有关 API 详细信息，请参阅DescribeCases《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client('support')
        return cls(support_client)

    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
        try:
            cases = []
            paginator = self.support_client.get_paginator('describe_cases')
            for page in paginator.paginate(
                    afterTime=after_time,
                    beforeTime=before_time,
                    includeResolvedCases=resolved,
                    language='en'):
                cases += page['cases']
        except ClientError as err:
```

```
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            if resolved:
                cases = filter(lambda case: case['status'] == 'resolved', cases)
            return cases
```

- 有关 API 详细信息，请参阅DescribeCases《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

使用 AWS SDK 描述案例的 AWS Support 通信

以下代码示例显示如何描述案例的 AWS Support 通信。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 开始使用案例 (p. 274)

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
 _amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s")
```

```
            });
        // Get the entire list using the paginator.
        await foreach (var communications in paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }
```

- 有关 API 的详细信息，请参阅 DescribeCommunicationsAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
   public static String listCommunications(SupportClient supportClient, String
caseId) {
       try {
           String attachId = null;
           DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                   .caseId(caseId)
                   .maxResults(10)
                   .build();

           DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
           List<Communication> communications = response.communications();
           for (Communication comm: communications) {
               System.out.println("the body is: " + comm.body());

               //Get the attachment id value.
               List<AttachmentDetails> attachments = comm.attachmentSet();
               for (AttachmentDetails detail : attachments) {
                   attachId = detail.attachmentId();
               }
           }
           return attachId;

       } catch (SupportException e) {
           System.out.println(e.getLocalizedMessage());
           System.exit(1);
       }
       return "";
   }
```

- 有关 API 的详细信息，请参阅 DescribeCommunicationsAWS SDK for Java 2.xAPI 参考文档。

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
import { DescribeCommunicationsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get all communications for the support case.
    // Filter results by providing parameters to the DescribeCommunicationsCommand.
 Refer
    // to the TypeScript definition and the API doc for more information on
 possible parameters.
    // https://docs.aws.amazon.com/AWSJavaScriptSDK/v3/latest/clients/client-
support/interfaces/describecommunicationscommandinput.html
    const response = await client.send(
      new DescribeCommunicationsCommand({
        // Set value to an existing case id.
        caseId: "CASE_ID",
      })
    );
    const text = response.communications.map((item) => item.body).join("\n");
    console.log(text);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 有关 API 的详细信息，请参阅 DescribeCommunicationsAWS SDK for JavaScriptAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest = DescribeCommunicationsRequest {
        caseId = caseIdVal
        maxResults = 10
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
}
```

- 有关 API 详细信息，请参阅DescribeCommunications《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client('support')
        return cls(support_client)

    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
 self.support_client.get_paginator('describe_communications')
            for page in paginator.paginate(caseId=case_id):
                communications += page['communications']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return communications
```

- 有关 API 详细信息，请参阅DescribeCommunications《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

使用 AWS SDK 描述支持案例的可用 AWS 服务

以下代码示例显示如何描述 AWS 服务列表。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 开始使用案例 (p. 274)

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
/// <summary>
/// Get the descriptions of AWS services.
/// </summary>
/// <param name="name">Optional language for services.
/// Currently "en" (English) and "ja" (Japanese) are supported.</param>
/// <returns>The list of AWS service descriptions.</returns>
public async Task<List<Service>> DescribeServices(string language = "en")
{
    var response = await _amazonSupport.DescribeServicesAsync(
        new DescribeServicesRequest()
        {
            Language = language
        });
    return response.Services;
}
```

- 有关 API 的详细信息，请参阅 DescribeServicesAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
   // Return a List that contains a Service name and Category name.
   public static List<String> displayServices(SupportClient supportClient) {
       try {
           DescribeServicesRequest servicesRequest =
DescribeServicesRequest.builder()
                .language("en")
                .build();

           DescribeServicesResponse response =
supportClient.describeServices(servicesRequest);
           String serviceCode = null;
           String catName = null;
           List<String> sevCatList = new ArrayList<>();
           List<Service> services = response.services();
```

```
            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service: services) {
                if (index== 11)
                    break;

                System.out.println("The Service name is: "+service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat: categories) {
                    System.out.println("The category name is: "+cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
             index++ ;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
```

- 有关 API 的详细信息，请参阅 DescribeServicesAWS SDK for Java 2.xAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
```

```
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- 有关 API 详细信息，请参阅DescribeServices《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client('support')
        return cls(support_client)

    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(
                language=language)
```

```
            services = response['services']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why: %s:
 %s", language,
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return services
```

- 有关 API 详细信息，请参阅DescribeServices《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

使用 AWS SDK 描述 AWS Support 严重性级别

以下代码示例显示如何描述 AWS Support 严重性级别。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 开始使用案例 (p. 274)

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
   /// <summary>
   /// Get the descriptions of support severity levels.
   /// </summary>
   /// <param name="name">Optional language for severity levels.
   /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
   /// <returns>The list of support severity levels.</returns>
   public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language =
"en")
   {
       var response = await _amazonSupport.DescribeSeverityLevelsAsync(
           new DescribeSeverityLevelsRequest()
           {
               Language = language
           });
       return response.SeverityLevels;
   }
```

- 有关 API 的详细信息，请参阅 DescribeSeverityLevelsAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
 DescribeSeverityLevelsRequest.builder()
                .language("en")
                .build();

            DescribeSeverityLevelsResponse response =
 supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
            String levelName = null;
            for (SeverityLevel sevLevel: severityLevels) {
                System.out.println("The severity level name is: "+
 sevLevel.name());
                if (sevLevel.name().compareTo("High")==0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }
```

- 有关 API 的详细信息，请参阅 DescribeSeverityLevelsAWS SDK for Java 2.xAPI 参考文档。

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
import { DescribeSeverityLevelsCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

export const main = async () => {
  try {
    // Get the list of severity levels.
    // The available values depend on the support plan for the account.
    const response = await client.send(new DescribeSeverityLevelsCommand({}));
    console.log(response.severityLevels)
    return response;
  } catch (err) {
    console.error(err);
  }
```

```
};
```

- 有关 API 的详细信息，请参阅 DescribeSeverityLevelsAWS SDK for JavaScriptAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest = DescribeSeverityLevelsRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}
```

- 有关 API 详细信息，请参阅DescribeSeverityLevels《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client('support')
```

```
        return cls(support_client)

    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
 language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response = self.support_client.describe_severity_levels(
                language=language)
            severity_levels = response['severityLevels']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why: %s:
 %s", language,
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return severity_levels
```

- 有关 API 详细信息，请参阅DescribeSeverityLevels《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

使用 AWS SDK 解析 AWS Support 案例

以下代码示例显示如何解析 AWS Support 案例。

操作示例是大型程序的代码摘录，必须在上下文中运行。在以下代码示例中，您可以查看此操作的上下文：

- 开始使用案例 (p. 274)

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
```

```
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }
```

- 有关 API 的详细信息，请参阅 ResolveCaseAWS SDK for .NETAPI 参考文档。

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                .caseId(caseId)
                .build();

            ResolveCaseResponse response = supportClient.resolveCase(caseRequest);
            System.out.println("The status of case "+caseId +" is
"+response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }
```

- 有关 API 的详细信息，请参阅 ResolveCaseAWS SDK for Java 2.xAPI 参考文档。

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
import { ResolveCaseCommand } from "@aws-sdk/client-support";

import { client } from "../libs/client.js";

const main = async () => {
  try {
    const response = await client.send(
      new ResolveCaseCommand({
        caseId: "CASE_ID",
      })
```

```
    );

    console.log(response.finalCaseStatus);
    return response;
  } catch (err) {
    console.error(err);
  }
};
```

- 有关 API 的详细信息，请参阅 ResolveCaseAWS SDK for JavaScriptAPI 参考文档。

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest = ResolveCaseRequest {
        caseId = caseIdVal
    }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}
```

- 有关 API 详细信息，请参阅ResolveCase《AWSSDK for Kotlin API 参考》中的 API 详细信息。

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client('support')
        return cls(support_client)
```

```
    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(
                caseId=case_id
                )
            final_status = response['finalCaseStatus']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return final_status
```

- 有关 API 详细信息，请参阅ResolveCase《AWSSDK for Python (Boto3) API 参考》中的 API 详细信息。

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

使用 AWS 开发工具包的 AWS Support 场景

以下代码示例显示如何通过 AWS 开发工具包实施 AWS Support 中的常见场景。这些场景显示了如何通过在 AWS Support 中调用多个函数来完成特定任务。每个场景都包含一个链接GitHub，其中包含了有关如何设置和运行代码的说明。

示例

- 使用 AWS SDK 开始处理 AWS Support 案例 (p. 274)

使用 AWS SDK 开始处理 AWS Support 案例

以下代码示例显示了如何：

- 获取并显示案例的可用服务和严重级别。
- 使用选定的服务、类别和严重性级别创建支持案例。
- 获取并显示当天打开案例的列表。
- 向新案例添加附件集和通信。
- 描述该案例的新附件和通信。
- 解析案例。
- 获取并显示当天未解决的案例列表。

.NET

AWS SDK for .NET

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

在命令提示符中运行交互式场景。

```
/// <summary>
/// Hello AWS Support example.
/// </summary>
public static class SupportCaseScenario
{
    /*
    Before running this .NET code example, set up your development environment,
 including your credentials.
    To use the AWS Support API, you must have one of the following AWS Support
 plans: Business, Enterprise On-Ramp, or Enterprise.

    This .NET example performs the following tasks:
    1.  Get and display services. Select a service from the list.
    2.  Select a category from the selected service.
    3.  Get and display severity levels and select a severity level from the list.
    4.  Create a support case using the selected service, category, and severity
 level.
    5.  Get and display a list of open support cases for the current day.
    6.  Create an attachment set with a sample text file to add to the case.
    7.  Add a communication with the attachment to the support case.
    8.  List the communications of the support case.
    9.  Describe the attachment set.
    10. Resolve the support case.
    11. Get a list of resolved cases for the current day.
   */

    private static SupportWrapper _supportWrapper = null!;

    static async Task Main(string[] args)
    {
        // Set up dependency injection for the AWS Support service.
        // Use your AWS profile name, or leave it blank to use the default profile.
        using var host = Host.CreateDefaultBuilder(args)
            .ConfigureLogging(logging =>
                logging.AddFilter("System", LogLevel.Debug)
                    .AddFilter<DebugLoggerProvider>("Microsoft",
 LogLevel.Information)
                    .AddFilter<ConsoleLoggerProvider>("Microsoft", LogLevel.Trace))
            .ConfigureServices((_, services) =>
                services.AddAWSService<IAmazonAWSSupport>(new AWSOptions()
 { Profile = "default" })
                    .AddTransient<SupportWrapper>()
            )
            .Build();

        var logger = LoggerFactory.Create(builder =>
        {
            builder.AddConsole();
        }).CreateLogger(typeof(SupportCaseScenario));

        _supportWrapper = host.Services.GetRequiredService<SupportWrapper>();

        Console.WriteLine(new string('-', 80));
        Console.WriteLine("Welcome to the AWS Support case example scenario.");
        Console.WriteLine(new string('-', 80));
```

```
       try
       {
           var apiSupported = await _supportWrapper.VerifySubscription();
           if (!apiSupported)
           {
               logger.LogError("You must have a Business, Enterprise On-Ramp, or
Enterprise Support " +
                               "plan to use the AWS Support API. \n\tPlease
upgrade your subscription to run these examples.");
               return;
           }

           var service = await DisplayAndSelectServices();

           var category = DisplayAndSelectCategories(service);

           var severityLevel = await DisplayAndSelectSeverity();

           var caseId = await CreateSupportCase(service, category, severityLevel);

           await DescribeTodayOpenCases();

           var attachmentSetId = await CreateAttachmentSet();

           await AddCommunicationToCase(attachmentSetId, caseId);

           var attachmentId = await ListCommunicationsForCase(caseId);

           await DescribeCaseAttachment(attachmentId);

           await ResolveCase(caseId);

           await DescribeTodayResolvedCases();

           Console.WriteLine(new string('-', 80));
           Console.WriteLine("AWS Support case example scenario complete.");
           Console.WriteLine(new string('-', 80));
       }
       catch (Exception ex)
       {
           logger.LogError(ex, "There was a problem executing the scenario.");
       }
   }

   /// <summary>
   /// List some available services from AWS Support, and select a service for the
example.
   /// </summary>
   /// <returns>The selected service.</returns>
   private static async Task<Service> DisplayAndSelectServices()
   {
       Console.WriteLine(new string('-', 80));
       var services = await _supportWrapper.DescribeServices();
       Console.WriteLine($"AWS Support client returned {services.Count}
services.");

       Console.WriteLine($"1. Displaying first 10 services:");
       for (int i = 0; i < 10 && i < services.Count; i++)
       {
           Console.WriteLine($"\t{i + 1}. {services[i].Name}");
       }

       var choiceNumber = 0;
       while (choiceNumber < 1 || choiceNumber > services.Count)
       {
```

```
            Console.WriteLine(
                "Select an example support service by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return services[choiceNumber - 1];
    }

    /// <summary>
    /// List the available categories for a service and select a category for the
example.
    /// </summary>
    /// <param name="service">Service to use for displaying categories.</param>
    /// <returns>The selected category.</returns>
    private static Category DisplayAndSelectCategories(Service service)
    {
        Console.WriteLine(new string('-', 80));

        Console.WriteLine($"2. Available support categories for Service
\"{service.Name}\":");
        for (int i = 0; i < service.Categories.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {service.Categories[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > service.Categories.Count)
        {
            Console.WriteLine(
                "Select an example support category by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
            Int32.TryParse(choice, out choiceNumber);
        }

        Console.WriteLine(new string('-', 80));

        return service.Categories[choiceNumber - 1];
    }

    /// <summary>
    /// List available severity levels from AWS Support, and select a level for the
example.
    /// </summary>
    /// <returns>The selected severity level.</returns>
    private static async Task<SeverityLevel> DisplayAndSelectSeverity()
    {
        Console.WriteLine(new string('-', 80));
        var severityLevels = await _supportWrapper.DescribeSeverityLevels();

        Console.WriteLine($"3. Get and display available severity levels:");
        for (int i = 0; i < 10 && i < severityLevels.Count; i++)
        {
            Console.WriteLine($"\t{i + 1}. {severityLevels[i].Name}");
        }

        var choiceNumber = 0;
        while (choiceNumber < 1 || choiceNumber > severityLevels.Count)
        {
            Console.WriteLine(
                "Select an example severity level by entering a number from the
preceding list:");
            var choice = Console.ReadLine();
```

```
            Int32.TryParse(choice, out choiceNumber);
        }
        Console.WriteLine(new string('-', 80));

        return severityLevels[choiceNumber - 1];
    }

    /// <summary>
    /// Create an example support case.
    /// </summary>
    /// <param name="service">Service to use for the new case.</param>
    /// <param name="category">Category to use for the new case.</param>
    /// <param name="severity">Severity to use for the new case.</param>
    /// <returns>The caseId of the new support case.</returns>
    private static async Task<string> CreateSupportCase(Service service,
        Category category, SeverityLevel severity)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"4. Create an example support case" +
                          $" with the following settings:" +
                          $" \n\tService: {service.Name}, Category: {category.Name}
" +
                          $"and Severity Level: {severity.Name}.");
        var caseId = await _supportWrapper.CreateCase(service.Code, category.Code,
severity.Code,
            "Example case for testing, ignore.", "This is my example support
case.");

        Console.WriteLine($"\tNew case created with ID {caseId}");

        Console.WriteLine(new string('-', 80));

        return caseId;
    }

    /// <summary>
    /// List open cases for the current day.
    /// </summary>
    /// <returns>Async task.</returns>
    private static async Task DescribeTodayOpenCases()
    {
        Console.WriteLine($"5. List the open support cases for the current day.");
        // Describe the cases. If it is empty, try again and allow time for the new
case to appear.
        List<CaseDetails> currentOpenCases = null!;
        while (currentOpenCases == null || currentOpenCases.Count == 0)
        {
            Thread.Sleep(1000);
            currentOpenCases = await _supportWrapper.DescribeCases(
                new List<string>(),
                null,
                false,
                false,
                DateTime.UtcNow.Date,
                DateTime.UtcNow);
        }

        foreach (var openCase in currentOpenCases)
        {
            Console.WriteLine($"\tCase: {openCase.CaseId} created
{openCase.TimeCreated}");
        }

        Console.WriteLine(new string('-', 80));
    }
```

```
    /// <summary>
    /// Create an attachment set for a support case.
    /// </summary>
    /// <returns>The attachment set id.</returns>
    private static async Task<string> CreateAttachmentSet()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"6. Create an attachment set for a support case.");
        var fileName = "example_attachment.txt";

        // Create the file if it does not already exist.
        if (!File.Exists(fileName))
        {
            await using StreamWriter sw = File.CreateText(fileName);
            await sw.WriteLineAsync(
                "This is a sample file for attachment to a support case.");
        }

        await using var ms = new MemoryStream(await
 File.ReadAllBytesAsync(fileName));

        var attachmentSetId = await _supportWrapper.AddAttachmentToSet(
            ms,
            fileName);

        Console.WriteLine($"\tNew attachment set created with id: \n
\t{attachmentSetId.Substring(0, 65)}...");

        Console.WriteLine(new string('-', 80));

        return attachmentSetId;
    }

    /// <summary>
    /// Add an attachment set and communication to a case.
    /// </summary>
    /// <param name="attachmentSetId">Id of the attachment set.</param>
    /// <param name="caseId">Id of the case to receive the attachment set.</param>
    /// <returns>Async task.</returns>
    private static async Task AddCommunicationToCase(string attachmentSetId, string
 caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"7. Add attachment set and communication to {caseId}.");

        await _supportWrapper.AddCommunicationToCase(
            caseId,
            "This is an example communication added to a support case.",
            attachmentSetId);

        Console.WriteLine($"\tNew attachment set and communication added to
 {caseId}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List the communications for a case.
    /// </summary>
    /// <param name="caseId">Id of the case to describe.</param>
    /// <returns>An attachment id.</returns>
    private static async Task<string> ListCommunicationsForCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"8. List communications for case {caseId}.");
```

```
        var communications = await _supportWrapper.DescribeCommunications(caseId);
        var attachmentId = "";
        foreach (var communication in communications)
        {
            Console.WriteLine(
                $"\tCommunication created on: {communication.TimeCreated} has
{communication.AttachmentSet.Count} attachments.");
            if (communication.AttachmentSet.Any())
            {
                attachmentId = communication.AttachmentSet.First().AttachmentId;
            }
        }

        Console.WriteLine(new string('-', 80));
        return attachmentId;
    }

    /// <summary>
    /// Describe an attachment by id.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment to describe.</param>
    /// <returns>Async task.</returns>
    private static async Task DescribeCaseAttachment(string attachmentId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"9. Describe the attachment set.");

        var attachment = await _supportWrapper.DescribeAttachment(attachmentId);
        var data = Encoding.ASCII.GetString(attachment.Data.ToArray());
        Console.WriteLine($"\tAttachment includes {attachment.FileName} with data:
\n\t{data}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// Resolve the support case.
    /// </summary>
    /// <param name="caseId">Id of the case to resolve.</param>
    /// <returns>Async task.</returns>
    private static async Task ResolveCase(string caseId)
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"10. Resolve case {caseId}.");

        var status = await _supportWrapper.ResolveCase(caseId);
        Console.WriteLine($"\tCase {caseId} has final status {status}");

        Console.WriteLine(new string('-', 80));
    }

    /// <summary>
    /// List resolved cases for the current day.
    /// </summary>
    /// <returns>Async Task.</returns>
    private static async Task DescribeTodayResolvedCases()
    {
        Console.WriteLine(new string('-', 80));
        Console.WriteLine($"11. List the resolved support cases for the current
day.");
        var currentCases = await _supportWrapper.DescribeCases(
            new List<string>(),
            null,
            false,
            true,
            DateTime.UtcNow.Date,
```

```
            DateTime.UtcNow);

        foreach (var currentCase in currentCases)
        {
            if (currentCase.Status == "resolved")
            {
                Console.WriteLine(
                    $"\tCase: {currentCase.CaseId}: status {currentCase.Status}");
            }
        }

        Console.WriteLine(new string('-', 80));
    }
}
```

场景用于 AWS Support 操作的包装程序方法。

```
/// <summary>
/// Wrapper methods to use AWS Support for working with support cases.
/// </summary>
public class SupportWrapper
{
    private readonly IAmazonAWSSupport _amazonSupport;
    public SupportWrapper(IAmazonAWSSupport amazonSupport)
    {
        _amazonSupport = amazonSupport;
    }


    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <returns>The list of AWS service descriptions.</returns>
    public async Task<List<Service>> DescribeServices(string language = "en")
    {
        var response = await _amazonSupport.DescribeServicesAsync(
            new DescribeServicesRequest()
            {
                Language = language
            });
        return response.Services;
    }



    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <returns>The list of support severity levels.</returns>
    public async Task<List<SeverityLevel>> DescribeSeverityLevels(string language =
 "en")
    {
        var response = await _amazonSupport.DescribeSeverityLevelsAsync(
            new DescribeSeverityLevelsRequest()
            {
                Language = language
            });
        return response.SeverityLevels;
    }
```

```
   /// <summary>
   /// Create a new support case.
   /// </summary>
   /// <param name="serviceCode">Service code for the new case.</param>
   /// <param name="categoryCode">Category for the new case.</param>
   /// <param name="severityCode">Severity code for the new case.</param>
   /// <param name="subject">Subject of the new case.</param>
   /// <param name="body">Body text of the new case.</param>
   /// <param name="language">Optional language support for your case.
   /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
   /// <param name="attachmentSetId">Optional Id for an attachment set for the new
case.</param>
   /// <param name="issueType">Optional issue type for the new case. Options are
"customer-service" or "technical".</param>
   /// <returns>The caseId of the new support case.</returns>
   public async Task<string> CreateCase(string serviceCode, string categoryCode,
string severityCode, string subject,
       string body, string language = "en", string? attachmentSetId = null, string
issueType = "customer-service")
   {
       var response = await _amazonSupport.CreateCaseAsync(
           new CreateCaseRequest()
           {
               ServiceCode = serviceCode,
               CategoryCode = categoryCode,
               SeverityCode = severityCode,
               Subject = subject,
               Language = language,
               AttachmentSetId = attachmentSetId,
               IssueType = issueType,
               CommunicationBody = body
           });
       return response.CaseId;
   }



   /// <summary>
   /// Add an attachment to a set, or create a new attachment set if one does not
exist.
   /// </summary>
   /// <param name="data">The data for the attachment.</param>
   /// <param name="fileName">The file name for the attachment.</param>
   /// <param name="attachmentSetId">Optional setId for the attachment. Creates a
new attachment set if empty.</param>
   /// <returns>The setId of the attachment.</returns>
   public async Task<string> AddAttachmentToSet(MemoryStream data, string
fileName, string? attachmentSetId = null)
   {
       var response = await _amazonSupport.AddAttachmentsToSetAsync(
           new AddAttachmentsToSetRequest
           {
               AttachmentSetId = attachmentSetId,
               Attachments = new List<Attachment>
               {
                   new Attachment
                   {
                       Data = data,
                       FileName = fileName
                   }
               }
           });
       return response.AttachmentSetId;
```

```
    }



    /// <summary>
    /// Get description of a specific attachment.
    /// </summary>
    /// <param name="attachmentId">Id of the attachment, usually fetched by
 describing the communications of a case.</param>
    /// <returns>The attachment object.</returns>
    public async Task<Attachment> DescribeAttachment(string attachmentId)
    {
        var response = await _amazonSupport.DescribeAttachmentAsync(
            new DescribeAttachmentRequest()
            {
                AttachmentId = attachmentId
            });
        return response.Attachment;
    }



    /// <summary>
    /// Add communication to a case, including optional attachment set ID and CC
 email addresses.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <param name="body">Body text of the communication.</param>
    /// <param name="attachmentSetId">Optional Id for an attachment set.</param>
    /// <param name="ccEmailAddresses">Optional list of CC email addresses.</param>
    /// <returns>True if successful.</returns>
    public async Task<bool> AddCommunicationToCase(string caseId, string body,
        string? attachmentSetId = null, List<string>? ccEmailAddresses = null)
    {
        var response = await _amazonSupport.AddCommunicationToCaseAsync(
            new AddCommunicationToCaseRequest()
            {
                CaseId = caseId,
                CommunicationBody = body,
                AttachmentSetId = attachmentSetId,
                CcEmailAddresses = ccEmailAddresses
            });
        return response.Result;
    }



    /// <summary>
    /// Describe the communications for a case, optionally with a date filter.
    /// </summary>
    /// <param name="caseId">The ID of the support case.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <returns>The list of communications for the case.</returns>
    public async Task<List<Communication>> DescribeCommunications(string caseId,
 DateTime? afterTime = null, DateTime? beforeTime = null)
    {
        var results = new List<Communication>();
        var paginateCommunications =
_amazonSupport.Paginators.DescribeCommunications(
            new DescribeCommunicationsRequest()
            {
                CaseId = caseId,
                AfterTime = afterTime?.ToString("s"),
```

```
                BeforeTime = beforeTime?.ToString("s")
            });
        // Get the entire list using the paginator.
        await foreach (var communications in paginateCommunications.Communications)
        {
            results.Add(communications);
        }
        return results;
    }



    /// <summary>
    /// Get case details for a list of case ids, optionally with date filters.
    /// </summary>
    /// <param name="caseIds">The list of case IDs.</param>
    /// <param name="displayId">Optional display ID.</param>
    /// <param name="includeCommunication">True to include communication. Defaults
 to true.</param>
    /// <param name="includeResolvedCases">True to include resolved cases. Defaults
 to false.</param>
    /// <param name="afterTime">The optional start date for a filtered search.</
param>
    /// <param name="beforeTime">The optional end date for a filtered search.</
param>
    /// <param name="language">Optional language support for your case.
    /// Currently "en" (English) and "ja" (Japanese) are supported.</param>
    /// <returns>A list of CaseDetails.</returns>
    public async Task<List<CaseDetails>> DescribeCases(List<string> caseIds,
 string? displayId = null, bool includeCommunication = true,
        bool includeResolvedCases = false, DateTime? afterTime = null, DateTime?
 beforeTime = null,
        string language = "en")
    {
        var results = new List<CaseDetails>();
        var paginateCases = _amazonSupport.Paginators.DescribeCases(
            new DescribeCasesRequest()
            {
                CaseIdList = caseIds,
                DisplayId = displayId,
                IncludeCommunications = includeCommunication,
                IncludeResolvedCases = includeResolvedCases,
                AfterTime = afterTime?.ToString("s"),
                BeforeTime = beforeTime?.ToString("s"),
                Language = language
            });
        // Get the entire list using the paginator.
        await foreach (var cases in paginateCases.Cases)
        {
            results.Add(cases);
        }
        return results;
    }



    /// <summary>
    /// Resolve a support case by caseId.
    /// </summary>
    /// <param name="caseId">Id for the support case.</param>
    /// <returns>The final status of the case after resolving.</returns>
    public async Task<string> ResolveCase(string caseId)
    {
        var response = await _amazonSupport.ResolveCaseAsync(
            new ResolveCaseRequest()
            {
```

```
                CaseId = caseId
            });
        return response.FinalCaseStatus;
    }


    /// <summary>
    /// Verify the support level for AWS Support API access.
    /// </summary>
    /// <returns>True if the subscription level supports API access.</returns>
    public async Task<bool> VerifySubscription()
    {
        try
        {
            var response = await _amazonSupport.DescribeServicesAsync(
                new DescribeServicesRequest()
                {
                    Language = "en"
                });
            return response.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (Amazon.AWSSupport.AmazonAWSSupportException ex)
        {
            if (ex.ErrorCode == "SubscriptionRequiredException")
            {
                return false;
            }
            else throw;
        }
    }
}
```

- 有关 API 详细信息，请参阅《AWS SDK for .NET API 参考》中的以下主题。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Java

SDK for Java 2.x

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

运行各种 AWS Support 操作。

```
/**
 * Before running this Java (v2) code example, set up your development environment,
 including your credentials.
 *
 * For more information, see the following documentation topic:
 *
```

```
 * https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
 *
 *  In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:
 *
 *  https://aws.amazon.com/premiumsupport/plans/
 *
 *  This Java example performs the following tasks:
 *
 * 1. Gets and displays available services.
 * 2. Gets and displays severity levels.
 * 3. Creates a support case by using the selected service, category, and severity
 level.
 * 4. Gets a list of open cases for the current day.
 * 5. Creates an attachment set with a generated file.
 * 6. Adds a communication with the attachment to the support case.
 * 7. Lists the communications of the support case.
 * 8. Describes the attachment set included with the communication.
 * 9. Resolves the support case.
 * 10. Gets a list of resolved cases for the current day.
 */
public class SupportScenario {

    public static final String DASHES = new String(new char[80]).replace("\0",
 "-");
    public static void main(String[] args) {
        final String usage = "\n" +
            "Usage:\n" +
            "    <fileAttachment>" +
            "Where:\n" +
            "    fileAttachment - The file can be a simple saved .txt file to use
 as an email attachment. \n";

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

        String fileAttachment = args[0];
        Region region = Region.US_WEST_2;
        SupportClient supportClient = SupportClient.builder()
            .region(region)
            .build();

        System.out.println(DASHES);
        System.out.println("***** Welcome to the AWS Support case example
 scenario.");
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("1. Get and display available services.");
        List<String> sevCatList = displayServices(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("2. Get and display Support severity levels.");
        String sevLevel = displaySevLevels(supportClient);
        System.out.println(DASHES);

        System.out.println(DASHES);
        System.out.println("3. Create a support case using the selected service,
 category, and severity level.");
        String caseId = createSupportCase(supportClient, sevCatList, sevLevel);
        if (caseId.compareTo("")==0) {
            System.out.println("A support case was not successfully created!");
            System.exit(1);
```

```
       } else
           System.out.println("Support case "+caseId +" was successfully
created!");
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("4. Get open support cases.");
       getOpenCase(supportClient);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("5. Create an attachment set with a generated file to
add to the case.");
       String attachmentSetId = addAttachment(supportClient, fileAttachment);
       System.out.println("The Attachment Set id value is" +attachmentSetId);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("6. Add communication with the attachment to the support
case.");
       addAttachSupportCase(supportClient, caseId, attachmentSetId);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("7. List the communications of the support case.");
       String attachId = listCommunications(supportClient, caseId);
       System.out.println("The Attachment id value is" +attachId);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("8. Describe the attachment set included with the
communication.");
       describeAttachment(supportClient, attachId);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("9. Resolve the support case.");
       resolveSupportCase(supportClient, caseId);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("10. Get a list of resolved cases for the current
day.");
       getResolvedCase(supportClient);
       System.out.println(DASHES);

       System.out.println(DASHES);
       System.out.println("***** This Scenario has successfully completed");
       System.out.println(DASHES);
   }

   public static void getResolvedCase(SupportClient supportClient) {
       try {
           // Specify the start and end time.
           Instant now = Instant.now();
           java.time.LocalDate.now();
           Instant yesterday = now.minus(1, ChronoUnit.DAYS);

           DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                .maxResults(30)
                .afterTime(yesterday.toString())
                .beforeTime(now.toString())
                .includeResolvedCases(true)
                .build();
```

```
            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase: cases) {
                if (sinCase.status().compareTo("resolved") ==0)
                    System.out.println("The case status is "+sinCase.status());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void resolveSupportCase(SupportClient supportClient, String
caseId) {
        try {
            ResolveCaseRequest caseRequest = ResolveCaseRequest.builder()
                .caseId(caseId)
                .build();

            ResolveCaseResponse response = supportClient.resolveCase(caseRequest);
            System.out.println("The status of case "+caseId +" is
"+response.finalCaseStatus());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static void describeAttachment(SupportClient supportClient,String
attachId) {
        try {
            DescribeAttachmentRequest attachmentRequest =
DescribeAttachmentRequest.builder()
                .attachmentId(attachId)
                .build();

            DescribeAttachmentResponse response =
supportClient.describeAttachment(attachmentRequest);
            System.out.println("The name of the file is
"+response.attachment().fileName());

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String listCommunications(SupportClient supportClient, String
caseId) {
        try {
            String attachId = null;
            DescribeCommunicationsRequest communicationsRequest =
DescribeCommunicationsRequest.builder()
                .caseId(caseId)
                .maxResults(10)
                .build();

            DescribeCommunicationsResponse response =
supportClient.describeCommunications(communicationsRequest);
            List<Communication> communications = response.communications();
            for (Communication comm: communications) {
                System.out.println("the body is: " + comm.body());
```

```
                //Get the attachment id value.
                List<AttachmentDetails> attachments = comm.attachmentSet();
                for (AttachmentDetails detail : attachments) {
                    attachId = detail.attachmentId();
                }
            }
            return attachId;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static void addAttachSupportCase(SupportClient supportClient, String
caseId, String attachmentSetId) {
        try {
            AddCommunicationToCaseRequest caseRequest =
AddCommunicationToCaseRequest.builder()
                .caseId(caseId)
                .attachmentSetId(attachmentSetId)
                .communicationBody("Please refer to attachment for details.")
                .build();

            AddCommunicationToCaseResponse response =
supportClient.addCommunicationToCase(caseRequest);
            if (response.result())
                System.out.println("You have successfully added a communication to
an AWS Support case");
            else
                System.out.println("There was an error adding the communication to
an AWS Support case");

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String addAttachment(SupportClient supportClient, String
fileAttachment) {
        try {
            File myFile = new File(fileAttachment);
            InputStream sourceStream = new FileInputStream(myFile);
            SdkBytes sourceBytes = SdkBytes.fromInputStream(sourceStream);

            Attachment attachment = Attachment.builder()
                .fileName(myFile.getName())
                .data(sourceBytes)
                .build();

            AddAttachmentsToSetRequest setRequest =
AddAttachmentsToSetRequest.builder()
                .attachments(attachment)
                .build();

            AddAttachmentsToSetResponse response =
supportClient.addAttachmentsToSet(setRequest);
            return response.attachmentSetId();

        } catch (SupportException | FileNotFoundException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
```

```
    }

    public static void getOpenCase(SupportClient supportClient) {
        try {
            // Specify the start and end time.
            Instant now = Instant.now();
            java.time.LocalDate.now();
            Instant yesterday = now.minus(1, ChronoUnit.DAYS);

            DescribeCasesRequest describeCasesRequest =
DescribeCasesRequest.builder()
                .maxResults(20)
                .afterTime(yesterday.toString())
                .beforeTime(now.toString())
                .build();

            DescribeCasesResponse response =
supportClient.describeCases(describeCasesRequest);
            List<CaseDetails> cases = response.cases();
            for (CaseDetails sinCase: cases) {
                System.out.println("The case status is "+sinCase.status());
                System.out.println("The case Id is "+sinCase.caseId());
                System.out.println("The case subject is "+sinCase.subject());
            }

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
    }

    public static String createSupportCase(SupportClient supportClient,
List<String> sevCatList, String sevLevel) {
        try {
            String serviceCode = sevCatList.get(0);
            String caseCat = sevCatList.get(1);
            CreateCaseRequest caseRequest = CreateCaseRequest.builder()
                .categoryCode(caseCat.toLowerCase())
                .serviceCode(serviceCode.toLowerCase())
                .severityCode(sevLevel.toLowerCase())
                .communicationBody("Test issue with "+serviceCode.toLowerCase())
                .subject("Test case, please ignore")
                .language("en")
                .issueType("technical")
                .build();

            CreateCaseResponse response = supportClient.createCase(caseRequest);
            return response.caseId();

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    public static String displaySevLevels(SupportClient supportClient) {
        try {
            DescribeSeverityLevelsRequest severityLevelsRequest =
DescribeSeverityLevelsRequest.builder()
                .language("en")
                .build();

            DescribeSeverityLevelsResponse response =
supportClient.describeSeverityLevels(severityLevelsRequest);
            List<SeverityLevel> severityLevels = response.severityLevels();
```

```
            String levelName = null;
            for (SeverityLevel sevLevel: severityLevels) {
                System.out.println("The severity level name is: "+
 sevLevel.name());
                if (sevLevel.name().compareTo("High")==0)
                    levelName = sevLevel.name();
            }
            return levelName;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return "";
    }

    // Return a List that contains a Service name and Category name.
    public static List<String> displayServices(SupportClient supportClient) {
        try {
            DescribeServicesRequest servicesRequest =
 DescribeServicesRequest.builder()
                .language("en")
                .build();

            DescribeServicesResponse response =
 supportClient.describeServices(servicesRequest);
            String serviceCode = null;
            String catName = null;
            List<String> sevCatList = new ArrayList<>();
            List<Service> services = response.services();

            System.out.println("Get the first 10 services");
            int index = 1;
            for (Service service: services) {
                if (index== 11)
                    break;

                System.out.println("The Service name is: "+service.name());
                if (service.name().compareTo("Account") == 0)
                    serviceCode = service.code();

                // Get the Categories for this service.
                List<Category> categories = service.categories();
                for (Category cat: categories) {
                    System.out.println("The category name is: "+cat.name());
                    if (cat.name().compareTo("Security") == 0)
                        catName = cat.name();
                }
             index++ ;
            }

            // Push the two values to the list.
            sevCatList.add(serviceCode);
            sevCatList.add(catName);
            return sevCatList;

        } catch (SupportException e) {
            System.out.println(e.getLocalizedMessage());
            System.exit(1);
        }
        return null;
    }
}
```

- 有关 API 详细信息，请参阅《AWS SDK for Java 2.x API 参考》中的以下主题。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

JavaScript

SDK fo JavaScript r (v3)

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

在终端中运行交互式场景。

```
import {
  AddAttachmentsToSetCommand,
  AddCommunicationToCaseCommand,
  CreateCaseCommand,
  DescribeAttachmentCommand,
  DescribeCasesCommand,
  DescribeCommunicationsCommand,
  DescribeServicesCommand,
  DescribeSeverityLevelsCommand,
  ResolveCaseCommand,
  SupportClient,
} from "@aws-sdk/client-support";
import inquirer from "inquirer";

// Retry an asynchronous function on failure.
const retry = async ({ intervalInMs = 500, maxRetries = 10 }, fn) => {
  try {
    return await fn();
  } catch (err) {
    console.log(`Function call failed. Retrying.`);
    console.error(err.message);
    if (maxRetries === 0) throw err;
    await new Promise((resolve) => setTimeout(resolve, intervalInMs));
    return retry({ intervalInMs, maxRetries: maxRetries - 1 }, fn);
  }
};

const wrapText = (text, char = "=") => {
  const rule = char.repeat(80);
  return `${rule}\n    ${text}\n${rule}\n`;
};

const client = new SupportClient({ region: "us-east-1" });

// Verify that the account has a Support plan.
export const verifyAccount = async () => {
  const command = new DescribeServicesCommand({});

  try {
```

```
    await client.send(command);
  } catch (err) {
    if (err.name === "SubscriptionRequiredException") {
      throw new Error(
        "You must be subscribed to the AWS Support plan to use this feature."
      );
    } else {
      throw err;
    }
  }
};

// Get the list of available services.
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const { selectedService } = await inquirer.prompt({
    name: "selectedService",
    type: "list",
    message:
      "Select a service. Your support case will be created for this service. The
 list of services is truncated for readability.",
    choices: services.slice(0, 10).map((s) => ({ name: s.name, value: s })),
  });
  return selectedService;
};

// Get the list of available support case categories for a service.
export const getCategory = async (service) => {
  const { selectedCategory } = await inquirer.prompt({
    name: "selectedCategory",
    type: "list",
    message: "Select a category.",
    choices: service.categories.map((c) => ({ name: c.name, value: c })),
  });
  return selectedCategory;
};

// Get the available severity levels for the account.
export const getSeverityLevel = async () => {
  const command = new DescribeSeverityLevelsCommand({});
  const { severityLevels } = await client.send(command);
  const { selectedSeverityLevel } = await inquirer.prompt({
    name: "selectedSeverityLevel",
    type: "list",
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

// Create a new support case and return the caseId.
export const createCase = async ({
  selectedService,
  selectedCategory,
  selectedSeverityLevel,
}) => {
  const command = new CreateCaseCommand({
    subject: "IGNORE: Test case",
    communicationBody: "This is a test. Please ignore.",
    serviceCode: selectedService.code,
    categoryCode: selectedCategory.code,
    severityCode: selectedSeverityLevel.code,
  });
  const { caseId } = await client.send(command);
  return caseId;
};
```

```
// Get a list of open support cases created today.
export const getTodaysOpenCases = async () => {
  const d = new Date();
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
  });

  const { cases } = await client.send(command);

  if (cases.length === 0) {
    throw new Error(
      "Unexpected number of cases. Expected more than 0 open cases."
    );
  }
  return cases;
};

// Create an attachment set.
export const createAttachmentSet = async () => {
  const command = new AddAttachmentsToSetCommand({
    attachments: [
      {
        fileName: "example.txt",
        data: new TextEncoder().encode("some example text"),
      },
    ],
  });
  const { attachmentSetId } = await client.send(command);
  return attachmentSetId;
};

export const linkAttachmentSetToCase = async (attachmentSetId, caseId) => {
  const command = new AddCommunicationToCaseCommand({
    attachmentSetId,
    caseId,
    communicationBody: "Adding attachment set to case.",
  });
  await client.send(command);
};

// Get all communications for a support case.
export const getCommunications = async (caseId) => {
  const command = new DescribeCommunicationsCommand({
    caseId,
  });
  const { communications } = await client.send(command);
  return communications;
};

// Get an attachment set.
export const getFirstAttachment = (communications) => {
  const firstCommWithAttachment = communications.find(
    (c) => c.attachmentSet.length > 0
  );
  return firstCommWithAttachment?.attachmentSet[0].attachmentId;
};

// Get an attachment.
export const getAttachment = async (attachmentId) => {
  const command = new DescribeAttachmentCommand({
    attachmentId,
  });
  const { attachment } = await client.send(command);
```

```
  return attachment;
};

// Resolve the case matching the given case ID.
export const resolveCase = async (caseId) => {
  const { shouldResolve } = await inquirer.prompt({
    name: "shouldResolve",
    type: "confirm",
    message: `Do you want to resolve ${caseId}?`,
  });

  if (shouldResolve) {
    const command = new ResolveCaseCommand({
      caseId: caseId,
    });

    await client.send(command);
    return true;
  }
  return false;
};

// Find a specific case in the list of provided cases by case ID.
// If the case is not found, and the results are paginated, continue
// paging through the results.
export const findCase = async ({ caseId, cases, nextToken }) => {
  const foundCase = cases.find((c) => c.caseId === caseId);

  if (foundCase) {
    return foundCase;
  }

  if (nextToken) {
    const response = await client.send(
      new DescribeCasesCommand({
        nextToken,
        includeResolvedCases: true,
      })
    );
    return findCase({
      caseId,
      cases: response.cases,
      nextToken: response.nextToken,
    });
  }

  throw new Error(`${caseId} not found.`);
};

// Get all cases created today.
export const getTodaysResolvedCases = async (caseIdToWaitFor) => {
  const d = new Date("2023-01-18");
  const startOfToday = new Date(d.getFullYear(), d.getMonth(), d.getDate());
  const command = new DescribeCasesCommand({
    includeCommunications: false,
    afterTime: startOfToday.toISOString(),
    includeResolvedCases: true,
  });
  const { cases, nextToken } = await client.send(command);
  await findCase({ cases, caseId: caseIdToWaitFor, nextToken });
  return cases.filter((c) => c.status === "resolved");
};

const main = async () => {
  let caseId;
  try {
```

```
   console.log(wrapText("Welcome to the AWS Support basic usage scenario."));

   // Verify that the account is subscribed to support.
   await verifyAccount();

   // Provided a truncated list of services and prompt the user to select one.
   const selectedService = await getService();

   // Provided the categories for the selected service and prompt the user to
select one.
   const selectedCategory = await getCategory(selectedService);

   // Provide the severity available severity levels for the account and prompt
the user to select one.
   const selectedSeverityLevel = await getSeverityLevel();

   // Create a support case.
   console.log("\nCreating a support case.");
   caseId = await createCase({
     selectedService,
     selectedCategory,
     selectedSeverityLevel,
   });
   console.log(`Support case created: ${caseId}`);

   // Display a list of open support cases created today.
   const todaysOpenCases = await retry(
     { intervalInMs: 1000, maxRetries: 15 },
     getTodaysOpenCases
   );
   console.log(
     `\nOpen support cases created today: ${todaysOpenCases.length}`
   );
   console.log(todaysOpenCases.map((c) => `${c.caseId}`).join("\n"));

   // Create an attachment set.
   console.log("\nCreating an attachment set.");
   const attachmentSetId = await createAttachmentSet();
   console.log(`Attachment set created: ${attachmentSetId}`);

   // Add the attachment set to the support case.
   console.log(`\nAdding attachment set to ${caseId}`);
   await linkAttachmentSetToCase(attachmentSetId, caseId);
   console.log(`Attachment set added to ${caseId}`);

   // List the communications for a support case.
   console.log(`\nListing communications for ${caseId}`);
   const communications = await getCommunications(caseId);
   console.log(
     communications
       .map(
         (c) =>
           `Communication created on ${c.timeCreated}. Has
${c.attachmentSet.length} attachments.`
       )
       .join("\n")
   );

   // Describe the first attachment.
   console.log(`\nDescribing attachment ${attachmentSetId}`);
   const attachmentId = getFirstAttachment(communications);
   const attachment = await getAttachment(attachmentId);
   console.log(
     `Attachment is the file '${
       attachment.fileName
     }' with data: \n${new TextDecoder().decode(attachment.data)}`
```

```
    );

    // Confirm that the support case should be resolved.
    const isResolved = await resolveCase(caseId);
    if (isResolved) {
      // List the resolved cases and include the one previously created.
      // Resolved cases can take a while to appear.
      console.log(
        "\nWaiting for case status to be marked as resolved. This can take some
 time."
      );
      const resolvedCases = await retry(
        { intervalInMs: 20000, maxRetries: 15 },
        () => getTodaysResolvedCases(caseId)
      );
      console.log("Resolved cases:");
      console.log(resolvedCases.map((c) => c.caseId).join("\n"));
    }
  } catch (err) {
    console.error(err);
  }
};
```

- 有关 API 详细信息，请参阅《AWS SDK for JavaScript API 参考》中的以下主题。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Kotlin

SDK for Kotlin

Note

这是适用于预览版中功能的预发行文档。本文档随时可能更改。

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

```
/**
Before running this Kotlin code example, set up your development environment,
including your credentials.

For more information, see the following documentation topic:

https://docs.aws.amazon.com/sdk-for-kotlin/latest/developer-guide/setup.html
In addition, you must have the AWS Business Support Plan to use the AWS Support
 Java API. For more information, see:

https://aws.amazon.com/premiumsupport/plans/

This Kotlin example performs the following tasks:
```

```
1. Gets and displays available services.
2. Gets and displays severity levels.
3. Creates a support case by using the selected service, category, and severity
 level.
4. Gets a list of open cases for the current day.
5. Creates an attachment set with a generated file.
6. Adds a communication with the attachment to the support case.
7. Lists the communications of the support case.
8. Describes the attachment set included with the communication.
9. Resolves the support case.
10. Gets a list of resolved cases for the current day.
*/

suspend fun main(args: Array<String>) {
    val usage = """
    Usage:
        <fileAttachment>
    Where:
         fileAttachment - The file can be a simple saved .txt file to use as an
 email attachment.
    """

    if (args.size != 1) {
        println(usage)
        exitProcess(0)
    }

    val fileAttachment = args[0]
    println("***** Welcome to the AWS Support case example scenario.")
    println("***** Step 1. Get and display available services.")
    val sevCatList = displayServices()

    println("***** Step 2. Get and display Support severity levels.")
    val sevLevel = displaySevLevels()

    println("***** Step 3. Create a support case using the selected service,
 category, and severity level.")
    val caseIdVal = createSupportCase(sevCatList, sevLevel)
    if (caseIdVal != null) {
        println("Support case $caseIdVal was successfully created!")
    } else {
        println("A support case was not successfully created!")
        exitProcess(1)
    }

    println("***** Step 4. Get open support cases.")
    getOpenCase()

    println("***** Step 5. Create an attachment set with a generated file to add to
 the case.")
    val attachmentSetId = addAttachment(fileAttachment)
    println("The Attachment Set id value is $attachmentSetId")

    println("***** Step 6. Add communication with the attachment to the support
 case.")
    addAttachSupportCase(caseIdVal, attachmentSetId)

    println("***** Step 7. List the communications of the support case.")
    val attachId = listCommunications(caseIdVal)
    println("The Attachment id value is $attachId")

    println("***** Step 8. Describe the attachment set included with the
 communication.")
    describeAttachment(attachId)

    println("***** Step 9. Resolve the support case.")
```

```
    resolveSupportCase(caseIdVal)

    println("***** Step 10. Get a list of resolved cases for the current day.")
    getResolvedCase()
    println("***** This Scenario has successfully completed")
}

suspend fun getResolvedCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 30
        afterTime = yesterday.toString()
        beforeTime = now.toString()
        includeResolvedCases = true
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest = ResolveCaseRequest {
        caseId = caseIdVal
    }
    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}

suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest = DescribeAttachmentRequest {
        attachmentId = attachId
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}

suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest = DescribeCommunicationsRequest {
        caseId = caseIdVal
        maxResults = 10
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCommunications(communicationsRequest)
        response.communications?.forEach { comm ->
            println("the body is: " + comm.body)
            comm.attachmentSet?.forEach { detail ->
                return detail.attachmentId
            }
        }
    }
    return ""
```

```
}

suspend fun addAttachSupportCase(caseIdVal: String?, attachmentSetIdVal: String?) {
    val caseRequest = AddCommunicationToCaseRequest {
        caseId = caseIdVal
        attachmentSetId = attachmentSetIdVal
        communicationBody = "Please refer to attachment for details."
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addCommunicationToCase(caseRequest)
        if (response.result) {
            println("You have successfully added a communication to an AWS Support
 case")
        } else {
            println("There was an error adding the communication to an AWS Support
 case")
        }
    }
}

suspend fun addAttachment(fileAttachment: String): String? {
    val myFile = File(fileAttachment)
    val sourceBytes = (File(fileAttachment).readBytes())
    val attachmentVal = Attachment {
        fileName = myFile.name
        data = sourceBytes
    }

    val setRequest = AddAttachmentsToSetRequest {
        attachments = listOf(attachmentVal)
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}

suspend fun getOpenCase() {
    // Specify the start and end time.
    val now = Instant.now()
    LocalDate.now()
    val yesterday = now.minus(1, ChronoUnit.DAYS)
    val describeCasesRequest = DescribeCasesRequest {
        maxResults = 20
        afterTime = yesterday.toString()
        beforeTime = now.toString()
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeCases(describeCasesRequest)
        response.cases?.forEach { sinCase ->
            println("The case status is ${sinCase.status}")
            println("The case Id is ${sinCase.caseId}")
            println("The case subject is ${sinCase.subject}")
        }
    }
}

suspend fun createSupportCase(sevCatListVal: List<String>, sevLevelVal: String):
 String? {
    val serCode = sevCatListVal[0]
    val caseCategory = sevCatListVal[1]
    val caseRequest = CreateCaseRequest {
        categoryCode = caseCategory.lowercase(Locale.getDefault())
```

```
        serviceCode = serCode.lowercase(Locale.getDefault())
        severityCode = sevLevelVal.lowercase(Locale.getDefault())
        communicationBody = "Test issue with
 ${serCode.lowercase(Locale.getDefault())}"
        subject = "Test case, please ignore"
        language = "en"
        issueType = "technical"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}

suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest = DescribeSeverityLevelsRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeSeverityLevels(severityLevelsRequest)
        response.severityLevels?.forEach { sevLevel ->
            println("The severity level name is: ${sevLevel.name}")
            if (sevLevel.name == "High") {
                levelName = sevLevel.name!!
            }
        }
        return levelName
    }
}

// Return a List that contains a Service name and Category name.
suspend fun displayServices(): List<String> {
    var serviceCode = ""
    var catName = ""
    val sevCatList = mutableListOf<String>()
    val servicesRequest = DescribeServicesRequest {
        language = "en"
    }

    SupportClient { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeServices(servicesRequest)
        println("Get the first 10 services")
        var index = 1

        response.services?.forEach { service ->
            if (index == 11) {
                return@forEach
            }

            println("The Service name is ${service.name}")
            if (service.name == "Account") {
                serviceCode = service.code.toString()
            }

            // Get the categories for this service.
            service.categories?.forEach { cat ->
                println("The category name is ${cat.name}")
                if (cat.name == "Security") {
                    catName = cat.name!!
                }
            }
            index++
        }
```

```
    }

    // Push the two values to the list.
    serviceCode.let { sevCatList.add(it) }
    catName.let { sevCatList.add(it) }
    return sevCatList
}
```

- 有关 API 详细信息，请参阅《AWS SDK for Kotlin API 参考》中的以下主题。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Python

适用于 Python (Boto3) 的 SDK

Note

还有更多GitHub。查找完整示例，学习如何在 AWS 代码示例存储库中进行设置和运行。

在命令提示符中运行交互式场景。

```
class SupportCasesScenario:
    """Runs an interactive scenario that shows how to get started using AWS
 Support."""

    def __init__(self, support_wrapper):
        """
        :param support_wrapper: An object that wraps AWS Support actions.
        """
        self.support_wrapper = support_wrapper

    def display_and_select_service(self):
        """
        Lists support services and prompts the user to select one.

        :return: The support service selected by the user.
        """
        print('-' * 88)
        services_list = self.support_wrapper.describe_services('en')
        print(f"AWS Support client returned {len(services_list)} services.")
        print("Displaying first 10 services:")

        service_choices = [svc['name'] for svc in services_list[:10]]
        selected_index = q.choose(
            "Select an example support service by entering a number from the
 preceding list:",
            service_choices)
        selected_service = services_list[selected_index]
        print('-' * 88)
        return selected_service
```

```
    def display_and_select_category(self, service):
        """
        Lists categories for a support service and prompts the user to select one.

        :param service: The service of the categories.
        :return: The selected category.
        """
        print('-' * 88)
        print(f"Available support categories for Service {service['name']}
{len(service['categories'])}:")
        categories_choices = [category['name'] for category in
service['categories']]
        selected_index = q.choose(
            "Select an example support category by entering a number from the
preceding list:",
            categories_choices)
        selected_category = service['categories'][selected_index]
        print('-' * 88)
        return selected_category

    def display_and_select_severity(self):
        """
        Lists available severity levels and prompts the user to select one.

        :return: The selected severity level.
        """
        print('-' * 88)
        severity_levels_list = self.support_wrapper.describe_severity_levels('en')
        print(f"Available severity levels:")
        severity_choices = [level['name'] for level in severity_levels_list]
        selected_index = q.choose(
            "Select an example severity level by entering a number from the
preceding list:",
            severity_choices)
        selected_severity = severity_levels_list[selected_index]
        print('-' * 88)
        return selected_severity

    def create_example_case(self, service, category, severity_level):
        """
        Creates an example support case with the user's selections.

        :param service: The service for the new case.
        :param category: The category for the new case.
        :param severity_level: The severity level for the new case.
        :return: The caseId of the new support case.
        """
        print('-' * 88)
        print(f"Creating new case for service {service['name']}.")
        case_id = self.support_wrapper.create_case(service, category,
severity_level)
        print(f"\tNew case created with ID {case_id}.")
        print('-' * 88)
        return case_id

    def list_open_cases(self):
        """
        List the open cases for the current day.
        """
        print('-' * 88)
        print("Let's list the open cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        open_cases = self.support_wrapper.describe_cases(start_time, end_time,
False)
        for case in open_cases:
```

```
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print('-' * 88)

    def create_attachment_set(self):
        """
        Create an attachment set with a sample file.

        :return: The attachment set ID of the new attachment set.
        """
        print('-' * 88)
        print("Creating attachment set with a sample file.")
        attachment_set_id = self.support_wrapper.add_attachment_to_set()
        print(f"\tNew attachment set created with ID {attachment_set_id}.")
        print('-' * 88)
        return attachment_set_id

    def add_communication(self, case_id, attachment_set_id):
        """
        Add a communication with an attachment set to the case.

        :param case_id: The ID of the case for the communication.
        :param attachment_set_id: The ID of the attachment set to
        add to the communication.
        """
        print('-' * 88)
        print(f"Adding a communication and attachment set to the case.")
        self.support_wrapper.add_communication_to_case(attachment_set_id, case_id)
        print(f"Added a communication and attachment set {attachment_set_id} to the
case {case_id}.")
        print('-' * 88)

    def list_communications(self, case_id):
        """
        List the communications associated with a case.

        :param case_id: The ID of the case.
        :return: The attachment ID of an attachment.
        """
        print('-' * 88)
        print("Let's list the communications for our case.")
        attachment_id = ''
        communications =
self.support_wrapper.describe_all_case_communications(case_id)
        for communication in communications:
            print(f"\tCommunication created on {communication['timeCreated']} "
                  f"has {len(communication['attachmentSet'])} attachments.")
            if len(communication['attachmentSet']) > 0:
                attachment_id = communication['attachmentSet'][0]['attachmentId']
        print('-' * 88)
        return attachment_id

    def describe_case_attachment(self, attachment_id):
        """
        Describe an attachment associated with a case.

        :param attachment_id: The ID of the attachment.
        """
        print('-' * 88)
        print("Let's list the communications for our case.")
        attached_file = self.support_wrapper.describe_attachment(attachment_id)
        print(f"\tAttachment includes file {attached_file}.")
        print('-' * 88)

    def resolve_case(self, case_id):
        """
        Shows how to resolve an AWS Support case by its ID.
```

```
        :param case_id: The ID of the case to resolve.
        """
        print('-' * 88)
        print(f"Resolving case with ID {case_id}.")
        case_status = self.support_wrapper.resolve_case(case_id)
        print(f"\tFinal case status is {case_status}.")
        print('-' * 88)

    def list_resolved_cases(self):
        """
        List the resolved cases for the current day.
        """
        print('-' * 88)
        print("Let's list the resolved cases for the current day.")
        start_time = str(datetime.utcnow().date())
        end_time = str(datetime.utcnow().date() + timedelta(days=1))
        resolved_cases = self.support_wrapper.describe_cases(start_time, end_time,
 True)
        for case in resolved_cases:
            print(f"\tCase: {case['caseId']}: status {case['status']}.")
        print('-' * 88)

    def run_scenario(self):
        logging.basicConfig(level=logging.INFO, format='%(levelname)s:
 %(message)s')

        print('-'*88)
        print("Welcome to the AWS Support get started with support cases demo.")
        print('-'*88)

        selected_service = self.display_and_select_service()
        selected_category = self.display_and_select_category(selected_service)
        selected_severity = self.display_and_select_severity()
        new_case_id = self.create_example_case(selected_service, selected_category,
 selected_severity)
        wait(10)
        self.list_open_cases()
        new_attachment_set_id = self.create_attachment_set()
        self.add_communication(new_case_id, new_attachment_set_id)
        new_attachment_id = self.list_communications(new_case_id)
        self.describe_case_attachment(new_attachment_id)
        self.resolve_case(new_case_id)
        wait(10)
        self.list_resolved_cases()

        print("\nThanks for watching!")
        print('-'*88)


if __name__ == '__main__':
    try:
        scenario = SupportCasesScenario(SupportWrapper.from_client())
        scenario.run_scenario()
    except Exception:
        logging.exception("Something went wrong with the demo.")
```

定义一个sDK for 客户端操作的类。

```
class SupportWrapper:
    """Encapsulates Support actions."""
    def __init__(self, support_client):
        """
        :param support_client: A Boto3 Support client.
```

```
        """
        self.support_client = support_client

    @classmethod
    def from_client(cls):
        """
        Instantiates this class from a Boto3 client.
        """
        support_client = boto3.client('support')
        return cls(support_client)

    def describe_services(self, language):
        """
        Get the descriptions of AWS services available for support for a language.

        :param language: The language for support services.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of AWS service descriptions.
        """
        try:
            response = self.support_client.describe_services(
                language=language)
            services = response['services']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't get Support services for language %s. Here's why: %s:
 %s", language,
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return services

    def describe_severity_levels(self, language):
        """
        Get the descriptions of available severity levels for support cases for a
 language.

        :param language: The language for support severity levels.
        Currently, only "en" (English) and "ja" (Japanese) are supported.
        :return: The list of severity levels.
        """
        try:
            response = self.support_client.describe_severity_levels(
                language=language)
            severity_levels = response['severityLevels']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't get severity levels for language %s. Here's why: %s:
 %s", language,
                    err.response['Error']['Code'], err.response['Error']
['Message'])
```

```
                raise
        else:
            return severity_levels

    def create_case(self, service, category, severity):
        """
        Create a new support case.

        :param service: The service to use for the new case.
        :param category: The category to use for the new case.
        :param severity: The severity to use for the new case.
        :return: The caseId of the new case.
        """
        try:
            response = self.support_client.create_case(
                subject='Example case for testing, ignore.',
                serviceCode=service['code'],
                severityCode=severity['code'],
                categoryCode=category['code'],
                communicationBody='Example support case body.',
                language='en',
                issueType='customer-service'
            )
            case_id = response['caseId']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't create case. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return case_id

    def add_attachment_to_set(self):
        """
        Add an attachment to a set, or create a new attachment set if one does not
 exist.

        :return: The attachment set ID.
        """
        try:
            response = self.support_client.add_attachments_to_set(
                attachments=[
                    {
                        'fileName': 'attachment_file.txt',
                        'data': b"This is a sample file for attachment to a support
 case."
                    }
                ])
            new_set_id = response['attachmentSetId']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
```

```
                    "Couldn't add attachment. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return new_set_id

    def add_communication_to_case(self, attachment_set_id, case_id):
        """
        Add a communication and an attachment set to a case.

        :param attachment_set_id: The ID of an existing attachment set.
        :param case_id: The ID of the case.
        """
        try:
            self.support_client.add_communication_to_case(
                caseId=case_id,
                communicationBody="This is an example communication added to a
 support case.",
                attachmentSetId=attachment_set_id
            )
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't add communication. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise


    def describe_all_case_communications(self, case_id):
        """
        Describe all the communications for a case using a paginator.

        :param case_id: The ID of the case.
        :return: The communications for the case.
        """
        try:
            communications = []
            paginator =
 self.support_client.get_paginator('describe_communications')
            for page in paginator.paginate(caseId=case_id):
                communications += page['communications']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't describe communications. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return communications

    def describe_attachment(self, attachment_id):
```

```
        """
        Get information about an attachment by its attachmentID.

        :param attachment_id: The ID of the attachment.
        :return: The name of the attached file.
        """
        try:
            response = self.support_client.describe_attachment(
                attachmentId=attachment_id
            )
            attached_file = response['attachment']['fileName']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't get attachment description. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return attached_file

    def resolve_case(self, case_id):
        """
        Resolve a support case by its caseId.

        :param case_id: The ID of the case to resolve.
        :return: The final status of the case.
        """
        try:
            response = self.support_client.resolve_case(
                caseId=case_id
                )
            final_status = response['finalCaseStatus']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't resolve case. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            return final_status

    def describe_cases(self, after_time, before_time, resolved):
        """
        Describe support cases over a period of time, optionally filtering
        by status.

        :param after_time: The start time to include for cases.
        :param before_time: The end time to include for cases.
        :param resolved: True to include resolved cases in the results,
            otherwise results are open cases.
        :return: The final status of the case.
        """
```

```
        try:
            cases = []
            paginator = self.support_client.get_paginator('describe_cases')
            for page in paginator.paginate(
                    afterTime=after_time,
                    beforeTime=before_time,
                    includeResolvedCases=resolved,
                    language='en'):
                cases += page['cases']
        except ClientError as err:
            if err.response['Error']['Code'] == 'SubscriptionRequiredException':
                logger.info("You must have a Business, Enterprise On-Ramp, or
 Enterprise Support "
                            "plan to use the AWS Support API. \n\tPlease upgrade
 your subscription to run these "
                            "examples.")
            else:
                logger.error(
                    "Couldn't describe cases. Here's why: %s: %s",
                    err.response['Error']['Code'], err.response['Error']
['Message'])
                raise
        else:
            if resolved:
                cases = filter(lambda case: case['status'] == 'resolved', cases)
            return cases
```

- 有关 API 详细信息，请参阅《AWS SDK for Python (Boto3) API 参考》中的以下主。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

有关 AWS 软件开发工具包开发人员指南和代码示例的完整列表，请参阅 将 AWS Support 与 AWS 开发工具包配合使用 (p. 14)。本主题还包括有关入门的信息以及有关先前的软件开发工具包版本的详细信息。

AWS Support 的监控和日志记录

监控是保持 AWS Support 和您的其他 AWS 解决方案的可靠性、可用性和性能的重要方面。AWS 提供了以下一些监控工具来监控 AWS Support、在出现错误时进行报告并适时自动采取措施。

- Amazon EventBridge 提供近乎实时的系统事件流，这些系统事件流，这些系统事件描述了AWS资源的更改。 EventBridge 支持自动事件驱动型计算，因为您可以编写规则，以监控某些事件和在这些事件发生时在其他AWS服务中触发自动操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。
- AWS CloudTrail 捕获由您的 AWS 账户或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Simple Storage Service（Amazon S3）存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 AWS CloudTrail 用户指南。

主题

- 与亚马逊一起监控AWS Support案例 EventBridge (p. 311)
- 使用 AWS Support 记录 AWS CloudTrail API 调用 (p. 314)
- 使用 AWS CloudTrail 记录 Slack API 调用中的 AWS Support App (p. 316)

与亚马逊一起监控AWS Support案例 EventBridge

您可以使用亚马逊EventBridge来检测和应对AWS Support案例的变化。然后，EventBridge 会根据您创建的规则，在事件与您在规则中指定的值匹配时调用一个或多个目标操作。

根据具体事件，您可以发送通知、捕获事件信息、采取纠正措施、启动事件或采取其他操作。例如，每当您的账户中发生以下操作时，您都可以收到通知：

- 创建支持案例
- 将案例通信添加到现有支持案例
- 解析支持案例
- 重新打开支持案例

> Note
>
> AWS Support 将尽最大效能传送事件。并不总是能保证将事件传送到 EventBridge。

为 AWS Support 案例创建一个 EventBridge 规则

您可以创建 EventBridge 规则，以针对 AWS Support 案例事件获得通知。该规则将监控针对您账户中的支持案例的更新，包括您、您的 IAM 用户或支持代理执行的操作。在为 AWS Support 案例事件创建规则之前，请执行以下操作：

- 熟悉 EventBridge 中的事件、规则和目标。有关更多信息，请参阅什么是亚马逊EventBridge？ 在亚马逊EventBridge用户指南中。
- 创建要在您的事件规则中使用的目标。例如，您可以创建 Amazon Simple Notification Service (Amazon SNS) 主题，以便每当更新支持案例时，您都会收到短信或电子邮件。有关更多信息，请参阅 EventBridge 目标。

> Note
>
> AWS Support 是一项全球性服务。要接收支持案例的更新，您可以使用以下区域之一：美国东部（弗吉尼亚北部）区域、美国西部（俄勒冈）地区或欧洲（爱尔兰）区域。

为 AWS Support 案例事件创建 EventBridge 规则

1. 通过 https://console.aws.amazon.com/events/ 打开亚马逊EventBridge控制台。
2. 如果您尚未这样做，请使用页面的右上角的 Region selector（区域选择器），然后选择 US East (N. Virginia)（美国东部（弗吉尼亚北部））。
3. 在导航窗格中，选择 Rules (规则)。
4. 选择 Create rule (创建规则)。
5. 在 Define rule detail（定义规则详细信息）页面上，输入规则名称和描述。
6. 对于 Event bus（事件总线）和 Rule type（规则类型），保留默认值，然后选择 Next（下一步）。
7. 在 “生成事件模式” 页面上，为 “事件源” 选择 “AWS事件” 或 “EventBridge合作伙伴事件”。
8. 在 Event pattern（事件模式）下，请保留默认值（ AWS 服务）。
9. 对于 AWS 服务，选择 Support。
10. 对于 Event type（事件类型），选择 Support Case Update（支持案例更新）。
11. 选择下一步。
12. 在 Select targets（选择目标）部分中，选择您为此规则创建的目标，然后配置该类型所需的任何其他选项。例如，如果您选择 Amazon SNS，请确保正确配置 SNS 主题，以便通过电子邮件或短信通知您。
13. 选择下一步。
14. （可选）在 Configure tags（配置标签）页面上，添加任意标签，然后选择 Next（下一步）。
15. 在 Review and create（检查并创建）页面上，检查您的规则设置并确保其符合您的事件监控要求。
16. 选择 Create rule（创建规则）。您的规则现在将监控 AWS Support 案例事件，然后将它们发送到您指定的目标。

注意

- 当您收到事件时，可以使用 `origin` 参数来确定是您还是 AWS Support 代理向支持案例添加了案例通信。`origin` 的值可以是 `CUSTOMER` 或 `AWS`。

  目前，仅 `AddCommunicationToCase` 操作的事件将具有此值。
- 有关创建事件模式的更多信息，请参阅《亚马逊EventBridge用户指南》中的事件模式。
- 您也可以通过CloudTrail事件类型为 AWS API 调用创建另一条规则。此规则将监控您的账户中 AWS Support API 调用的 AWS CloudTrail 日志。

示例 AWS Support 事件

当您的账户中发生支持操作时，将创建以下事件。

Example ：创建支持案例

当创建支持案例时，将创建以下事件。

```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
```

```
        "event-name": "CreateCase",
        "origin": ""
    }
}
```

Example ：更新支持案例

当 AWS Support 回复支持案例时，将创建以下事件。

```
{
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```

Example ：解析支持案例

当解析支持案例时，将创建以下事件。

```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
    }
}
```

Example ：重新打开支持案例

当重新打开支持案例时，将创建以下事件。

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
```

```
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

另请参阅

有关如何将 EventBridge 与 AWS Support 配合使用的更多信息，请参阅以下资源：

- 如何使用亚马逊自动化 AWS Support API EventBridge
- AWS Support案例活动通知器已开启 GitHub

使用 AWS Support 记录 AWS CloudTrail API 调用

AWS Support已与AWS CloudTrail集成，此服务提供了中由用户、角色或AWS服务所采取操作的记录AWS Support。 CloudTrail 将的 API 调用AWS Support作为事件捕获。捕获的调用包含来自 AWS Support 控制台和代码的 AWS Support API 操作调用。

如果您创建了跟踪记录，则可以将 CloudTrail 事件持续传送到 Amazon Simple Storage Service (Amazon S3) 存储桶（包括的事件）AWS Support。如果您不配置跟踪记录，则仍可在 Event history（事件历史记录 CloudTrail ）中查看最新事件。

通过使用收集的信息 CloudTrail，您可以确定向发出了什么请求AWS Support、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

要了解 CloudTrail更多信息（包括如何对其进行配置和启用），请参阅 AWS CloudTrailUser Guide。

AWS Support中的信息 CloudTrail

CloudTrail 在您创建AWS账户时，即针对该账户启用了。当中发生受支持的事件活动时，该活动将记录在AWS Support事件历史记录中，并与其他AWS服务 CloudTrail 事件一同保存在 Event history（事件历史记录）中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录 AWS 账户中的事件（包括 AWS Support 的事件），请创建跟踪。通过跟踪 CloudTrail ，可以将日志文件传送至 Amazon S3 桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他AWS服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取操作。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为配置 Amazon SNS 通知 CloudTrail
- 从多个区域接收 CloudTrail 日志文件和从多个账户中接收 CloudTrail 日志文件

AWS SupportAPI 操作均由 API 参考记录 CloudTrail 并保存在 AWS SupportAPI 参考中。

例如，调用`CreateCase`、`DescribeCases`和`ResolveCase`操作会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

您也可以将多个 AWS 区域和多个 AWS 账户的 AWS Support 日志文件聚合到单个 Amazon S3 存储桶中。

CloudTrail 日志记录中的 AWS Trusted Advisor 信息

Trusted Advisor 是一项 AWS Support 服务，您可以用它检查您的 AWS 账户以了解如何节省成本、增强安全性和优化您的账户。

Trusted AdvisorAPI 操作均由 API 参考记录 CloudTrail 并保存在 AWS SupportAPI 参考中。

例如，调用DescribeTrustedAdvisorCheckRefreshStatuses、DescribeTrustedAdvisorCheckResult和RefreshTr作会在 CloudTrail 日志文件中生成条目。

> **Note**
>
> CloudTrail 还记录Trusted Advisor控制台操作。请参阅使用 AWS CloudTrail 记录 AWS Trusted Advisor 控制台操作 (p. 337)。

了解 AWS Support 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件 表示来自任何源的单个请求。它包括有关所请求操作的信息、操作的日期和时间和请求参数等。 CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

Example ：的日志条目 CreateCase

以下示例显示了该CreateCase操作 CloudTrail 的日志条目。


```
{
   "Records": [
      {
         "eventVersion": "1.04",
         "userIdentity": {
            "type": "IAMUser",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::111122223333:user/janedoe",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "janedoe",
            "sessionContext": {
               "attributes": {
                  "mfaAuthenticated": "false",
                  "creationDate": "2016-04-13T17:51:37Z"
               }
            },
            "invokedBy": "signin.amazonaws.com"
         },
         "eventTime": "2016-04-13T18:05:53Z",
         "eventSource": "support.amazonaws.com",
         "eventName": "CreateCase",
         "awsRegion": "us-east-1",
```

```
        "sourceIPAddress": "198.51.100.15",
        "userAgent": "signin.amazonaws.com",
        "requestParameters": {
           "severityCode": "low",
           "categoryCode": "other",
           "language": "en",
           "serviceCode": "support-api",
           "issueType": "technical"
        },
        "responseElements": {
           "caseId": "case-111122223333-muen-2016-c3f2077e504940f2"
        },
        "requestID": "58c257ef-01a2-11e6-be2a-01c031063738",
        "eventID": "5aa34bfc-ad5b-4fb1-8a55-2277c86e746a",
        "eventType": "AwsApiCall",
        "recipientAccountId": "111122223333"
      }
   ],
   ...
}
```

Example ：的日志条目 RefreshTrustedAdvisorCheck

以下示例显示了该RefreshTrustedAdvisorCheck操作 CloudTrail 的日志条目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/Admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Admin"
    },
    "eventTime": "2020-10-21T16:34:13Z",
    "eventSource": "support.amazonaws.com",
    "eventName": "RefreshTrustedAdvisorCheck",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.67",
    "userAgent": "signin.amazonaws.com",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

使用 AWS CloudTrail 记录 Slack API 调用中的 AWS Support App

Slack 中的AWS Support App 已与集成AWS CloudTrail。 CloudTrail 提供用户、角色或AWS Support AppAWS 服务 中的所执行操作的记录。要创建此记录，请将AWS Support App 的所有公有 API 调用 CloudTrail 捕获为事件。这些捕获的调用包含来自 AWS Support App 控制台的调用和代码对 AWS Support App 公有 API 操作的调用。如果您创建跟踪，则可以将 CloudTrail 事件持续传送到 Amazon S3 存储桶。其中包括 AWS Support App 事件。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的 Event history（事

件历史记录）中查看最新事件。您可以使用所 CloudTrail 收集的信息来确定向 AAWS Support pp 发送了什么请求。您还可以了解发起调用的 IP 地址、请求方、请求时间以及其他详细信息。

要了解更多信息 CloudTrail，请参阅AWS CloudTrail用户指南。

AWS Support中的应用程序信息 CloudTrail

创建后即可AWS 账户将在该账户 CloudTrail 上激活。当AWS Support App 中发生公有 API 活动时，该活动将记录在事件中，并与其他AWS服务 CloudTrail 事件一同保存在 Event history（事件历史记录）中。您可以在 AWS 账户 中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录 AWS 账户 中的事件（包括 AWS Support App 事件），请创建 trail（跟踪）。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他 AWS 服务，进一步分析 CloudTrail 日志中收集的事件数据，并根据数据采取相应行动。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为配置 Amazon SNS 通知 CloudTrail
- 从多个区域接收 CloudTrail 日志文件和从多个账户中接收 CloudTrail 日志文件

CloudTrail 记录所有公有AWS Support App 操作。这些操作也记录在 App Slack API 中的 AWS Support App API 参考中。例如，对的`CreateSlackChannelConfiguration`调用`GetAccountAlias`和`UpdateSlackChannelConfiguration`操作会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务 发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 AWS Support App 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。 CloudTrail 日志文件不是公有 API 调用的有序堆栈跟踪。这意味着这些日志不会按任何特定顺序显示。

Example ：**`CreateSlackChannelConfiguration`** 的日志示例

以下示例显示了该CreateSlackChannelConfiguration操作 CloudTrail 的日志条目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:JaneDoe",
        "arn": "arn:aws:sts::111122223333:assumed-role/Administrator/JaneDoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
```

```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Administrator",
                "accountId": "111122223333",
                "userName": "Administrator"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-02-26T01:37:57Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-02-26T01:48:20Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "CreateSlackChannelConfiguration",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": {
        "notifyOnCreateOrReopenCase": true,
        "teamId": "T012ABCDEFG",
        "notifyOnAddCorrespondenceToCase": true,
        "notifyOnCaseSeverity": "all",
        "channelName": "troubleshooting-channel",
        "notifyOnResolveCase": true,
        "channelId": "C01234A5BCD",
        "channelRoleArn": "arn:aws:iam::111122223333:role/AWSSupportAppRole"
    },
    "responseElements": null,
    "requestID": "d06df6ca-c233-4ffb-bbff-63470c5dc255",
    "eventID": "0898ce29-a396-444a-899d-b068f390c361",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example ：**ListSlackChannelConfigurations** 的日志示例

以下示例显示了该ListSlackChannelConfigurations操作 CloudTrail 的日志条目。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:AWSSupportAppRole",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:06:32Z",
                "mfaAuthenticated": "false"
```

```
            }
        }
    },
    "eventTime": "2022-03-01T20:06:46Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "ListSlackChannelConfigurations",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.131",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "20f81d63-31c5-4351-bd02-9eda7f76e7b8",
    "eventID": "70acb7fe-3f84-47cd-8c28-cc148ad06d21",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example ：**`GetAccountAlias`** 的日志示例

以下示例显示了该GetAccountAlias操作 CloudTrail 的日志条目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE:devdsk",
        "arn": "arn:aws:sts::111122223333:assumed-role/AWSSupportAppRole/devdsk",
        "accountId": "111122223333",
        "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AWSSupportAppRole",
                "accountId": "111122223333",
                "userName": "AWSSupportAppRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-01T20:31:27Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-01T20:31:47Z",
    "eventSource": "supportapp.amazonaws.com",
    "eventName": "GetAccountAlias",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.217.142",
    "userAgent": "aws-cli/1.3.23 Python/2.7.6 Linux/2.6.18-164.el5",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "a225966c-0906-408b-b8dd-f246665e6758",
    "eventID": "79ebba8d-3285-4023-831a-64af7de8d4ad",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

AWS Support Plans 的监控和日志记录

监控是保持 Support Plans 和您的其他 AWS 解决方案的可靠性、可用性和性能的重要方面。AWS 提供了以下一些监控工具来监控 Support Plans、在出现错误时进行报告并适时自动采取措施：

- AWS CloudTrail 捕获由您的 AWS 账户或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Simple Storage Service（Amazon S3）存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 AWS CloudTrail 用户指南。

主题

- 使用 AWS CloudTrail 记录 AWS Support Plans API 调用 (p. 320)

使用 AWS CloudTrail 记录 AWS Support Plans API 调用

AWS Support Plans与 AWS CloudTrail 集成，后者是记录用户、角色或 AWS 服务 所执行操作的服务。CloudTrail将的 API 调用AWS Support作为事件捕获。捕获的调用包含来自 AWS Support Plans 控制台和代码对 AWS Support Plans API 操作的调用。

如果您创建跟踪记录，则可以使 Amazon SimpSimple Storage Service (Amazon S3) 存储桶（包括 PlansAWS Support 事件）。CloudTrail如果您不配置跟踪记录，则仍可在 CloudTrail 控制台的 Event history（事件历史记录）中查看最新事件。

通过使用收集的信息CloudTrail，您可以确定向AWS Support Plans 发出了什么请求、发出请求的 IP 地址、发出请求的用户、发出请求的时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息（包括如何配置和启用它），请参阅 AWS CloudTrail 用户指南。

AWS Support中的计划信息CloudTrail

在您创建 AWS 账户 账户时，即针对该账户启用了 CloudTrail。当 Plans 中AWS Support发生受支持的事件活动时，该活动将记录在 ECloudTrail vent history（AWS 服务事件历史记录）中。您可以在 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录您的账户中的事件（包括 AWS Support Plans 事件），请创建一个 trail（跟踪）。通过跟踪 CloudTrail，可将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户中接收 CloudTrail 日志文件

所有的AWS Support Plans API 操作均由记录CloudTrail。每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务 发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

您也可以将多个 AWS 区域 和多个账户的 AWS Support Plans 日志文件聚合到单个 Amazon S3 存储桶中。

了解 AWS Support Plans 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 桶。CloudTrail 日志文件包含一个或多个日志条目。事件 表示来自任何源的单个请求。它包括有关所请求操作的信息、操作的日期和时间和请求参数等。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

Example ：**`GetSupportPlan`** 的日志条目

以下示例显示了 `GetSupportPlan` 操作的一个 CloudTrail 日志条目。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:11Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlan",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "7665c39a-d6bf-4d0d-8010-2f59740b8ecb",
    "eventID": "b711bc30-16a5-4579-8f0d-9ada8fe6d1ce",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Example ：**GetSupportPlanUpdateStatus** 的日志条目

以下示例显示了 GetSupportPlanUpdateStatus 操作的一个 CloudTrail 日志条目。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:39:02Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "GetSupportPlanUpdateStatus",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37a2756181
    },
    "responseElements": null,
    "requestID": "75e5c767-8703-4ed3-b01e-4dda28020322",
    "eventID": "28d1c0e3-ccb6-4fd1-8793-65be010114cc",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example ：**StartSupportPlanUpdate** 的日志条目

以下示例显示了 StartSupportPlanUpdate 操作的一个 CloudTrail 日志条目。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-06-29T16:30:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-06-29T16:38:55Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "StartSupportPlanUpdate",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "98add111-dcc9-464d-8722-438d697fe242",
        "update": {
            "supportLevel": "BASIC"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn":
 "arn:aws:supportplans::111122223333:supportplanupdate/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37a2756181
    },
    "requestID": "e5ff9382-5fb8-4764-9993-0f33fb0b1e17",
    "eventID": "5dba89f8-2e5b-42b9-9b8f-395580c52962",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Example ：**`CreateSupportPlanSchedule`** 的日志条目

以下示例显示了 `CreateSupportPlanSchedule` 操作的一个 CloudTrail 日志条目。


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-09T16:30:04Z",
                "mfaAuthenticated": "false"
```

```
            }
        }
    },
    "eventTime": "2023-05-09T16:30:04Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "CreateSupportPlanSchedule",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.183",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "clientToken": "b998de5e-ad1c-4448-90db-2bf86d6d9e9a",
        "scheduleCreationDetails": {
            "startLevel": "BUSINESS",
            "startOffer": "TrialPlan7FB93B",
            "startTimestamp": "2023-06-03T17:23:56.109Z",
            "endLevel": "BUSINESS",
            "endOffer": "StandardPlan2074BB",
            "endTimestamp": "2023-09-03T17:23:55.109Z"
        }
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "supportPlanUpdateArn": "arn:aws:supportplans::111122223333:supportplanschedule/
b9a9a4336a3974950a6e670f7dab79b77a4b104db548a0d57050ce4544721d4b"
    },
    "requestID": "150450b8-e61a-4b15-93a8-c3b557a1ca48",
    "eventID": "a2a1ba44-610d-4dc8-bf16-29f1635b57a9",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

记录对您的 AWS Support 计划的更改

Important

自 2022 年 8 月 3 日起，以下操作已弃用，将不会出现在您的新 CloudTrail 日志中。有关支持的操作的列表，请参阅 了解 AWS Support Plans 日志文件条目 (p. 321)。

- `DescribeSupportLevelSummary` – 当您打开 Support 计划页面时，此操作显示在您的日志中。
- `UpdateProbationAutoCancellation` – 当您注册开发人员支持计划或业务支持计划，然后尝试在 30 天内取消后，您的计划将在该期限结束时自动取消。当您在 Support plans（支持计划）页面中显示的横幅中选择 Opt-out of automatic cancellation（退出自动取消）时，此操作显示在您的日志中。您将恢复您的开发人员支持或业务支持计划。
- `UpdateSupportLevel` – 当您更改支持计划时，此操作显示在您的日志中。

Note

`eventSource` 字段具有这些操作的 `support-subscription.amazonaws.com` 命名空间。

Example ：DescribeSupportLevelSummary 的日志条目

以下示例说明了 `DescribeSupportLevelSummary` 操作的 CloudTrail 日志条目。

```
{
  "eventVersion": "1.08",
```

```
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:07Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "DescribeSupportLevelSummary",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "b423b84d-829b-4090-a239-2b639b123abc",
  "eventID": "e1eeda0e-d77c-487b-a7e5-4014f7123abc",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


Example ：UpdateProbationAutoCancellation 的日志条目

以下示例说明了 UpdateProbationAutoCancellation 操作的 CloudTrail 日志条目。


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE"
  },
  "eventTime": "2021-01-07T23:28:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateProbationAutoCancellation",
  "awsRegion": "us-east-1", "sourceIPAddress": "100.127.8.67",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "lang": "en"
  },
  "responseElements": null,
  "requestID": "5492206a-e200-4c33-9fcf-4162d4123abc",
  "eventID": "f4a58c09-0bb0-4ba2-a8d3-df6909123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

Example ：UpdateSupportLevel 的日志条目

以下示例显示了用于更改开发人员支持计划的 UpdateSupportLevel 操作的 CloudTrail 日志条目。


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:iam::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-01-07T22:08:05Z"
      }
    }
  },
  "eventTime": "2021-01-07T22:08:43Z",
  "eventSource": "support-subscription.amazonaws.com",
  "eventName": "UpdateSupportLevel",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "100.127.8.247",
  "userAgent": "AWS-SupportPlansConsole, aws-internal/3",
  "requestParameters": {
    "supportLevel": "new_developer"
  },
  "responseElements": {
    "aispl": false,
    "supportLevel": "new_developer"
  },
  "requestID": "5df3da3a-61cd-4a3c-8f41-e5276b123abc",
  "eventID": "c69fb149-c206-47ce-8766-8df6ec123abc",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

AWS Trusted Advisor 的监控和日志记录

监控是保持 Trusted Advisor 和您的其他 AWS 解决方案的可靠性、可用性和性能的重要方面。AWS 提供了以下一些监控工具来监控 Trusted Advisor、在出现错误时进行报告并适时自动采取措施。

- Amazon EventBridge Events 提供近乎实时的系统事件流，这些系统事件描述了AWS资源的更改。EventBridge 支持自动事件驱动型计算，因为您可以编写规则，以监控某些事件和在这些事件发生时在其他AWS服务中触发自动操作。

  例如，Trusted Advisor 提供 Amazon S3 存储桶权限检查。此检查确定您是否具有满足以下条件的存储桶：具有开放的访问权限或允许任何经过身份验证的 AWS 用户进行访问。如果存储桶权限发生变化，则 Trusted Advisor检查的状态会发生更改。 EventBridge 检测到此事件，然后向您发送通知，以便您可以采取措施。有关更多信息，有关更多信息，Amazon V Amazon EventBridge VAmazon C
- AWS Trusted Advisor 检查可确定供您降低成本、改善性能和提高 AWS 账户安全性的方法。您可以使用 A EventBridge mazonTrusted Advisor 检查的状态。然后，您可以使用 Amazon Amazon E CloudWatch vents 创建有关Trusted Advisor指标的警报 当 Trusted Advisor 检查的状态发生变化（例如，更新了资源或已达到服务配额）时，这些警报向您发出通知。
- AWS CloudTrail 捕获由您的 AWS 账户或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Simple Storage Service（Amazon S3）存储桶。您可以标识哪些用户和账户调用了 AWS、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 AWS CloudTrail 用户指南。

主题

- 与亚马逊一起监控AWS Trusted Advisor检查结果EventBridge (p. 327)
- 创建亚马逊 CloudWatch 警报以监控AWS Trusted Advisor指标 (p. 329)
- 使用 AWS CloudTrail 记录 AWS Trusted Advisor 控制台操作 (p. 337)

与亚马逊一起监控AWS Trusted Advisor检查结果EventBridge

您可以使用 EventBridge 来检测对 Trusted Advisor 的检查何时会更改状态。随后，当您在规则中指定的某个值的状态更改时，EventBridge 会根据您创建的规则调用一个或多个目标操作。

根据具体的状态更改，您可以发送通知、捕获状态信息、采取纠正措施、启动事件或采取其他操作。例如，如果检查状态由未检测到的问题（绿色）更改为建议的操作（红色），则可以指定以下目标类型。

- 使用 AWS Lambda 函数将通知传入 Slack 通道。
- 将有关检查的数据推送到 Amazon Kinesis 流，以支持全面、实时的状态监控。
- 将 Amazon Simple Notification Service 主题发送到您的电子邮件。
- 通过 AmazonCloudWatch 告警操作接收通知。

有关如何使用EventBridge和 Lambda 函数自动响应的更多信息Trusted Advisor，请参阅中的Trusted Advisor工具GitHub。

注意

- Trusted Advisor 将尽最大效能传送事件。并不总是能保证将事件传送到 EventBridge。

- 您必须拥有 AWS Support 计划才能为 Trusted Advisor 检查创建规则。有关更多信息，请参阅更改 AWS Support Plans (p. 18)：
- 与全局服务一样，所有EvenTrusted Advisor ts 均在美国东部（弗吉尼亚北部）区域发送 Events。EventBridge

按照以下过程为 Trusted Advisor 创建 EventBridge 规则。在创建事件规则之前，请执行以下操作：

- 熟悉 EventBridge 中的事件、规则和目标。有关更多信息，请参阅什么是 AmazonEventBridge？ 在亚马逊EventBridge用户指南中。
- 创建将在事件规则中使用的目标。

为 Trusted Advisor 创建 EventBridge 规则

1. 通过 https://console.aws.amazon.com/events/ 打开亚马逊EventBridge控制台。
2. 要更改区域，请使用页面右上角的 Region selector（区域选择器），然后选择 US East (N. Virginia)（美国东部（弗吉尼亚北部））。
3. 在导航窗格中，选择 Rules (规则)。
4. 选择 Create rule (创建规则)。
5. 在 Define rule detail（定义规则详细信息）页面上，输入规则名称和描述。
6. 对于 Event bus（事件总线）和 Rule type（规则类型），保留默认值，然后选择 Next（下一步）。
7. 在生成事件模式页面上，为事件源选择AWS事件或EventBridge合作伙伴事件。
8. 在 Event pattern（事件模式）下，请保留默认值（ AWS 服务）。
9. 对于 AWS 服务，选择 Trusted Advisor。
10. 对于 Event type（事件类型），选择 Check Item Refresh Status（检查项目刷新状态）。
11. 为检查状态选择以下选项之一：
    - 选择 Any status（任何状态）以创建监控任何状态更改的规则。
    - 选择 Specific status(es)（特定状态），然后选择要让您的规则监控的值。
      - ERROR（错误）– Trusted Advisor 为检查建议某一操作。
      - INFO（信息）– Trusted Advisor 无法确定检查的状态。
      - OK（正常）– Trusted Advisor 没有检测到检查的问题。
      - WARN（警告）–Trusted Advisor 检测到检查可能存在问题并建议调查。
12. 为您的检查选择以下选项之一：
    - 选择 Any check（任何检查）。
    - 选择 Specific check(s)（特定检查），然后从列表中选择一个或多个检查名称。
13. 为 AWS 资源选择以下选项之一：
    - 选择 Any resource ID（任何资源 ID）来创建监控所有资源的规则。
    - 选择 Specific resource ID(s) by ARN（按 ARN 排列的特定资源 ID），然后输入您想要的 Amazon Resource Name (ARN)。
14. 选择下一步。
15. 在 Select target(s)（选择目标）页面中，选择您为此规则创建的目标类型，然后配置该类型所需的任何其他选项。例如，您可以将事件发送到 Amazon SQS 队列或 Amazon SNS 主题。
16. 选择下一步。
17. （可选）在 Configure tags（配置标签）页面上，添加任意标签，然后选择 Next（下一步）。
18. 在 Review and create（审查并创建）页面上，审查您的规则设置并确保其符合您的事件监控要求。
19. 选择 Create rule（创建规则）。您的规则现在将监控 Trusted Advisor 检查，然后将事件发送到您指定的目标。

创建亚马逊 CloudWatch 警报以监控AWS Trusted Advisor指标

AWS Trusted Advisor刷新您的检查时，将有关您的检查结果的指标Trusted Advisor发布到 CloudWatch。您可以在 CloudWatch 中查看指标。您还可以创建告警以检测 Trusted Advisor 检查的状态变化和资源的状态变化，以及服务配额使用情况（以前称为限制）。例如，您可以创建告警，以跟踪 Service Limits 类别中的检查的状态变化。当您达到或超出您的 AWS 账户的服务配额时，告警会通知您。

按照以下步骤为特定的Trusted Advisor指标创建 CloudWatch 告警。

主题

- 先决条件 (p. 329)
- CloudWatch 的指标Trusted Advisor (p. 331)
- Trusted Advisor 指标和维度 (p. 336)

先决条件

在为Trusted Advisor指标创建 CloudWatch 告警之前，请查看以下信息：

- 了解如何 CloudWatch 使用指标和告警。有关更多信息，请参阅《亚马逊 CloudWatch 用户指南》中的“CloudWatch 工作原理”。
- 使用 Trusted Advisor 控制台或 AWS Support API 来刷新您的检查并获取最新的检查结果。有关更多信息，请参阅刷新检查结果 (p. 24)：

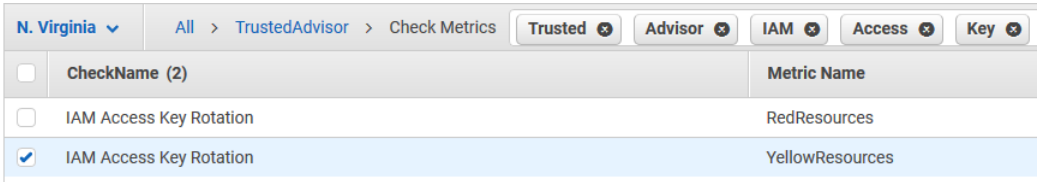
为Trusted Advisor指标创建 CloudWatch 警报

1. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 主机。
2. 使用区域选择器，然后选择美国东部（弗吉尼亚北部）AWS 区域。
3. 在导航窗格中，选择 Alarms (告警)。
4. 选择 Create Alarm (创建警报)。
5. 选择选择指标。
6. 对于指标，输入一个或多个维度值，以筛选指标列表。例如，您可以输入指标名称ServiceLimitUsage或维度，例如Trusted Advisor检查名称。

   Tip

   - 您可以搜索 **`Trusted Advisor`** 以列出服务的所有指标。
   - 有关指标和维度名称的列表，请参阅 Trusted Advisor 指标和维度 (p. 336)。
7. 在结果表中，选中指标的复选框。

   在以下示例中，检查名称为 IAM 访问密钥轮换，指标名称为YellowResources。



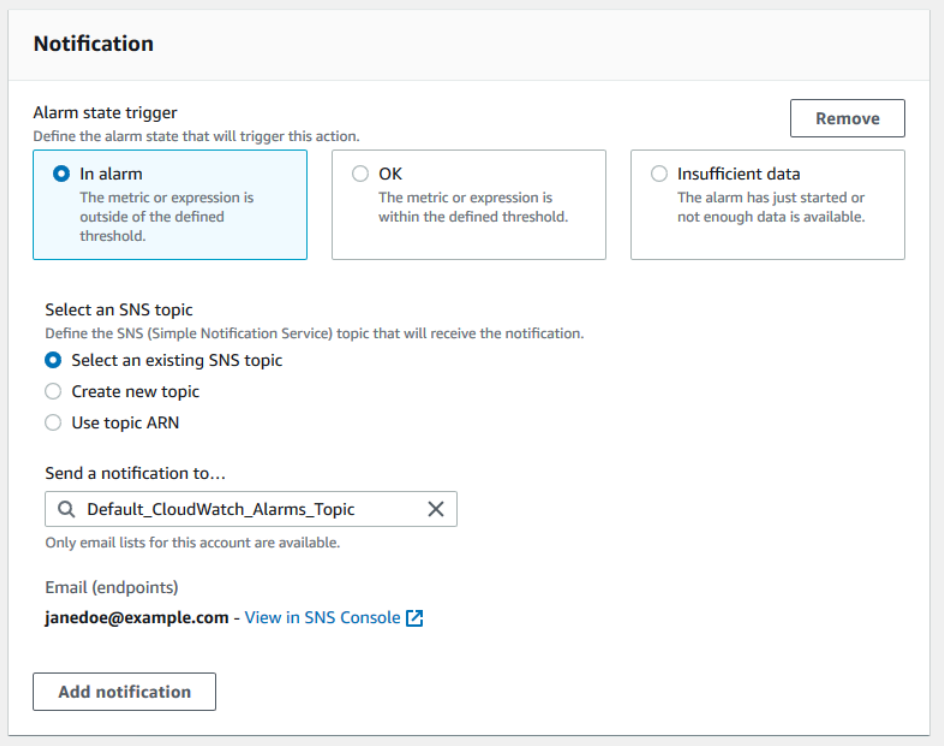
8. 选择选择指标。
9. 在 Specif y metric and c onditions conditions conditions CheckName，验证您选择的 Metric name
10. 对于 Period（期限），您可以指定当检查状态变化时您希望告警开始的时间期限，如 5 分钟。

11. 在 Conditions（条件）下，选择 Static（静态），然后指定告警启动时的告警条件。

    例如，如果您选择大于等于 >=阈值并输入 **1** 作为阈值，这意味着告警在 Trusted Advisor 检测到至少有一个在过去 90 天内未轮换的 IAM 访问密钥时开始。

    注意

    - 对于GreenChecks、RedChecks、YellowChecksRedResources、和YellowResources指标，您可以指定一个阈值，该阈值是任何大于或等于零的整数。
    - Trusted Advisor不会发送的指标 GreenResources，这些资源Trusted Advisor尚未检测到任何问题。
12. 选择下一步。
13. 在 Configure actions（配置操作）页面上，对于 Alarm state trigger（告警状态触发器），选择 In alarm（告警中）。
14. 对于 Select an SNS topic（选择 SNS 主题），选择现有的 Amazon Simple Notification Service (Amazon SNS) 主题或创建一个主题。



15. 选择下一步。
16. 对于名称和描述，输入告警的名称和描述。
17. 选择下一步。
18. 在 Preview and create（预览和创建）页面上，查看告警详细信息，然后选择 Create alarm（创建告警）。

    当IAM 访问密钥轮换检查变为红色 5 分钟时，您的告警将向您的 SNS 主题发送通知。

Example ：有关告 CloudWatch 警的电子邮件通知

以下电子邮件消息显示告警检测到 IAM 访问密钥轮换检查发生更改。

```
You are receiving this email because your Amazon CloudWatch Alarm
 "IAMAcessKeyRotationCheckAlarm" in the US East (N. Virginia) region has entered the ALARM
 state,
because "Threshold Crossed: 1 out of the last 1 datapoints [9.0 (26/03/21 22:44:00)]
 was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM
 transition)." at "Friday 26 March, 2021 22:49:42 UTC".

View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more AWS access keys in my AWS
 account have not been rotated in the last 90 days.
- State Change:               INSUFFICIENT_DATA -> ALARM
- Reason for State Change:    Threshold Crossed: 1 out of the last 1 datapoints [9.0
 (26/03/21 22:44:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint
 for OK -> ALARM transition).
- Timestamp:                  Friday 26 March, 2021 22:49:42 UTC
- AWS Account:                123456789012
- Alarm Arn:                  arn:aws:cloudwatch:us-
east-1:123456789012:alarm:IAMAcessKeyRotationCheckAlarm

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0 for
 300 seconds.

Monitored Metric:
- MetricNamespace:                    AWS/TrustedAdvisor
- MetricName:                         RedResources
- Dimensions:                         [CheckName = IAM Access Key Rotation]
- Period:                             300 seconds
- Statistic:                          Average
- Unit:                               not specified
- TreatMissingData:                   missing


State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:123456789012:Default_CloudWatch_Alarms_Topic]
- INSUFFICIENT_DATA:
```

CloudWatch 的指标Trusted Advisor

您可以使用 CloudWatch 控制台或AWS Command Line Interface (AWS CLI) 查找可用的指标Trusted Advisor。

有关发布指标的所有服务的命名空间、指标和维度的列表，请参阅 Amazon CloudWatch 用户指南中的发布 CloudWatch 指标的AWS服务。

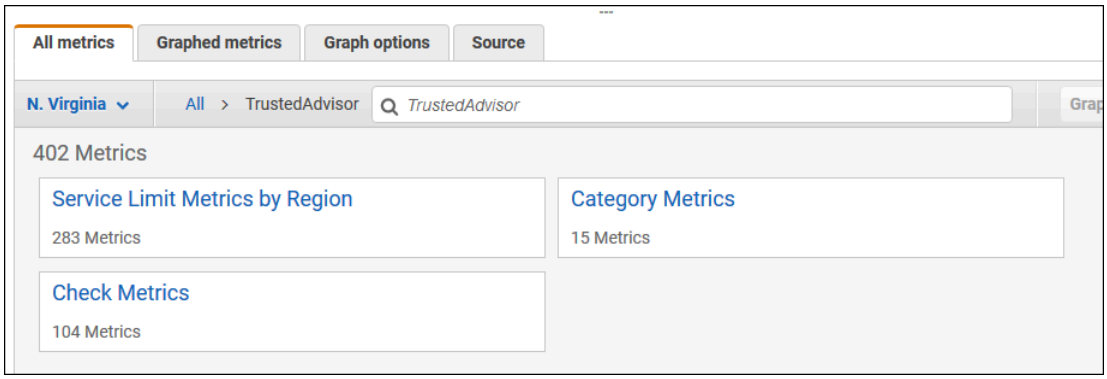
查看 Trusted Advisor 指标（控制台）

您可以登录 CloudWatch 控制台并查看的可用指标Trusted Advisor。

要查看可用的 Trusted Advisor 指标（控制台）

1. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 主机。
2. 使用区域选择器，然后选择美国东部（弗吉尼亚北部）AWS 区域。
3. 在导航窗格中，选择 Metrics（指标）。
4. 输入指标命名空间，例如 **TrustedAdvisor**。

5. 选择指标维度，例如检查指标。



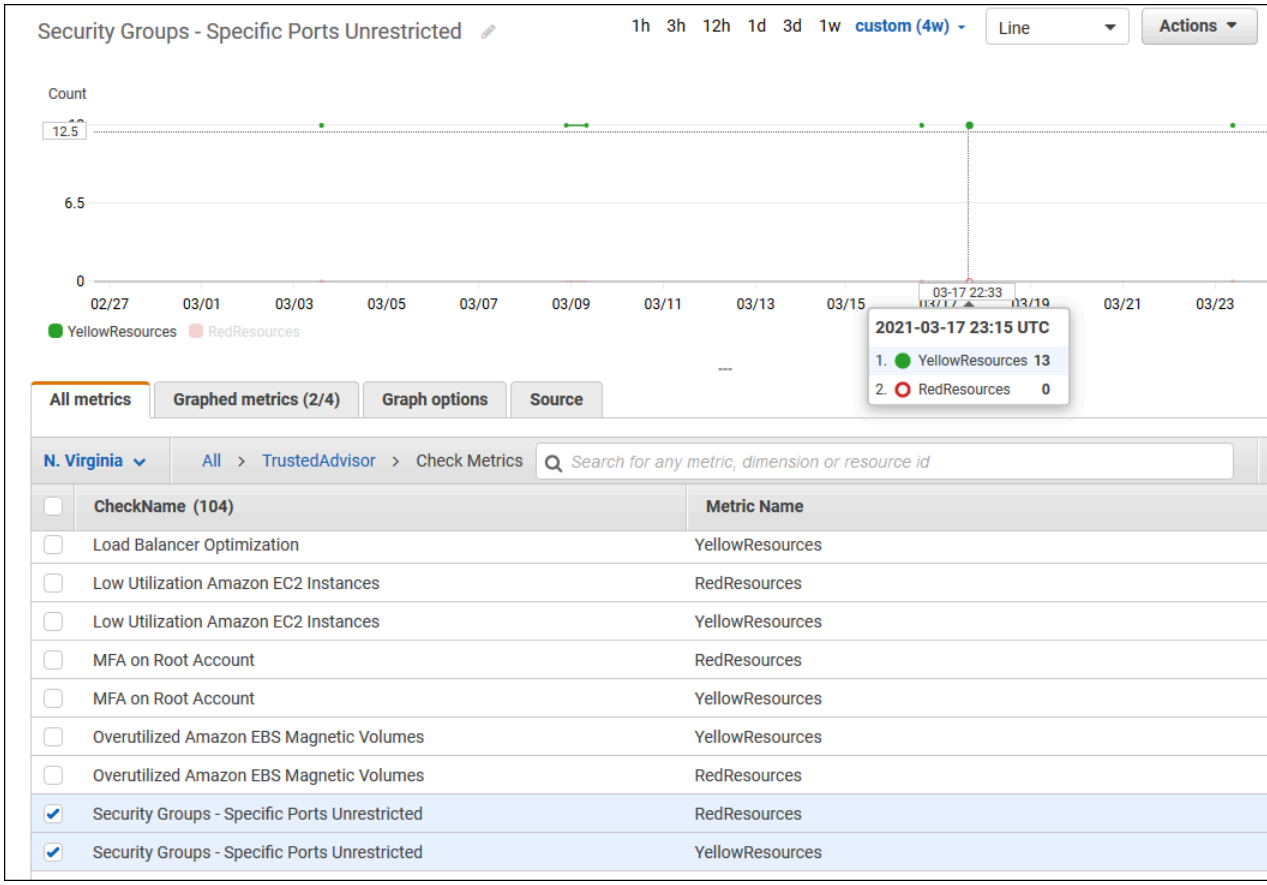
6. All metrics（所有指标）选项卡显示命名空间中该维度的指标。您可执行以下操作：

   a. 要对表进行排序，请选择列标题。

   b. 要为指标绘制图表，请选中该指标旁的复选框。要选择所有指标，请选中表的标题行中的复选框。

   c. 要按指标进行筛选，请选择指标名称，然后选择 Add to search（添加到搜索）。

   以下示例显示了安全组 - 不受限制的特定端口检查的结果。该检查标识 13 个黄色的资源。Trusted Advisor 建议您调查黄色的检查。



7. （可选）要将此图表添加到 CloudWatch 控制面板，请选择 Ad d t o dashboard（可选）。

有关创建图表以查看指标的更多信息，请参阅 Amazon CloudWatch 用户指南中的绘制指标的图表。

查看 Trusted Advisor 指标 (CLI)

您可以使用 list-metrics AWS CLI 命令查看 Trusted Advisor 的可用指标。

Example ：列出 Trusted Advisor 的所有指标

以下示例指定 AWS/TrustedAdvisor 命名空间以查看 Trusted Advisor 的所有指标。

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor
```

您的输出可能与以下内容类似。

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Magnetic (standard) volume storage (TiB)"
                },
                {
                    "Name": "Region",
                    "Value": "ap-northeast-2"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Overutilized Amazon EBS Magnetic Volumes"
                }
            ],
            "MetricName": "YellowResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "eu-west-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
```

```
                {
                    "Name": "ServiceName",
                    "Value": "EBS"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Provisioned IOPS"
                },
                {
                    "Name": "Region",
                    "Value": "ap-south-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example ：列出维度的所有指标

以下示例指定 AWS/TrustedAdvisor 命名空间和 Region 维度以查看指定 AWS 区域的可用指标。

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --dimensions
 Name=Region,Value=us-east-1
```

您的输出可能与以下内容类似。

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "SES"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Daily sending quota"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "AutoScaling"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Launch configurations"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
```

```
            ],
            "MetricName": "ServiceLimitUsage"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "ServiceName",
                    "Value": "CloudFormation"
                },
                {
                    "Name": "ServiceLimit",
                    "Value": "Stacks"
                },
                {
                    "Name": "Region",
                    "Value": "us-east-1"
                }
            ],
            "MetricName": "ServiceLimitUsage"
        },
    ...
  ]
}
```

Example ：列出特定指标名称的指标

以下示例指定 AWS/TrustedAdvisor 命名空间和 RedResources 指标名称以仅查看此指定指标的结果。

```
aws cloudwatch list-metrics --namespace AWS/TrustedAdvisor --metric-name RedResources
```

您的输出可能与以下内容类似。

```
{
    "Metrics": [
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Amazon RDS Security Group Access Risk"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Exposed Access Keys"
                }
            ],
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Large Number of Rules in an EC2 Security Group"
                }
            ],
```

```
            "MetricName": "RedResources"
        },
        {
            "Namespace": "AWS/TrustedAdvisor",
            "Dimensions": [
                {
                    "Name": "CheckName",
                    "Value": "Auto Scaling Group Health Check"
                }
            ],
            "MetricName": "RedResources"
        },
    ...
  ]
}
```

Trusted Advisor 指标和维度

请参阅下表以了解您可以用于 CloudWatch 告警和图表的 Trusted Advisor 指标和维度。

Trusted Advisor 检查级别指标

您可以将以下指标用于 Trusted Advisor 检查。

指标	描述
RedResources	处于红色状态的资源数（建议采取操作）。
YellowResources	处于黄色状态的资源数（建议调查）。

Trusted Advisor 类别级别指标

您可以将以下指标用于 Trusted Advisor 类别。

指标	描述
GreenChecks	处于绿色状态（未检测到任何问题）的 Trusted Advisor 检查的数量。
RedChecks	处于红色状态的 Trusted Advisor 检查数量（建议采取操作）。
YellowChecks	处于黄色状态的 Trusted Advisor 检查数量（建议调查）。

Trusted Advisor 服务配额级指标

您可以使用以下有关 AWS 服务限额的指标。

指标	描述
ServiceLimitUsage	资源使用量对服务配额（以前称为限制）的百分比。

检查级别指标的维度

您可以将以下维度用于 Trusted Advisor 检查。

维度	描述
CheckName	Trusted Advisor 检查的名称。 您可以在 Trusted Advisor 控制台或 AWS Trusted Advisor 检查引用 (p. 65) 中找到所有检查名称。

类别级别指标的维度

您可以将以下维度用于 Trusted Advisor 检查类别。

维度	描述
Category	Trusted Advisor 检查类别的名称。 您可以在 Trusted Advisor 控制台或 查看检查类别 (p. 21) 页面中找到所有检查类别。

服务配额指标的维度

您可以将以下维度用于 Trusted Advisor 服务配额指标。

维度	描述
Region	服务限额的 AWS 区域。
ServiceName	AWS 服务 的名称。
ServiceLimit	服务配额的名称。 有关服务限额的更多信息，请参阅 AWS 一般参考 中 AWS 服务 限额。

使用 AWS CloudTrail 记录 AWS Trusted Advisor 控制台操作

Trusted Advisor与AWS CloudTrail服务集成，后者提供了某个用户、角色或AWS服务在中执行的操作的记录 Trusted Advisor。 CloudTrail 将的调用Trusted Advisor作为事件捕获。捕获的调用包括来自 Trusted Advisor 控制台的调用。如果您创建了跟踪记录，则可以将 CloudTrail 事件持续传送到某个 Amazon Simple Simple Storage Service (Amazon S3) 存储桶（包括的事件）Trusted Advisor。如果您不配置跟踪记录，则仍可在 CloudTrail 控制台的 Event history（事件历史记录）中查看最新事件。通过使用收集的信息 CloudTrail，您可以确定向发出了什么请求Trusted Advisor、发出请求的 IP 地址、何人发出的请求、请求的用户、请求的发出时间以及其他详细信息。

要了解 CloudTrail更多信息（包括如何对其进行配置和启用），请参阅AWS CloudTrail用户指南。

Trusted Advisor中的信息 CloudTrail

CloudTrail 在您创建AWS账户时，将在该账户上启用。当Trusted Advisor控制台中发生受支持的事件活动时，该活动将记录在事件中，并与其他AWS服务 CloudTrail 事件一同保存在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录 AWS 账户中的事件（包括 Trusted Advisor 的事件），请创建跟踪。通过跟踪 CloudTrail ，可将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他AWS服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取操作。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 为配置 Amazon SNS 通知 CloudTrail
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail日志文件

Trusted Advisor支持将Trusted Advisor控制台操作的子集作为 CloudTrail 日志文件中的事件记录。CloudTrail 记录以下操作：

- `DescribeAccount`
- `DescribeAccountAccess`
- `DescribeChecks`
- `DescribeCheckItems`
- `DescribeCheckRefreshStatuses`
- `DescribeCheckSummaries`
- `DescribeNotificationPreferences`
- `DescribeOrganization`
- `DescribeOrganizationAccounts`
- `DescribeReports`
- `DescribeRisk`
- `DescribeRisks`
- `DescribeRiskResources`
- `DescribeServiceMetadata`
- `DownloadRisk`
- `ExcludeCheckItems`
- `GenerateReport`
- `IncludeCheckItems`
- `ListAccountsForParent`
- `ListRoots`
- `ListOrganizationalUnitsForParent`
- `RefreshCheck`
- `SetAccountAccess`
- `SetOrganizationAccess`
- `UpdateNotificationPreferences`
- `UpdateRiskStatus`

有关 Trusted Advisor 控制台操作的完整列表，请参阅 Trusted Advisor 操作 (p. 227)。

> **Note**
>
> CloudTrail 还在Trusted Advisor API 参考中记录AWS Support API 操作。有关更多信息，请参阅使用 AWS Support 记录 AWS CloudTrail API 调用 (p. 314)：

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

示例：Trusted Advisor 日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。 CloudTrail 日志文件不是公有 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

Example ：的日志条目 RefreshCheck

以下示例显示了一个 CloudTrail 日志条目，该条目说明了用于 Amazon S3 Bucket Versioning 检查 (IDR365s2Qddf) 的`RefreshCheck`操作。


```
{
   "eventVersion":"1.04",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/janedoe",
      "accountId":"123456789012",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "userName":"janedoe",
      "sessionContext":{
         "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2020-10-21T22:06:18Z"
         }
      }
   },
   "eventTime":"2020-10-21T22:06:33Z",
   "eventSource":"trustedadvisor.amazonaws.com",
   "eventName":"RefreshCheck",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"100.127.34.136",
   "userAgent":"signin.amazonaws.com",
   "requestParameters":{
      "checkId":"R365s2Qddf"
   },
   "responseElements":{
      "status":{
         "checkId":"R365s2Qddf",
         "status":"enqueued",
         "millisUntilNextRefreshable":3599993
      }
   },
   "requestID":"d23ec729-8995-494c-8054-dedeaEXAMPLE",
   "eventID":"a49d5202-560f-4a4e-b38a-02f1cEXAMPLE",
   "eventType":"AwsApiCall",
   "recipientAccountId":"123456789012"
}
```


Example ：的日志条目 UpdateNotificationPreferences

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了`UpdateNotificationPreferences`操作。

```
{
   "eventVersion":"1.04",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/janedoe",
      "accountId":"123456789012",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "userName":"janedoe",
      "sessionContext":{
         "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2020-10-21T22:06:18Z"
         }
      }
   },
   "eventTime":"2020-10-21T22:09:49Z",
   "eventSource":"trustedadvisor.amazonaws.com",
   "eventName":"UpdateNotificationPreferences",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"100.127.34.167",
   "userAgent":"signin.amazonaws.com",
   "requestParameters":{
      "contacts":[
         {
            "id":"billing",
            "type":"email",
            "active":false
         },
         {
            "id":"operational",
            "type":"email",
            "active":false
         },
         {
            "id":"security",
            "type":"email",
            "active":false
         }
      ],
      "language":"en"
   },
   "responseElements":null,
   "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
   "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
   "eventType":"AwsApiCall",
   "recipientAccountId":"123456789012"
}
```


Example ：的日志条目 GenerateReport

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了`GenerateReport`操作。此操作会为您的 AWS 组织创建报告。


```
{
   "eventVersion":"1.04",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/janedoe",
      "accountId":"123456789012",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "userName":"janedoe",
      "sessionContext":{
```

```
         "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2020-11-03T13:03:10Z"
         }
      }
   },
   "eventTime":"2020-11-03T13:04:29Z",
   "eventSource":"trustedadvisor.amazonaws.com",
   "eventName":"GenerateReport",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"100.127.36.171",
   "userAgent":"signin.amazonaws.com",
   "requestParameters":{
      "refresh":false,
      "includeSuppressedResources":false,
      "language":"en",
      "format":"JSON",
      "name":"organizational-view-report",
      "preference":{
         "accounts":[

         ],
         "organizationalUnitIds":[
            "r-j134"
         ],
         "preferenceName":"organizational-view-report",
         "format":"json",
         "language":"en"
      }
   },
   "responseElements":{
      "status":"ENQUEUED"
   },
   "requestID":"bb866dc1-60af-47fd-a660-21498EXAMPLE",
   "eventID":"2606c89d-c107-47bd-a7c6-ec92fEXAMPLE",
   "eventType":"AwsApiCall",
   "recipientAccountId":"123456789012"
}
```

资源问题排查

有关常见疑难解答，请参阅 AWS Support 知识中心。

Amazon EC2 为 Windows 实例提供了 EC2Rescue，客户可使用该工具检查其 Windows 实例以帮助识别常见问题、收集日志文件，以及帮助 AWS Support 排查问题。您还可以使用 EC2Rescue 分析无法运行的实例的引导卷。有关更多信息，请参阅我如何使用 EC2Rescue 在自己的 EC2 Windows 实例上排除并修复问题？

特定于服务的问题排查

大多数 AWS 服务文档都包含问题排查主题，您可以参考这些主题尝试解决问题，然后再联系 AWS Support。下表提供了指向问题排查主题的链接（按服务排列）。

Note

下表提供了最常见的服务列表。要搜索其他故障排除主题，请使用 AWS 文档登录页面上的搜索文本框。

服务	Link
Amazon Web Services	排除 AWS 签名版本 4 错误
Amazon API Gateway	HTTP API 故障排除
亚马逊 AppStream	亚马逊疑难解答 AppStream
Amazon Athena	在 Athena 中进行故障排除
Amazon Aurora MySQL	Amazon Aurora 故障排除
Amazon Aurora PostgreSQL	Amazon Aurora 故障排除
Amazon EC2 Auto Scaling	Auto Scaling 故障排除
AWS Certificate Manager (ACM)	故障排除
AWS CloudFormation	AWS CloudFormation 故障排除
亚马逊 CloudFront	问题排查 | RTMP 分配问题排查
AWS CloudHSM	故障排除
亚马逊 CloudSearch	亚马逊疑难解答 CloudSearch
AWS CodeDeploy	AWS CodeDeploy 故障排除
亚马逊 CloudWatch	https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-metric-streams-troubleshoot.html 故障排除
AWS Database Migration Service	对 AWS Database Migration Service 中的迁移任务进行故障排除
AWS Data Pipeline	故障排除
AWS Direct Connect	AWS Direct Connect 故障排除
AWS Directory Service	排查 AWS Directory Service 管理问题

服务	Link
Amazon DynamoDB	故障排除 | 建立 SSL/TLS 连接故障排除
AWS Elastic Beanstalk	故障排除
Amazon Elastic Compute Cloud (Amazon EC2)	实例问题排查 | Windows 实例问题排查 | VM Import/Export 问题排查 | API 请求错误排查 | AWS 管理包问题排查 | AWS Systems Manager for Microsoft SCVMM 问题排查 | 适用于 Microsoft Windows 服务器的 AWS 诊断
Amazon Elastic Container Service (Amazon ECS)	Amazon ECS 故障排除
Amazon Elastic Kubernetes Service (Amazon EKS)	Amazon EKS 故障排除
弹性负载均衡	对 Application Load Balancer 进行问题排查 | 对经典负载均衡器进行问题排查
Amazon ElastiCache Elazon E	对应用程序进行问题排查
ElastiCache 适用于 Redis 的亚马逊	对应用程序进行问题排查
Amazon EMR	集群问题排查
AWS Flow Framework	问题排查和调试提示
AWS Glue	AWS Glue 故障排除
AWS Glue DataBrew	对 AWS Glue DataBrew 中的身份和访问进行故障排除
AWS GovCloud (US)	故障排除
AWS Identity and Access Management (IAM)	IAM 故障排除
Amazon Keyspaces (for Apache Cassandra)	Amazon Keyspaces（Apache Cassandra 兼容）故障排除
Amazon Kinesis Data Streams	Amazon Kinesis Data Streams 创建器故障排除 | Amazon Kinesis Data Streams 使用器故障排除
Amazon Kinesis Data Analytics	性能故障排除 | Amazon Kinesis Data Analytics for SQL 应用程序故障排除
Amazon Kinesis Data Firehose	Amazon Kinesis Data Firehose 故障排除
AWS Lambda	故障排除和监控AWS Lambda功能 CloudWatch
亚马逊 OpenSearch 服务	亚马逊 OpenSearch 服务疑难解答
AWS OpsWorks	调试和问题排查指南
Amazon Personalize	故障排除
Amazon QLDB	Amazon QLDB 故障排除
亚马逊 QuickSight	亚马逊疑难解答 QuickSight | 排除跳行错误

服务	Link
AWS Resource Access Manager (AWS RAM)	排查 AWS RAM 的问题
Amazon Redshift	查询故障排除 | 数据负载故障排除 | Amazon Redshift 连接故障排除 | Amazon Redshift 审核记录故障排除 | Amazon Redshift Spectrum 查询故障排除
Amazon Relational Database Service (Amazon RDS)	故障排除 | Amazon RDS 上的应用程序故障排除 | Amazon RDS Custom 数据库问题故障排除
Amazon Route 53	Amazon Route 53 问题排查
亚马逊 SageMaker	排除错误 | 亚马逊 SageMaker 工作室疑难解答
Amazon Silk	故障排除
Amazon Simple Email Service (Amazon SES)	Amazon SES 故障排除
Amazon Simple Storage Service (Amazon S3)	故障排除
Amazon Simple Workflow Service (Amazon SWF)	适用于 Java 的 AWS 流框架：问题排查和调试提示 | 适用于 Ruby 的 AWS 流框架：问题排查和调试工作流程
AWS Storage Gateway	排查网关问题
AWS Systems Manager	SSM Agent 故障排除
Amazon Virtual Private Cloud (Amazon VPC)	故障排除
AWS Virtual Private Network (AWS VPN)	对客户网关设备进行故障排除
AWS WAF	测试和调整您的 AWS WAF 保护措施
亚马逊 WorkMail	对亚马逊 WorkMail Web 应用程序进行故障排除
亚马逊 WorkSpaces	亚马逊 WorkSpaces 问题疑难解答 | 亚马逊 WorkSpaces 客户端问题疑难解答
Amaz WorkSpaces on Manager (Amazon WAM)	Amazon WAM 应用程序故障排除

文档历史记录

下表介绍了自 AWS Support 服务上一次发布以来对文档所做的重要更改。

- AWS Support API 版本：2013-04-15
- AWS Support App API 版本：2021-08-20

下表介绍了自 2021 年 5 月 10 日以来对 AWS Support 和 AWS Trusted Advisor 文档的重要更新。您可以订阅 RSS 源来接收有关更新的通知。

变更	说明	日期
更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2023 年 6 月 26 日
更新了 Trusted Advisor 的文档 (p. 345)	为 Amazon MQ 添加了两项新的容错检查。为 Amazon Elastic 文件系统添加了一项新的容错检查和一项新的性能检查。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2023 年 6 月 1 日
更新了 Trusted Advisor 的文档 (p. 345)	为 NAT 网关添加了两项新的容错检查。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2023 年 5 月 16 日
更新了 AWS Support 计划的文档 (p. 345)	为创建支持计划时间表添加了新的权限和CloudTrail文档。有关更多信息，请参阅使用管理AWS Support计划访问权限、计划AWS托管策略和记录AWS Support计划 API 调用AWS CloudTrail。AWS Support	2023 年 5 月 8 日
更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2023 年 5 月 2 日
更新了 “Trusted Advisor参与和Trusted Advisor优先级” 的文档 (p. 345)	阐明了Trusted Advisor参与和Trusted Advisor优先级的先决条件。添加了能够使用 Eng Trusted Advisor age 和启用可信访问权限的 IAM 策略示例Trusted Advisor。	2023 年 4 月 28 日
更新了 Trusted Advisor 的文档 (p. 345)	为AWS Resilience Hub和事件管理器添加了两项新的容错检查。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2023 年 4 月 27 日

添加了 Eng Trusted Advisor age 的文档 (p. 345)	您可以使用 Eng AWS Trusted Advisor age 让您可以轻松查看、请求和跟踪所有主动参与，并就正在进行的活动与AWS 账户团队进行沟通，从而充分利用您的AWS Support计划。有关更多信息，请参阅 En g AWS Trusted Advisor age 入门。	2023 年 4 月 6 日
更新了 Trusted Advisor 的文档 (p. 345)	为 Amazon ECS 添加了两项新的容错检查。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2023 年 3 月 30 日
更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2023 年 3 月 16 日
添加了 Trusted Advisor Priority 的文档 (p. 345)	更新了 Trusted Advisor Priority 控制台： • 确认和忽略按钮取代了接受和拒绝按钮。 • 您无需输入职位名称或姓名便可确认、解决、忽略或重新打开建议。 有关更多信息，请参阅 Trusted Advisor Priority 入门。	2023 年 2 月 16 日
AWS Support 代码示例更新 (p. 345)	新增的 .NET、Java 和 Kotlin 代码示例显示如何将 AWS Support 与 AWS 软件开发工具包（SDK）一起使用。如需了解更多信息，请参阅为 AWS Support 使用 AWS 软件开发工具包的代码示例。	2023 年 1 月 16 日
更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2023 年 1 月 10 日
更新了 AWS Support App 的文档 (p. 345)	您可以使用筛选条件选项或按案例 ID 进行搜索，在 Slack 中搜索支持案例。有关更多信息，请参阅在 Slack 中搜索支持案例。	2022 年 12 月 29 日
更新了 AWS Support App 的文档 (p. 345)	您也可以使用 Terraform 为 AWS Support App 创建您的资源。有关更多信息，请参阅使用 Terraform 创建 AWS Support App 资源。	2022 年 12 月 22 日
更新了 Trusted Advisor 的文档 (p. 345)	为 M Amazon emoryDB、亚马逊ElastiCache和添加了三项新的容错检查。AWS CloudHSM有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2022 年 12 月 15 日

更新了 Slack 中的 AWS Support App 文档 (p. 345)	您现在可以为以下选项请求实时聊天支持： • 账户和账单案例。 • 为技术支持案例提供日语支持。 • 有关更多信息，请参阅在 Slack 通道中创建支持案例。	2022 年 12 月 14 日
更新了 AWS Support 的文档 (p. 345)	新增了有关 AWS Support API 新端点的文档。有关更多信息，请参阅关于 AWS Support API。	2022 年 12 月 14 日
添加了用于 Slack 中 AWS Support App 的 AWS CloudFormation 模板文档 (p. 345)	您可以使用 CloudFormation 模板为 AWS Organizations 中的 AWS 账户 创建 Slack 配置工作区和通道。有关更多信息，请参阅使用 AWS CloudFormation 创建 AWS Support App 资源。	2022 年 12 月 5 日
更新了 Trusted Advisor 的文档 (p. 345)	新增了两项 AWS Resilience Hub 的容错能力检查。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2022 年 11 月 17 日
在 Trusted Advisor 中增加了 AWS Security Hub 结果的文档 (p. 345)	从 Trusted Advisor 中快速删除来自 Security Hub 控件的检查结果。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2022 年 11 月 17 日
更新了 AWS Trusted Advisor 的文档 (p. 345)	添加了 Trusted Advisor 建议文档。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2022 年 11 月 16 日
更新了 Slack 中的 AWS Support App 文档 (p. 345)	新增了日语支持文档。有关更多信息，请参阅在 Slack 通道中创建支持案例。	2022 年 11 月 11 日
更新了 AWS Support 计划的文档 (p. 345)	添加了故障排除信息，可允许在组织中访问 Support 计划。有关更多信息，请参阅故障排除。	2022 年 11 月 9 日
更新了 Slack 中的 AWS Support App 文档 (p. 345)	添加了 `supportapp` 权限的文档。有关更多信息，请参阅 AWS Support App 连接到 Slack 所需的权限。	2022 年 11 月 1 日
更新了 Slack 中的 AWS Support App 文档 (p. 345)	您可以使用 `RegisterSlackWorkspaceForOrganization` API 操作为您的 AWS 账户 注册 Slack 工作区。要调用此 API，您的账户必须是 AWS Organizations 中的组织的一部分。有关更多信息，请参阅 Slack API 中的 AWS Support App 参考。	2022 年 10 月 19 日

更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2022 年 10 月 4 日
更新了 Support Plans 文档 (p. 345)	您现在可以使用 AWS Identity and Access Management（IAM）来管理权限以更改 AWS 账户 的支持计划。有关更多信息，请参阅以下主题： • 管理 AWS Support Plans 的访问权限 • 适用于 AWS Support Plans 的 AWS 托管策略 • 更改 AWS Support Plans • 使用 AWS CloudTrail 记录 AWS Support Plans API 调用	2022 年 9 月 29 日
更新了 Slack 中的 AWS Support App 文档 (p. 345)	新增了有关如何配置公有或专用通道以用于 AWS Support App 的文档。有关更多信息，请参阅 Configuring a Slack channel（配置 Slack 通道）。	2022 年 9 月 22 日
更新了 AWS Support 的文档 (p. 345)	新增了有关您的支持案例安全性的新章节。有关更多信息，请参阅 AWS Support 案例的安全性。	2022 年 9 月 9 日
更新了 Trusted Advisor 的文档 (p. 345)	新增了 Amazon EC2 安全性检查。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2022 年 9 月 1 日
更新了 Slack 中的 AWS Support App 文档 (p. 345)	请参阅以下主题： 您可以使用 AWS Support App 管理您的支持案例、请求增加服务限额并通过 Slack 通道直接与支持座席聊天。有关更多信息，请参阅 Slack 中的 AWS Support App 文档。 您可以将 AWS 托管策略附加到您的 IAM 角色上，以便使用 AWS Support App。有关更多信息，请参阅适用于 Slack 中的 AWS Support App 的 AWS 托管策略。 更新了 AWS Support App 的 API 参考。请参阅 AWS Support App API 参考。	2022 年 8 月 24 日
更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2022 年 8 月 17 日

添加了 Trusted Advisor Priority 的文档 (p. 345)	Trusted Advisor Priority 新增了对以下功能的支持： • 委派管理员 • 有关建议摘要的每日和每周电子邮件通知 • 重新打开已解决或已拒绝的建议 • AWS 托管策略 有关更多信息，请参阅 Trusted Advisor Priority 入门。	2022 年 8 月 17 日
更新了 Trusted Advisor 的文档 (p. 345)	Trusted Advisor 控制台中的 Preferences（首选项）页面进行了更新。有关更多信息，请参阅 AWS Trusted Advisor 入门。	2022 年 7 月 15 日
更新了 Trusted Advisor 的文档 (p. 345)	更新了检查以包含以下信息： • Alert Criteria（提醒条件） • Recommended Action（建议的操作） • 其他资源 • Report columns（报告列） 有关更多信息，请参阅 AWS Trusted Advisor 检查参考。	2022 年 7 月 7 日
更新了 AWS Support 的文档 (p. 345)	添加了介绍如何管理您的支持案例的文档。 • 更新现有的支持案例 • 故障排除	2022 年 6 月 28 日
更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	更新了为服务相关角色提供账单、管理和支持服务的权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2022 年 6 月 23 日
更新了 Trusted Advisor 的文档 (p. 345)	Trusted Advisor 支持源自 AWS Security Hub 的其他 AWS 基础安全最佳实践安全标准控件。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2022 年 6 月 23 日
更新了 Trusted Advisor 的文档 (p. 345)	添加了有关如何请求增加服务限额的更多信息。有关更多信息，请参阅服务限制。	2022 年 6 月 21 日
更新了 AWS Support 的文档 (p. 345)	Support 中心控制台中的工单创建体验已经更新。有关更多信息，请参阅创建支持工单和工单管理。	2022 年 5 月 18 日

更新了 Trusted Advisor 的文档 (p. 345)	增加了适用于 Amazon EBS 和 AWS Lambda 的四项检查。有关更多信息，请参阅启用 AWS Compute Optimizer 以增加 Trusted Advisor 检查。	2022 年 5 月 4 日
更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2022 年 4 月 27 日
更新了有关已泄露的访问密钥检查的文档 (p. 345)	此检查现在将自动为您刷新。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2022 年 4 月 25 日
更新了 Trusted Advisor 的文档 (p. 345)	容错类别中的 AWS Direct Connect 检查已更新。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2022 年 3 月 29 日
更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2022 年 3 月 14 日
添加了 Trusted Advisor Priority 的文档 (p. 345)	您可以使用 Trusted Advisor Priority 查看技术客户经理 (TAM) 提供的优先建议列表。有关更多信息，请参阅 Trusted Advisor Priority 入门。	2022 年 2 月 28 日
更新了有关使用亚马逊EventBridge的文档 Trusted Advisor (p. 345)	您可以创建 EventBridge 规则以监控对 Trusted Advisor 检查的更改。有关更多信息，请参阅 通过 EventBridge 监控 AWS Trusted Advisor 的检查结果。	2022 年 2 月 21 日
关于使用亚马逊EventBridge监控AWS Support案例的新文档 (p. 345)	您可以创建 EventBridge 规则以监控和接收有关您支持案例的通知。有关更多信息，请参阅使用 EventBridge 来监控 AWS Support 案例。	2022 年 2 月 21 日
更新了 AWSSupportServiceRolePolicy 的文档 (p. 345)	增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 AWS 托管策略：AWSSupportServiceRolePolicy。	2022 年 2 月 17 日
增加了有关与 AWS Security Hub 集成的文档 (p. 345)	现在，您可以在 Trusted Advisor 控制台中查看 AWS 基础安全最佳实践安全标准中的 Security Hub 控件检查结果。有关更多信息，请参阅在 AWS Trusted Advisor 控制台中查看 AWS Security Hub 控件。	2022 年 1 月 18 日

更新了 Trusted Advisor 的文档 (p. 345)	为运行 Microsoft SQL Server 的 Amazon EC2 实例添加了三项新的检查。 • 适用于 Microsoft SQL Server 的 Amazon EC2 实例整合 • 使用 Microsoft SQL Server 的 Amazon EC2 实例超限预置 • 使用终止支持版本的 Microsoft SQL Server 的 Amazon EC2 实例 有关更多信息，请参阅 AWS Trusted Advisor 检查参考。	2021 年 12 月 20 日
更新了 Trusted Advisor 的文档 (p. 345)	Trusted Advisor 增加了四项新的 AWS Well-Architected 检查 • AWS Well-Architected 成本优化高风险问题 • AWS Well-Architected 性能高风险问题 • AWS Well-Architected 安全性高风险问题 • AWS Well-Architected 可靠性高风险问题 有关更多信息，请参阅 AWS Trusted Advisor 检查参考。	2021 年 12 月 20 日
已更新的文档 (p. 345)	如果您拥有 Enterprise On-Ramp Support 计划，则可以访问所有的 Trusted Advisor 检查和 AWS Support API。	2021 年 11 月 24 日
更新了 Trusted Advisor 的文档 (p. 345)	Trusted Advisor 为 Amazon Comprehend 添加了两个新的检查。有关更多信息，请参阅 AWS Trusted Advisor 检查参考。	2021 年 9 月 29 日
更新了 Trusted Advisor 的文档 (p. 345)	更新了 Amazon OpenSearch Service Reserved Instance Optimization 的检查名称。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2021 年 9 月 8 日
更新了 Trusted Advisor 检查的文档 (p. 345)	增加了所有 Trusted Advisor 检查的参考主题。有关更多信息，请参阅 AWS Trusted Advisor 检查参考。	2021 年 9 月 1 日
更新了 Trusted Advisor 托管策略的文档 (p. 345)	更新了 Trusted Advisor 托管策略的文档 有关更多信息，请参阅 AWS Support 和 AWS Trusted Advisor 的 AWS 托管策略。	2021 年 8 月 10 日

更新了 Trusted Advisor 的文档 (p. 345)	更新了 Trusted Advisor 控制台的文档。有关更多信息，请参阅 AWS Trusted Advisor 入门。	2021 年 7 月 16 日
更新了创建 AWS Support 案例的文档 (p. 345)	增加了有关如何为永久关闭的案例创建相关支持案例的文档。有关更多信息，请参阅重新打开已关闭的案例和创建相关案例。	2021 年 6 月 8 日
更新了 Trusted Advisor 的文档 (p. 345)	Trusted Advisor 增加了两个 Amazon Elastic Block Store (Amazon EBS) 卷存储的新检查。有关更多信息，请参阅更改 AWS Trusted Advisor 检查的日志。	2021 年 6 月 8 日
已更新的文档 (p. 345)	更新了以下主题： • 在 “创建亚马逊CloudWatch警报以监控AWS Trusted Advisor指标” 主题中更新了程序并添加了内容 • 增加了 AWS Support API 的服务限额部分	2021 年 5 月 12 日

早期更新

更改	说明	日期
更新了 Trusted Advisor 的文档	增加了用于筛选、刷新和下载检查结果的文档。有关详细信息，请参阅以下章节： • 筛选您的检查 (p. 23) • 刷新检查结果 (p. 24) • 下载检查结果 (p. 24)	2021 年 3 月 16 日
更新了有关 AWS 托管策略的文档	增加了有关 `AWSSupportServiceRolePolicy` AWS 托管策略的信息。有关更多信息，请参阅将服务相关角色用于 AWS Support (p. 197)：	2021 年 3 月 16 日
增加了 AWS Lambda 的检查	在 AWS Trusted Advisor 的更改日志 (p. 145) 中增加了 Lambda 的 4 个 AWS Trusted Advisor 检查。	2021 年 3 月 8 日
更新了 Amazon Elastic Block Store 的服务限制检查	在 AWS Trusted Advisor 的更改日志 (p. 145) 中更新了 Amazon EBS 的 5 个 AWS Trusted Advisor 检查。	2021 年 3 月 5 日
更新了 CloudTrail 日志记录的文档	CloudTrail 支持在您更改 AWS Support 计划时对控制台操作进行日志记录。有关更多信息，请参阅记录对您的 AWS Support 计划的更改 (p. 324)：	2021 年 2 月 9 日
更新了 Trusted Advisor 的文档	更新了 开始使用 Trusted Advisor 建议 (p. 19) 主题。	2021 年 1 月 29 日
更新了 Trusted Advisor 报告的文档	增加了将 Trusted Advisor 报告与其他 AWS 服务结合使用的 问题排查 (p. 45) 部分。	2020 年 12 月 4 日

更改	说明	日期
增加了对 AWS CloudTrail 日志记录的 AWS Trusted Advisor 支持	CloudTrail 支持对 Trusted Advisor 控制台操作的子集进行日志记录。有关更多信息，请参阅使用 AWS CloudTrail 记录 AWS Trusted Advisor 控制台操作 (p. 337)：	2020 年 11 月 23 日
增加了更改日志主题	查看对 AWS Trusted Advisor 的更改日志 (p. 145) 中的 AWS Trusted Advisor 检查和类别的更改。	2020 年 11 月 18 日
增加了对组织单位的支持	您现在可以为组织单位 (OU) 的 Trusted Advisor 检查创建报告。有关更多信息，请参阅创建组织视图报告 (p. 30)：	2020 年 11 月 17 日
使用 AWS CloudTrail 主题更新了日志记录	增加了 Trusted Advisor API 操作的示例日志条目。请参阅 CloudTrail 日志记录中的 AWS Trusted Advisor 信息 (p. 315)。	2020 年 10 月 22 日
增加了 AWS Support 配额	增加了有关 AWS Support 的当前配额和限制的信息。请参阅 AWS 一般参考 中的 AWS Support 端点和限额。	2020 年 8 月 4 日
AWS Trusted Advisor 的组织视图	您现在可以为属于 AWS Organizations 部分的账户的 Trusted Advisor 检查创建报告。请参阅AWS Trusted Advisor 的组织视图 (p. 29)。	2020 年 7 月 17 日
安全性和 AWS Support	更新了有关使用 AWS Support 和 Trusted Advisor 时的安全注意事项的信息。请参阅 AWS Support 中的安全性 (p. 190)	2020 年 5 月 5 日
安全性和 AWS Support	添加了有关使用 AWS Support 时的安全注意事项的信息。	2020 年 1 月 10 日
使用 Trusted Advisor 即 Web 服务	添加了有关在获取 Trusted Advisor 检查的列表后刷新 Trusted Advisor 的更新说明。	2018 年 11 月 1 日
使用服务相关角色	增加了新部分。	2018 年 7 月 11 日
入门：问题排查	增加了 Route 53 和 AWS Certificate Manager 的问题排查链接。	2017 年 9 月 1 日
案例管理示例：创建案例	为拥有“基本”支持计划的用户添加了有关 CC 框的注释。	2017 年 8 月 1 日
使用CloudWatch事件监控Trusted Advisor检查结果	增加了新部分。	2016 年 11 月 18 日
案例管理	更新了案例严重性等级的名称。	2016 年 10 月 27 日
使用 AWS CloudTrail 记录 AWS Support 调用	增加了新部分。	2016 年 4 月 21 日
入门：问题排查	增加了更多问题排查链接。	2015 年 5 月 19 日
入门：问题排查	增加了更多问题排查链接。	2014 年 11 月 18 日
入门：案例管理	已更新，以反映 AWS Management Console 中的服务目录。	2014 年 10 月 30 日

更改	说明	日期
AWS Support 案例生命周期编程	增加了有关新 API 元素的信息，通过这些元素可为案例添加附件并在检索案例历史记录时省略案例通信信息。	2014 年 7 月 16 日
访问 AWS Support	删除了指定支持联系人的访问方式。	2014 年 5 月 28 日
入门	增加了“入门”章节。	2013 年 12 月 13 日
初次发布	发布了新的 AWS Support 服务。	2013 年 4 月 30 日

AWS 词汇表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。