亚马逊云科技

用户指南

Amazon Web Services 支持

API 版本 2026-01-12

Amazon Web Services 支持: 用户指南

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

Table of Contents

入门 Amazon Web Services 支持

Amazon Web Services 支持 提供了一系列计划，提供工具和专业知识，为 Amazon 解决方案的成功和运营健康提供支持。所有支持计划都提供对客户服务、 Amazon 文档、技术论文和支持论坛的 round-the-clock访问权限。要获得技术支持和更多用于规划、部署和改善 Amazon 环境的资源，您可以为自己的 Amazon 用例选择支持计划。

> **注意**
>
> - 要创建 Amazon Web Services 支持 交互以使用 AI 生成的疑难解答来解决您的问题，并可选择创建支持案例，请参阅Support Center 控制台中的 AI 增强型故障排除。
> - 有关不同 Amazon Web Services 支持 计划的更多信息，请参阅比较 Amazon Web Services 支持 计划和更改 Amazon Web Services 支持 计划。
> - 支持计划可为您的支持案例提供不同的响应时间。请参阅选择初始支持案例严重性级别和了解 Amazon Web Services 支持 响应时间。

主题

Support Center 控制台中的 AI 增强型故障排除

支持 Amazon Web Services 区域中提供了 AI 增强型故障排除功能，可帮助您更快、更高效地解决问题。如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则可以使用 Support Center Console 中的功能来解决技术问题以及账户和账单问题。如果您有基本 Amazon Web Services 支持 套餐，则可以使用 Support Center Console 中的功能来解决一般问题，并获得有关账户和账单问题的帮助。使用 AI 增强型故障排除可使用情境感知和自动诊断为您的环境提供有针对性的解决方案，从而简化支持体验。 Amazon

以下内容 Amazon Web Services 区域支持在 Support Center 控制台中进行人工智能增强型故障排除：

- US East (N. Virginia) Region
- 美国东部（俄亥俄州）区域
- 欧洲地区（爱尔兰）区域

> **Note**
>
> 如果您在 S Amazon Web Services 区域 upport Center Console 中不支持 AI 增强功能的环境中操作，那么您将使用传统的案例管理方法。有关更多信息，请参阅 传统体验：创建支持案例和案例管理。

当您访问 Support Center Console 时，您可以用自然语言输入问题描述，导入相关的 Amazon Q 对话，接收生成式 AI 疑难解答指南，并在需要时选择创建带有预填字段的支持案例。

您可以提供有关您的环境和问题的情境信息，以便在整个故障排除过程中获得个性化的解决方案。

Amazon Web Services 支持 控制台中的 AI 增强型故障排除具有以下主要优势：

- 更快地解决问题：描述问题后立即获得回复和相关解决方案。
- 上下文保存：导入您之前的 Amazon Q 对话以维护故障排除背景。
- 简化案例创建：使用自然语言描述问题，而不是浏览多个表单字段。
- 智能跟进：根据您的特定 Amazon 环境接收相关的后续问题。

有关 Support 计划中可用功能的完整列表，请参阅比较 Amazon Web Services 支持 计划。

> **注意**
>
> - 要更改您的支持计划，请参阅 更改 Amazon Web Services 支持 计划。
> - 要关闭您的账户，请参阅《Amazon Billing 用户指南》中的关闭账户。
> - 要查找的常见疑难解答主题 Amazon Web Services 服务，请参阅资源问题排查。
> - 如果您是属于的客户 Amazon Partner ，并且您使用 Resold Support Amazon Partner Network，请 Amazon Partner 直接与您联系以解决任何与账单相关的问题。 Amazon Web Services 支持 无法协助解决 Resold Support 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：
>   - Amazon 合作伙伴如何确定组织中的 Amazon Web Services 支持 计划

- 由Amazon Partner主导的支持

> **Important**
>
> 在开启支持互动或创建支持案例之前，请访问您的 a Amazon Health Dashboard t home#/，查看是否有影响您的账户资源的事件 https://phd.aws.amazon.com/phd/ #/。尽管发布事件可能会稍有延迟，但您可以在控制面板中验证任何 Amazon Web Services 服务 问题。如果您不确定是否存在活跃的事件，请提交支持案例。

主题

设置权限以使用 AI 增强型故障排除

要在 Support Center 中访问 AI 增强型疑难解答功能，您需要特定的 Amazon Identity and Access Management 权限。本节介绍必要的 IAM 权限，并说明如何对其进行配置，以便您可以充分利用这些功能。

人工智能增强型故障排除需要传统支持案例管理之外的权限。所需的权限分为三类：

- 支持互动权限：在 Support Center 中启用新的基于交互的工作流程。
- 人工智能驱动的分类权限：允许访问人工智能驱动的问题分类功能。
- Amazon Q 集成权限：允许从 Amazon Q 开发者导入对话。

这些权限是对您现有 Amazon Web Services 支持 权限的补充，不会取而代之。

您可以通过两种方式设置 AI 增强型故障排除的权限：

选项 1：使用 Amazon 托管策略（推荐）。将`AWSSupportAccess`托管策略附加到您的用户或角色。此政策包括所有必需的权限，并在发布新 Amazon Web Services 支持 功能时自动更新。

选项 2：创建具有最低所需权限的自定义策略。这种方法为您提供了更多的控制权，但在添加新功能时需要手动更新。

选项 1：使用 Amazon 托管策略（推荐）

如果您当前已附加 AWSSupport访问管理策略，则无需其他权限。但是，要继续使用 Support C enter Console API 中包含的功能，您必须在 2026 年 6 月 1 日之前将支持中心控制台操作添加到您的 IAM 策略中（如果您还没有）。为此，请更新 Amazon Web Services 支持 托管策略以包含`support-console:*`操作。有关更多信息，请参阅 为支持中心控制台 API 操作添加 IAM 策略。

选项 2：创建具有最低所需权限的自定义策略

您可以明确允许列出特定的操作，而不必使用通配符。以下是支持互动、案例创建和案例管理所需的权限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:CreateCase",
        "support:DescribeAttachment",
        "support:DescribeCaseAttributes",
        "support:DescribeCases",
        "support:DescribeCommunication",
        "support:DescribeCommunications",
        "support:DescribeCreateCaseOptions",
        "support:DescribeIssueTypes",
        "support:DescribeServices",
        "support:DescribeSeverityLevels",
        "support:DescribeSupportedLanguages",
        "support:DescribeSupportLevel",
        "support:GetInteraction",
        "support:InitiateCallForCase",
        "support:ListInteractionEntries",
        "support:ListInteractions",
        "support:InitiateChatForCase",
```

```
        "support:PutCaseAttributes",
        "support:ResolveCase",
        "support:ResolveInteraction",
        "support:SearchForCases",
        "support:StartInteraction",
        "support:UpdateInteraction",
        "support-console:GetAccountState",
        "support-console:GetAccountGovCloudEnabled",
        "support-console:GetCaseDraft",
        "support-console:CreateCaseDraft",
        "support-console:DeleteCaseDraft",
        "support-console:GetBanner",
        "support-console:DescribeDynamicHelp",
        "support-console:CreateContact",
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> 随着新功能的 Amazon Web Services 支持 发布，使用自定义策略需要持续维护。有关 Support Center 控制台 API 操作的更多信息，请参阅为支持中心控制台 API 操作添加 IAM 策略。有关每个 Amazon Web Services 支持 API 操作的更多信息，请参阅管理对 Cent Amazon Web Services 支持 er 的访问权限。

集成 Amazon Q 所需的权限

要使用 Support Center 中的 Amazon Q 对话导入功能，IAM 身份需要获得以下 Amazon Q 开发者操作的权限：

- `q:StartConversation`: 与 Amazon Q. 开始新的对话
- `q:SendMessage`: 在对话中发送消息。
- `q:GetConversation`: 检索对话详情。访问控制台需要执行此操作。
- `q:ListConversations`：列出可用的对话。访问控制台和 Support Center 集成需要执行此操作。

Amazon Q 与 Support Center Console 的集成特别要求您q:ListConversations有权显示您最近的对话以供导入。有关配置 Amazon Q 开发者权限的详细指南，请参阅 Amazon Q 开发者权限参考和使用策略管理对 Amazon Q 开发者的访问权限。

为支持互动应用所需的权限

要向您的 IAM 用户应用权限，请完成以下步骤：

1. 登录 Amazon Web Services 管理控制台 并打开 IAM 控制台，网址为https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择策略，然后选择创建策略。
3. 选择 JSON 选项卡，然后粘贴前几节中提到的其中一个政策文档。
4. 选择 “下一步：标签”，然后选择 “下一步：审阅”。
5. 输入策略名称（例如），SupportConsoleInteractionsAccess并提供描述以解释该策略的用途。
6. 选择创建策略。
7. 将策略附加到需要访问 Support Center 的 IAM 用户、群组或角色。

如果您已有 A AWSSupport ccess 托管策略附件，请将补充自定义策略与托管策略一起附上。

创建支持互动

支持互动是您开始互动的方式 Amazon Web Services 支持。您首先使用自然语言描述问题，然后使用人工智能增强型故障排除获得量身定制的帮助。您的初始互动可能包括澄清问题、情境解决方案和自动解决问题，而无需创建支持案例。如果需要，这些互动可以独立解决问题，也可以作为人类工程师循环处理支持案例的基础。

Amazon Web Services 支持 互动与支持案例的不同之处在于，支持案例包括与 Cloud Support 工程师的互动。您可以选择根据之前的支持互动自动生成支持案例。该支持案例保留了从最初的支持互动开始的所有背景信息，并包括人工智能生成的其他见解，以帮助 Cloud Support 工程师解决您的问题。将人工智能增强型故障排除与 Amazon Cloud Support Engineers 的帮助相结合，有可能更快地解决问题并缩短停机时间。

> **注意**
>
> - 在 Support Center Console 顶部的横幅中选择 “使用旧体验”，可以恢复到传统的案例管理方法。有关更多信息，请参阅 传统体验：创建支持案例和案例管理。

- 您可以以 Amazon Identity and Access Management (IAM) 用户身份登录 Support Center 控制台。有关更多信息，请参阅 管理对 Cent Amazon Web Services 支持 er 的访问权限。
- 如果您无法登录 Support Center 控制台并创建支持案例，则可以改用 “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。

要开始支持互动，请完成以下步骤：

1. 登录到 Amazon Support Center Console。

   > **Tip**
   >
   > 在中 Amazon Web Services 管理控制台，您还可以选择问号图标 ( ) ，然后选择 Su pport Center。

2. 您可以通过多种方式开始支持互动：

   - 输入有关您需要帮助的问题的详细信息。这就是您开始新的支持互动的方式。输入有关您的问题以及您已采取的任何故障排除步骤的详细信息。
   - 继续现有的支持互动：从 “描述你的问题” 或 “继续” 部分中显示的最近一次支持互动中进行选择。本节显示了最近的两次支持互动。访问查看过去的支持互动部分，查看过去的其他支持互动。
   - 使用 Amazon Q 笔录：在文本字段中选择 Amazon Q 图标可查看最近的 Amazon Q 对话列表。显示了 Amazon GovCloud （美国东部） Amazon Web Services 区域 最近的五次对话。或者，从 “描述您的问题” 中显示的最近 Amazon Q 互动中进行选择，或者继续。选择对话时，会生成该对话的摘要并将其添加到文本框中。如果您选择 Amazon Q 对话，则会看到有关 Amazon Web Services 区域 用户可访问性的免责声明。

3. 选择文本字段右下角的 “发送” 图标。

4. Amazon Web Services 支持 生成式 AI 驱动的故障排除可分析您的查询以及您的特定 Amazon 环境。系统可能会提示您提供其他信息以帮助进行分析。如果您看到提示您输入其他信息，请输入请求的数据，然后选择提交。如果您不知道或无法访问所请求的信息，则可以跳过此步骤，改为收到一般指导回复。请记住，一般指导回复并不针对您的 Amazon 环境。

   分析完成后，您将看到结果摘要以及补救步骤。要查看分析和修正步骤中使用的来源，请选择来源。

5. 如果您需要进一步的帮助，可以完成以下选项之一：

   - 继续使用 AI 辅助支持：要进一步完善 AI 辅助分析并生成新的响应，请选择添加更多详细信息以获得更好的响应。在 “其他详细信息” 字段中输入信息，然后选择 “提交”。请记住，此选项用于为原始问题提供更多背景信息。如果您需要为新问题输入上下文，请选择屏幕顶部或底部的开始新互动。
   - 创建支持案例：要使用创建支持案例 Amazon Web Services 支持，请选择创建案例。此选项启动案例创建工作流程。许多案例详细信息会根据您的支持互动自动填充。您可以根据需要更改此信息。您的支持互动（包括所提供的任何解决步骤的详细信息）已添加到支持案例中。有关如何创建支持案例的详细信息，请参阅通过支持互动创建支持案例。

在整个支持互动过程中，您可以随时使用 “竖起大拇指” 和 “大拇指向下” 图标来提供有关您的体验的反馈。

通过支持互动创建支持案例

当您在支持互动期间选择 “创建案例” 时，将为您创建一个支持案例，其中包含许多案例详细信息，例如主题、描述、案例类型、服务、类别和严重性级别。您可以根据需要更改此信息。请务必查看此信息以确保准确性。有关如何为案例选择严重级别的信息，请参阅选择初始支持案例严重级别。

> **Important**
>
> 在创建支持案例之前，请访问您的账户，查看是否有影响您的账户资源的事件。您可以在控制面板中验证任何 Amazon Web Services 服务 问题。发布事件可能会稍有延迟。如果您不确定是否存在活跃的事件，请提交支持案例。

选择 “创建案例” 后，输入或验证以下信息：

1. 验证此支持案例的主题。主题简要概述了您的支持互动内容。
2. 验证描述。您的初始询问将显示在 “描述” 字段中。根据需要修改此信息。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。
3. （可选）选择附加文件以向案例添加任何相关文件，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。
4. 对于案例类型，请选择以下选项之一：

   - 账户和计费

- 技术
- 服务配额。您只能从 Support Center 控制台请求增加某些类型的服务配额。有关更多信息，请参阅 请求提升服务配额。

> **Note**
>
> 如果您有基本 Amazon Web Services 支持 计划，则无法创建技术支持案例。

5. 验证服务、类别和严重性。
6. 在 “通信偏好” 部分，指明您想 Amazon 如何与您沟通。您可以选择以下选项之一：

   a. 电子邮件：收到对您的电子邮件的回复。

   b. 电话：接听支持代理的电话。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]

   c. 聊天：与支持人员开始实时聊天。如果您无法连接到聊天，请参阅 问题排查。

   （可选）如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则可以在其他联系人中输入最多 10 个额外的电子邮件地址。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。如果您使用根账户的电子邮件地址和密码登录，则无需包含您的电子邮件地址。

   > **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，在 “我的账户” 页面的 “备用联系人” 部分中指定的运营联系人会收到案例信函的副本，但仅限于账户和账单等特定案例类型。

7. 准备好提交支持案例时，选择提交。您将被引导至案例详情页面，您可以在其中查看您的案例详情、支持互动和案例信函。

   选择案例详细信息以查看有关您的案例的信息，例如附件或严重级别。选择 S u pport 互动查看与此案例相关的支持互动。

Enterprise Support 案例的最佳做法和目标响应时间

在创建支持案例之前，请访问您的账户，查看是否有影响您的账户资源的事件。您可以在控制面板中验证任何 Amazon Web Services 服务 问题。发布事件可能会稍有延迟。如果您不确定是否存在活跃的事件，请提交支持案例。

创建支持案例时，请确保选择正确的严重性级别并提供尽可能多的信息。有关应提供何种信息的更多信息，请参阅以下 E nterprise Support 案例最佳实践部分。

使用以下矩阵来帮助您确定正确的严重性。

对于严重或紧急情况，请务必留下联系方式，以便我们在需要时与您联系。

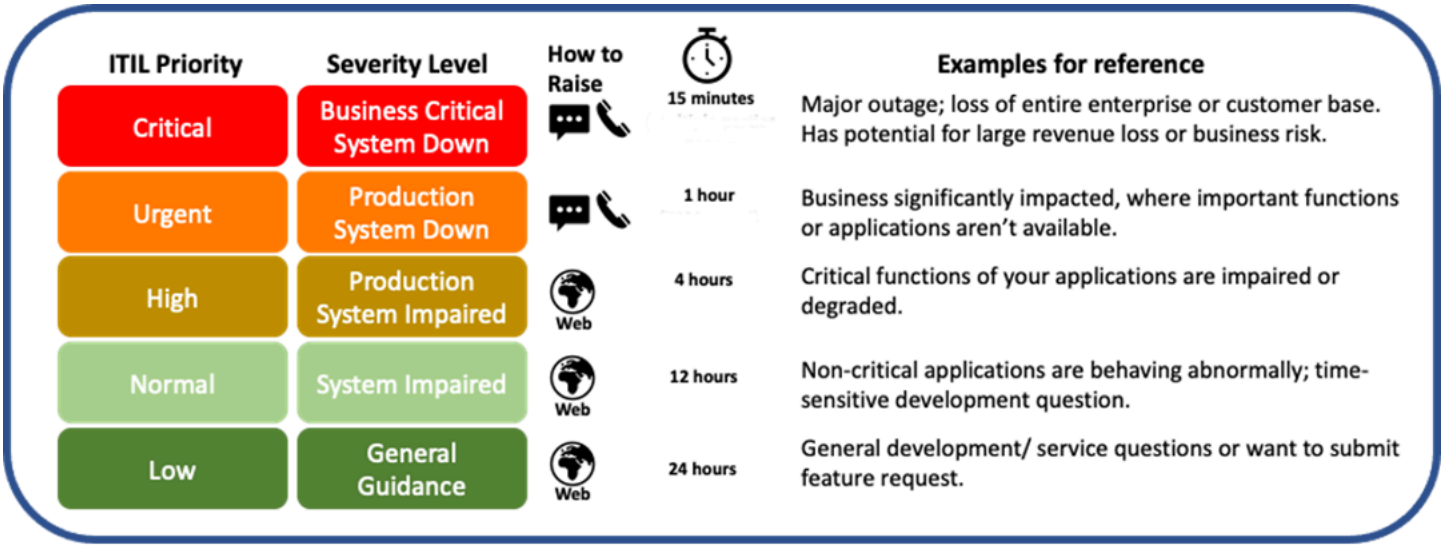
> **Note**
>
> 获取帮助的最快方法是使用 “聊天” 或 “电话” 联系方式。

主题

- Enterprise Support 案例目标响应
- 企业 Support 最佳做法
- 企业 Support 上报路径

Enterprise Support 案例目标响应

下图显示了不同案例严重性级别的目标 Amazon Web Services 支持 响应时间。



企业 Support 案例最佳实践

在适当的严重级别提交您的支持案例。

- 适当的严重级别有助于确保您的案例在各处可见， Amazon 并允许 TAM 管理您的问题。
- 每个事件或问题只提交一个案例。
- 确保你以正确的方式提出案例 Amazon Web Services 账户。

提供尽可能多的详细信息，回答以下列表中提供的相关问题：

- 谁：谁做了什么？ 谁受到影响？ 谁应该被圈进去？ 你已经和谁谈过了？
- 什么：到底发生了什么。冲击或爆炸半径是多少？ 你已经尝试过什么来解决这个问题？
- 时间：何时发生或何时发生（ 日期、时间、时区 ）？ 你什么时候需要答案？
- 其中： Amazon Web Services 区域、可用区、特定实例或资源 IDs以及其他标识符。
- 为什么：你为什么要开这个案例（ 信息、限额提高、事件分析或 RCA、中断 ）？
- 如何：包括有关如何重现问题、如何上报以及如何与您联系的信息。

> **Note**
>
> 创建支持案例后，您可以更改其严重性。有关信息，请参阅更改支持案例的严重性级别。

Enterprise Support 关键业务或生产系统停机

- 对于关键业务系统停机或生产系统停机情况，请使用 “聊天” 或 “电话”，并确保组织中有人员可以处理案例。
- 清楚地描述问题，包括你尝试了什么、你的期望和背景。总结业务影响。
- 提供（或开始捕获）尽可能多的指标、时间和症状。更多的数据意味着更快的诊断。
- 提供会议桥接器。打开关键业务系统停机问题时，请为支持团队提供会议桥以帮助解决问题。由于关键业务系统的停机问题是生产停机，因此最好让所有人通电话，并制定共同的行动计划以寻求解决方案。
- 确保在支持案例中捕获与事件相关的所有活动（来自控制台的更新，而不是通过电子邮件进行更新）。电话选项适用于实时通信；但是，请确保在支持案例中记录更新和结果。

企业 Support 上报路径

遇到问题时，您可以按照以下 step-by-step步骤操作。

1. Amazon Health Dashboard如果您认为问题可能与异常 Amazon Web Services 服务 操作有关，请@@ 检查。
2. 按照上述 “Support Case 最佳实践” 部分所述@@ 评估案例信息。
3. 如果需要快速响应，请选择适当的严重性并使用 “电话” 或 “聊天”。
4. 如果您需要其他帮助或者没有得到预期的回复，请@@ 联系您的 TAM。

查看支持互动

与过去的互动 Amazon Web Services 支持 可保存 10 年。您可以通过选择列表图标在 Amazon Web Services 支持 控制面板中查看过去的互动。然后，选择要查看的互动。 Amazon Web Services 支持 互动详情随即出现。如果您选择通过互动创建支持案例，则该互动将不再出现在您过去的互动列表中。现在，互动将显示在关联支持案例的案例详情页面中。

您可以向交互添加其他详细信息以生成新的响应。或者，您可以通过在互动详情屏幕上选择创建案例，选择通过 Amazon Web Services 支持 互动创建案例。 Amazon Web Services 支持

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。

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 Amazon Web Services 支持：
  - 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 Amazon Web Services 支持 使用电子邮件或电话联系方式进行联系。

案例管理

> **Note**
>
> 在 Support Center 控制台顶部的横幅中选择 “使用旧体验”，可以恢复到传统的案例管理方法。有关更多信息，请参阅 传统体验：创建支持案例和案例管理。

在中 Amazon Web Services 管理控制台，您可以在以下位置创建三种类型的客户案例 Amazon Web Services 支持：

- 所有 Amazon 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 Amazon 客户使用。有关默认服务配额（以前称为限制）的信息，请参阅 Amazon Web Services 一般参考 中的 Amazon 服务配额。
- 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 Amazon Web Services 支持 计划。
> - 要关闭账户，请参阅 Amazon Billing 用户指南中的关闭账户。

- 要查找的常见疑难解答主题 Amazon Web Services 服务，请参阅资源问题排查。
- 如果您是属于的客户 Amazon Partner ，并且您使用 Resold Support Amazon Partner Network，请 Amazon Partner 直接与您联系以解决任何与账单相关的问题。 Amazon Web Services 支持 无法协助解决 Resold Support 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：
  - Amazon 合作伙伴如何确定组织中的 Amazon Web Services 支持 计划
  - 由Amazon Partner主导的支持

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。

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。

选择初始支持案例严重性级别

创建支持案例时，请确保定义了正确的严重性并提供尽可能多的信息。

您可能希望按照您的支持计划所允许的最高严重性创建支持案例。但最佳做法是，仅当案例无法解决或直接影响生产应用程序时，才选择最高严重性。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 Amazon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

- 如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则可以重新分配支持案例的严重性级别，以反映紧急程度和业务影响的变化。例如，您可以将支持案例从系统受损更改为生产系统受损。当您更改案例严重性时，Amazon Web Services 支持 会收到通知并根据新的严重性级别路由案例。有关更多信息，请参阅 更改支持案例的严重性级别。
- 如果您有基本 Amazon Web Services 支持 计划，则在创建支持案例后无法更改其严重性级别。如果您的情况发生变化，请与 Amazon Web Services 支持 代理合作。
- 有关严重性级别的更多信息，请参阅 Amazon Web Services 支持 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。（B Amazon usiness Support+、 Amazon 企业支持或 Amazon 统一运营计划）
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。（B Amazon usiness Support+、 Amazon 企业支持或 Amazon 统一运营计划）
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。（B Amazon usiness Support+、 Amazon 企业支持或 Amazon 统一运营计划）
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。（B Amazon usiness Support+、Amazon 企业支持或 Amazon 统一运营计划）
业务关键系统停机	critical	• Amazon 商业支持+：少于 30 分钟 • Amazon Enterprise Support：不到 15 分钟 • Amazon 统一运营：事件管理	您的业务面临危险。您的应用程序的关键功能不可用。

严重性	严重性级别代码	第一响应时间	说明和支持计划
		工程师讲述 5 分钟	

了解 Amazon Web Services 支持 响应时间

Amazon Web Services 支持 尽一切合理努力在指定的时间范围内回复您的初始请求。有关每个 Amazon Web Services 支持 计划的支持范围的信息，请参阅Amazon Web Services 支持 功能。

如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则 round-the-clock可以获得技术支持。

> **Note**
>
> 如果您选择日语作为支持案例的首选联系语言，则可以获得如下日语支持：
>
> - 如果您需要非技术支持案例的客户服务，或者您有开发人员支持计划并需要技术支持，则可以在日本的工作时间内提供日语支持，该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 B Amazon usiness Support+、En Amazon terprise Suppor Amazon t 或 Unified Operations 计划，则可以全天候提供日语技术支持。
>
> 如果您选择中文作为支持案例的首选联系语言，则可能提供以下中文支持：
>
> - 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（GMT+8）提供支持，节假日和周末除外。
> - 如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划，则可以全天候提供中文技术支持。
>
> 如果您选择韩语作为支持案例的首选联系语言，则可以获得如下韩语支持：
>
> - 如果您需要非技术支持案例的客户服务，则可以在韩国的工作时间内提供韩语支持，该工作时间定义为韩国标准时间（GMT+9）上午 09:00 至下午 06:00，节假日和周末除外。

- 如果您有 B Amazon usiness Support+、En Amazon terprise Suppor Amazon t 或 Unified Operations 计划，则可以全天候提供韩语技术支持。

更改支持案例的严重性级别

如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则可以重新分配支持案例的严重性级别，以反映紧急程度和业务影响的变化。例如，您可以将支持案例从系统受损更改为生产系统受损。当您更改案例严重性时， Amazon Web Services 支持 会收到通知并根据新的严重性级别处理案例。

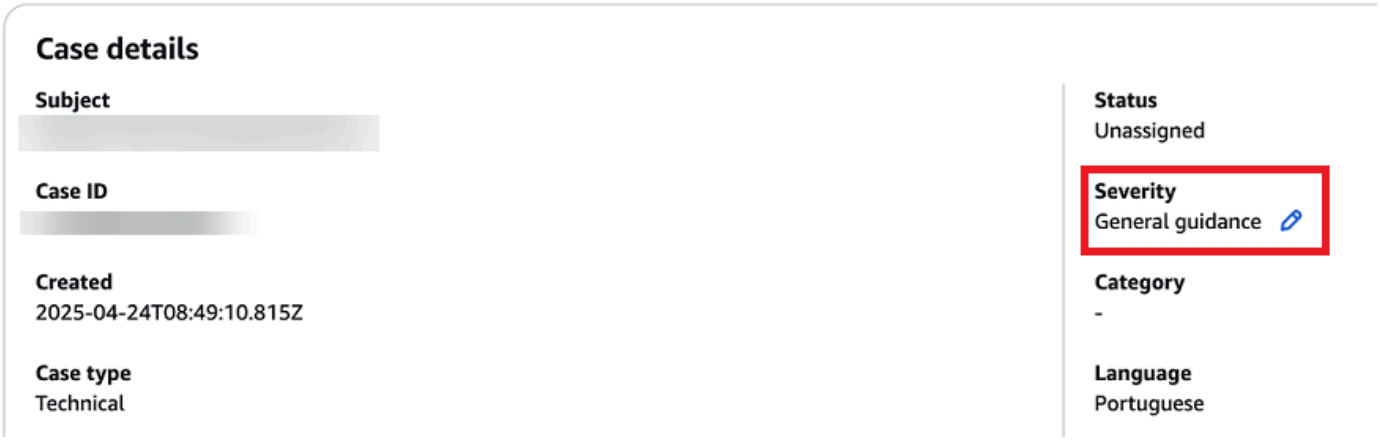
> **Note**
>
> 使用这些语言创建的日语 (JP) 账户或账单、服务配额增加请求 (SQIR) 和土耳其语 (TR) 账户或账单案例具有默认严重性，无法更改。

要更改支持案例的严重性，请完成以下步骤：

1. 登录到 Amazon Support Center Console。

   > **Tip**
   >
   > 在中 Amazon Web Services 管理控制台，您还可以选择问号图标 ( ) ，然后选择 Su pport Center。

2. 选择要更改其严重性级别的案例。
3. 在案例详细信息中，选择严重性字段旁边的铅笔图标，如以下示例所示。

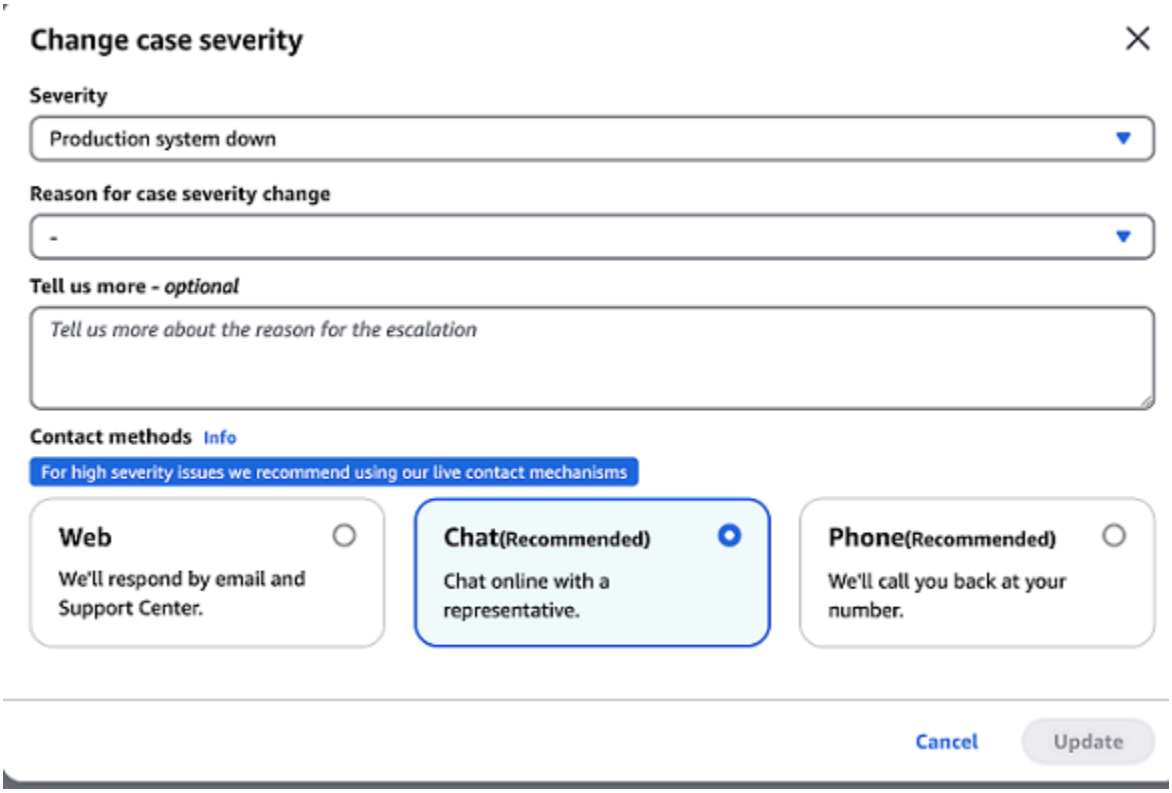


4. 对于严重性，请从以下选项中选择新的严重性级别：

   - 一般指导
   - 系统受损
   - 生产系统受损
   - 生产系统停机
   - 业务关键系统停机

5. 对于案例严重性更改原因，请从可用选项中进行选择，说明您更改案例严重性的原因。
6. （可选）在补充说明中，输入有关此更改的其他信息。
7. 请执行以下操作之一：

   - 如果您要降低支持案例的严重性，或者要将其从一般指导提升至系统受损或生产系统受损，请选择更新。
   - 如果您要将严重性提高到生产系统关闭或关键业务系统关闭，请使用 “联系方式” 部分中的一个选项进行互动 Amazon Web Services 支持，然后选择 “更新”。以下示例显示了联系方式部分中可用的选项。



Note

- 如果将支持案例的严重性升级为生产系统宕机或业务关键系统宕机，则必须等待 60 分钟后，方可再次更改严重性。
- 如果您的支持案例当前设置为关键业务系统关闭，则系统会提示您与之进行实时联系，Amazon Web Services 支持 而不是指定更高的严重性。
- 如果您在至少已升级过一次支持案例严重性级别的情况下，再次尝试提升级别，可能会遇到等待期。例如，如果您在早上 6:00 将严重性从系统受损更改为生产系统受损，则支持案例将遵循生产系统受损严重性级别对应的 4 小时首次响应时间规则。在此场景下，您需等到上午 10:00（即 4 小时窗口期结束后），方可再次升级该案例的严重性级别。有关各严重性级别的首次响应时间列表，请参阅了解 Amazon Web Services 支持 响应时间中的表格。

请求提升服务配额

您可以请求增加服务配额（以前称为“限额”）以满足您的工作负载要求。

使用服务配额服务直接请求增加服务配额。有关更多信息，请参阅以下文档：

- 《服务配额用户指南》中的什么是服务配额？
- 《服务配额用户指南》中的 Requesting a quota increase

目前，Service Quotas 不支持全部 Amazon Web Services 服务 服务配额 Amazon Web Services 区域。如果您的 Amazon Web Services 服务 或在 S ervice Quotas 控制台中 Amazon Web Services 区域 不可用，请完成以下步骤以创建请求增加配额的支持案例：

1. 登录到 Amazon Support Center Console。

   > **Tip**
   >
   > 在中 Amazon Web Services 管理控制台，您还可以选择问号图标 ( ) ，然后选择 Su pport Center。

2. 在 Su pport 互动页面上，输入有关此次提高服务限额的详细信息。出现提示时，选择创建案例。许多 Amazon Web Services 支持 案例字段将预先填充您在互动期间输入的文本。您可以根据需要编辑这些字段。有关创建支持互动的更多详细信息，请参阅创建支持互动。
3. 对于案例类型，选择服务配额。
4. 对于 “服务”，选择 “提高服务限制”。
5. 在 “类别” 中，从列表中选择您要请求的加价类型。此处仅列出 Support Center 中提供的服务限制提高请求。有关其他类型的服务限制请求，请参阅 Servic e Quotas 用户指南中的请求增加配额。
6. （可选）从 “首选联系语言” 下拉列表中，选择与您通信时 Amazon Web Services 支持 要使用的语言。
7. 在 “区域” 中，选择您申请加薪 Amazon Web Services 区域 的地点。

   > **Note**
   >
   > Amazon Web Services 区域 如果您选择 “常规” 作为 “类别”，则选择不可用。

8. （可选）要请求多次增加限额，请选择添加另一个限额，然后选择另一个 Amazon Web Services 区域。
9. 为本次或多次增加服务配额输入描述。如有需要，您可以附加文件。
10. 选择下一步：立即解决或联系我们。
11. 在联系选项中，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。
- 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]

12. 准备好提交支持案例时，选择提交。您将被引导至案例详情页面，您可以在其中查看您的案例详情、支持互动和案例信函。

    选择案例详细信息以查看有关您的案例的信息，例如附件或严重级别。选择 S u pport 互动查看与此案例相关的支持互动。

传统体验：创建支持案例和案例管理

> **Important**
>
> 在 Support Center 控制台顶部的横幅中选择 “使用旧体验”，可以恢复到传统的案例管理方法。

在中 Amazon Web Services 管理控制台，您可以在以下位置创建三种类型的客户案例 Amazon Web Services 支持：

- 所有 Amazon 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 Amazon 客户使用。有关默认服务配额（以前称为限制）的信息，请参阅 Amazon Web Services 一般参考 中的 Amazon 服务配额。
- 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 Amazon Web Services 支持 计划。
> - 要关闭账户，请参阅 Amazon Billing 用户指南中的关闭账户。
> - 要查找的常见疑难解答主题 Amazon Web Services 服务，请参阅资源问题排查。

- 如果您是属于的客户 Amazon Partner ，并且您使用 Resold Support Amazon Partner Network，请 Amazon Partner 直接与您联系以解决任何与账单相关的问题。 Amazon Web Services 支持 无法协助解决 Resold Support 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：
  - Amazon 合作伙伴如何确定组织中的 Amazon Web Services 支持 计划
  - 由Amazon Partner主导的支持

创建支持案例

您可以在 Amazon Web Services 管理控制台的支持中心创建支持案例。

> **注意**
>
> - 您可以以 Amazon Identity and Access Management (IAM) 用户身份登录 Support Center。有关更多信息，请参阅 管理对 Cent Amazon Web Services 支持 er 的访问权限。
> - 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 Amazon Support Center Console。

   > **Tip**
   >
   > 在中 Amazon Web Services 管理控制台，您还可以选择问号图标 ()，然后选择 Su pport Center。

2. 选择创建案例。
3. 请选择以下选项之一：
   - 账户和计费
   - 技术
   - 要增加服务配额，请选择想要增加服务配额？，然后按照请求提升服务配额的说明操作。

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：
     - Amazon Web Services 管理控制台
     - Amazon Command Line Interface (Amazon 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。
    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）以清除您的支持案例草稿。

12. （可选）如果您有 B Amazon usiness Support+、En Amazon terprise Suppor Amazon t 或统一运营计划，则会出现“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。

选择初始支持案例严重性级别

您可能希望按照您的支持计划所允许的最高严重性创建支持案例。但最佳做法是，仅当案例无法解决或直接影响生产应用程序时，才选择最高严重性。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 Amazon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**
>
> - 如果您拥有 Enterprise Support 或 Enterprise On-Ramp 计划，则可以重新指定支持案例的严重性级别，以反映紧急程度和业务影响的变化。例如，您可以将支持案例从系统受损更改为生产系统受损。当您更改案例严重性时， Amazon Web Services 支持 会收到通知并根据新的严重性级别路由案例。有关更多信息，请参阅 更改支持案例的严重性级别。

- 如果您没有 Enterprise Support 或 Enterprise On-Ramp 计划，则在创建支持案例后无法更改其严重性级别。如果您的情况发生变化，请与支持 Amazon Web Services 支持 人员合作处理您的支持案例。
- 有关严重性级别的更多信息，请参阅 Amazon Web Services 支持 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、B Amazon usiness Support+、Enter Amazon prise Support 或 Amazon 统一运营计划）
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、B Amazon usiness Support+、Enter Amazon prise Support 或 Amazon 统一运营计划）
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。（B Amazon usiness Support+、 Amazon 企业支持或 Amazon 统一运营计划）
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。（B Amazon usiness Support+、Amazon 企业支持或 Amazon 统一运营计划）
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。

了解 Amazon Web Services 支持 响应时间

Amazon Web Services 支持 尽一切合理努力在指定的时间范围内回复您的初始请求。有关每个 Amazon Web Services 支持 计划的支持范围的信息，请参阅Amazon Web Services 支持 功能。

如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则 round-the-clock可以获得技术支持。*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 Amazon Web Services 管理控制台中的 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，则可以获得如下日语支持：

- 如果您需要非技术支持案例的客户服务，或者您有开发人员支持计划并需要技术支持，则可以在日本的工作时间内提供日语支持，该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 B Amazon usiness Support+、En Amazon terprise Suppor Amazon t 或 Unified Operations 计划，则可以全天候提供日语技术支持。

如果您选择中文作为支持案例的首选联系语言，则可以获得如下中文支持：

- 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（GMT+8）提供支持，节假日和周末除外。
- 如果您有开发人员支持计划，则在我的账户中设置的工作时间内提供中文技术支持，该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。对于跨多个时区的国家/地区，工作时间可能不尽相同。
- 如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划，则可以全天候提供中文技术支持。

如果您选择韩语作为支持案例的首选联系语言，则可以获得如下韩语支持：

- 如果您需要非技术支持案例的客户服务，则可以在韩国的工作时间内提供韩语支持，该工作时间定义为韩国标准时间（GMT+9）上午 09:00 至下午 06:00，节假日和周末除外。
- 如果您有开发人员支持计划，则在我的账户中设置的工作时间内提供韩语技术支持，该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。对于跨多个时区的国家/地区，工作时间可能不尽相同。
- 如果您有 B Amazon usiness Support+、En Amazon terprise Suppor Amazon t 或 Unified Operations 计划，则可以全天候提供韩语技术支持。

更改支持案例的严重性级别

如果您拥有 Enterprise Support 或 Enterprise On-Ramp 计划，则可以重新指定支持案例的严重性级别，以反映紧急程度和业务影响的变化。例如，您可以将支持案例从系统受损更改为生产系统受损。当您更改案例严重性时， Amazon Web Services 支持 会收到通知并根据新的严重性级别处理案例。

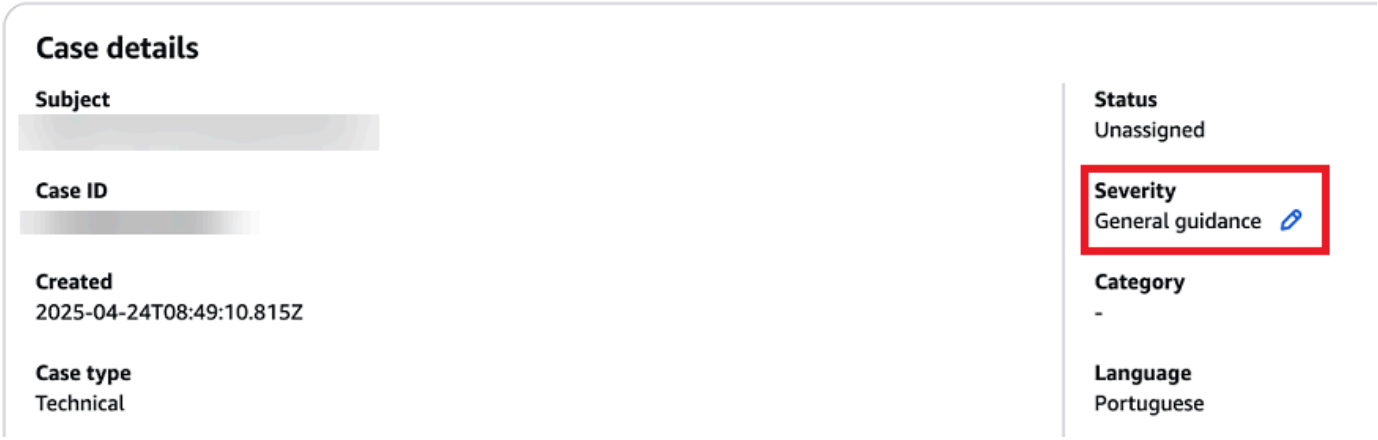
> **Note**
>
> 使用这些语言创建的日语 (JP) 账户或账单、服务配额增加请求 (SQIR) 和土耳其语 (TR) 账户或账单案例具有默认严重性，无法更改。

要更改支持案例的严重性，请完成以下步骤：

1. 登录到 Amazon Support Center Console。

   > **Tip**
   >
   > 在中 Amazon Web Services 管理控制台，您还可以选择问号图标 ( ) ，然后选择 Su pport Center。

2. 选择要更改其严重性级别的案例。
3. 在案例详细信息中，选择严重性字段旁边的铅笔图标，如以下示例所示。



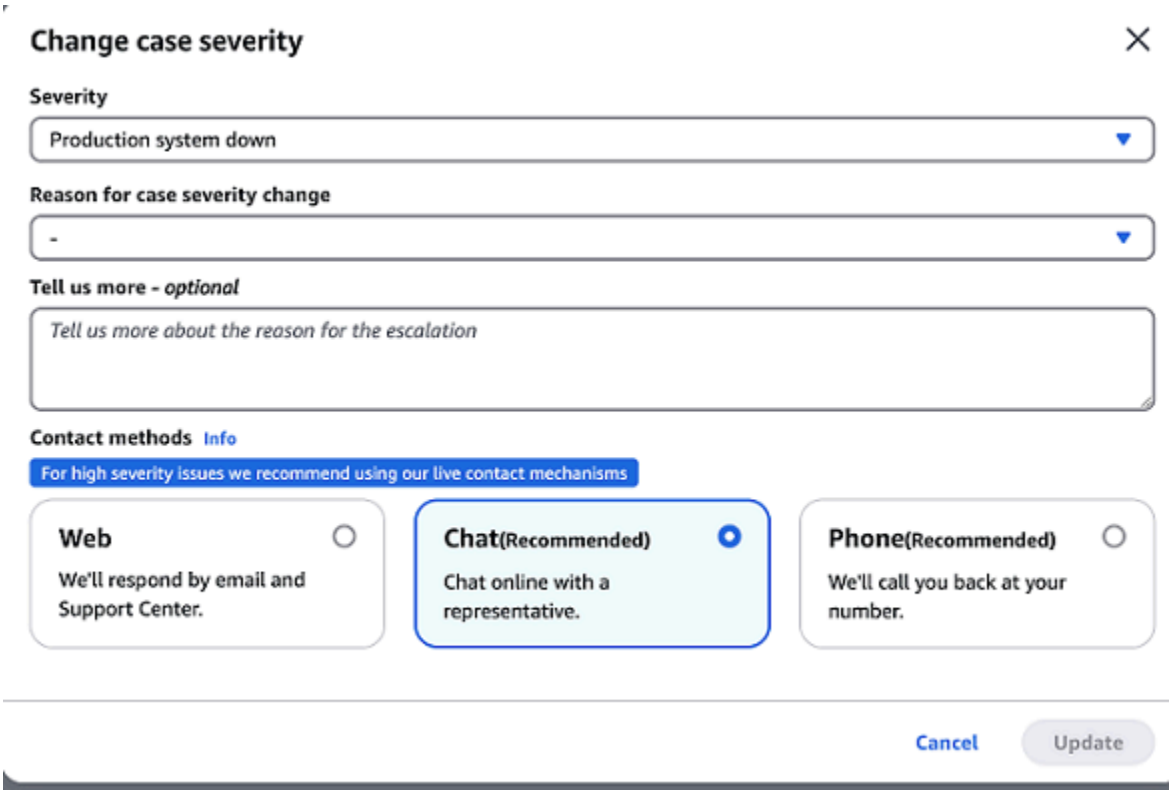
4. 对于严重性，请从以下选项中选择新的严重性级别：

   - 一般指导
   - 系统受损

- 生产系统受损
- 生产系统停机
- 业务关键系统停机

5. 对于案例严重性更改原因，请从可用选项中进行选择，说明您更改案例严重性的原因。
6. （可选）在补充说明中，输入有关此更改的其他信息。
7. 请执行以下操作之一：

- 如果您要降低支持案例的严重性，或者要将其从一般指导提升至系统受损或生产系统受损，请选择更新。
- 如果您要将严重性提高到生产系统关闭或关键业务系统关闭，请使用 “联系方式” 部分中的一个选项进行互动 Amazon Web Services 支持，然后选择 “更新”。以下示例显示了联系方式部分中可用的选项。

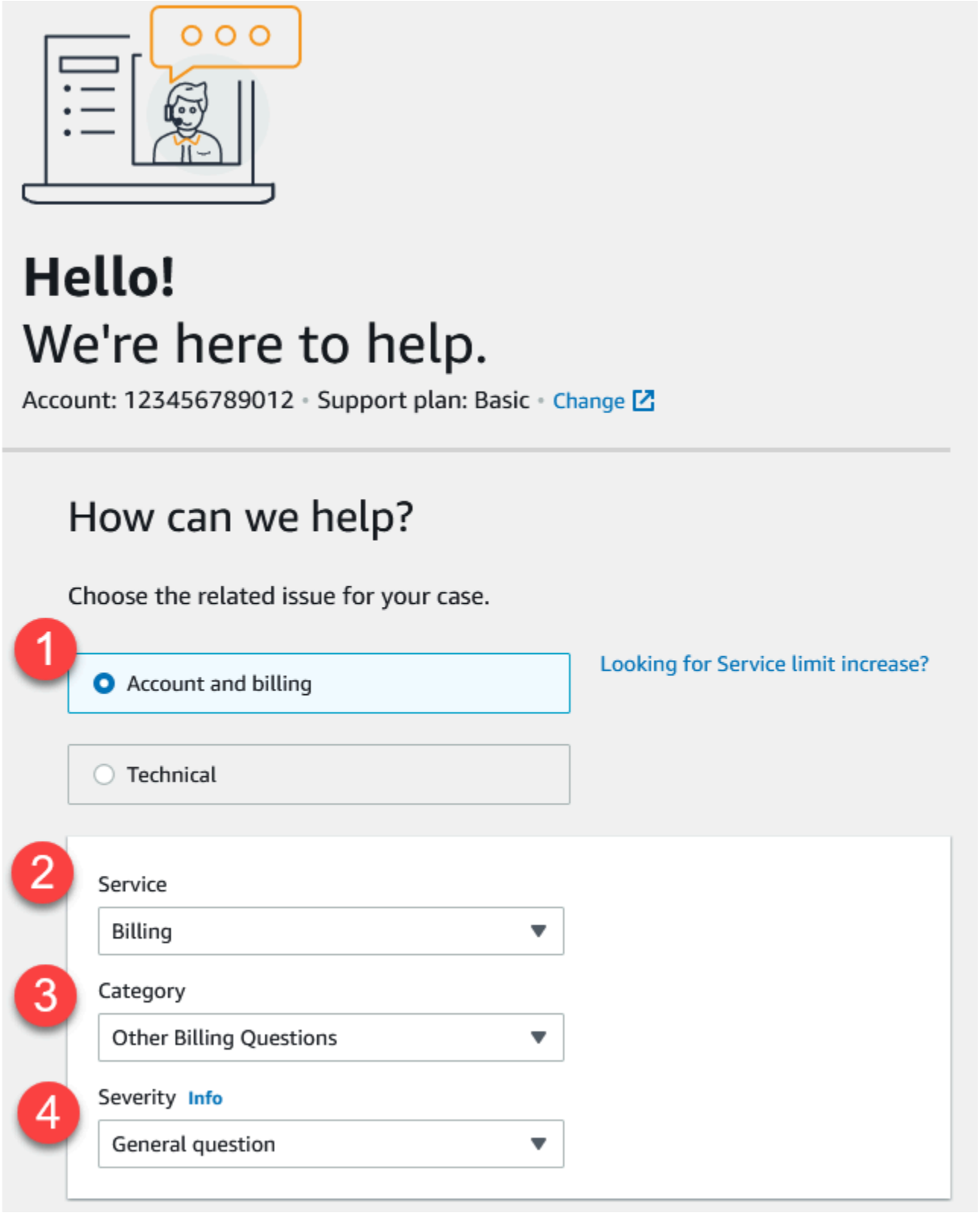


> **Note**
>
> - 如果将支持案例的严重性升级为生产系统宕机或业务关键系统宕机，则必须等待 60 分钟后，方可再次更改严重性。

- 如果您的支持案例当前设置为关键业务系统关闭，则系统会提示您与之进行实时联系，Amazon Web Services 支持 而不是指定更高的严重性。
- 如果您在至少已升级过一次支持案例严重性级别的情况下，再次尝试提升级别，可能会遇到等待期。例如，如果您在早上 6:00 将严重性从系统受损更改为生产系统受损，则支持案例将遵循生产系统受损严重性级别对应的 4 小时首次响应时间规则。在此场景下，您需等到上午 10:00（即 4 小时窗口期结束后），方可再次升级该案例的严重性级别。有关各严重性级别的首次响应时间列表，请参阅了解 Amazon Web Services 支持 响应时间中的表格。

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）。

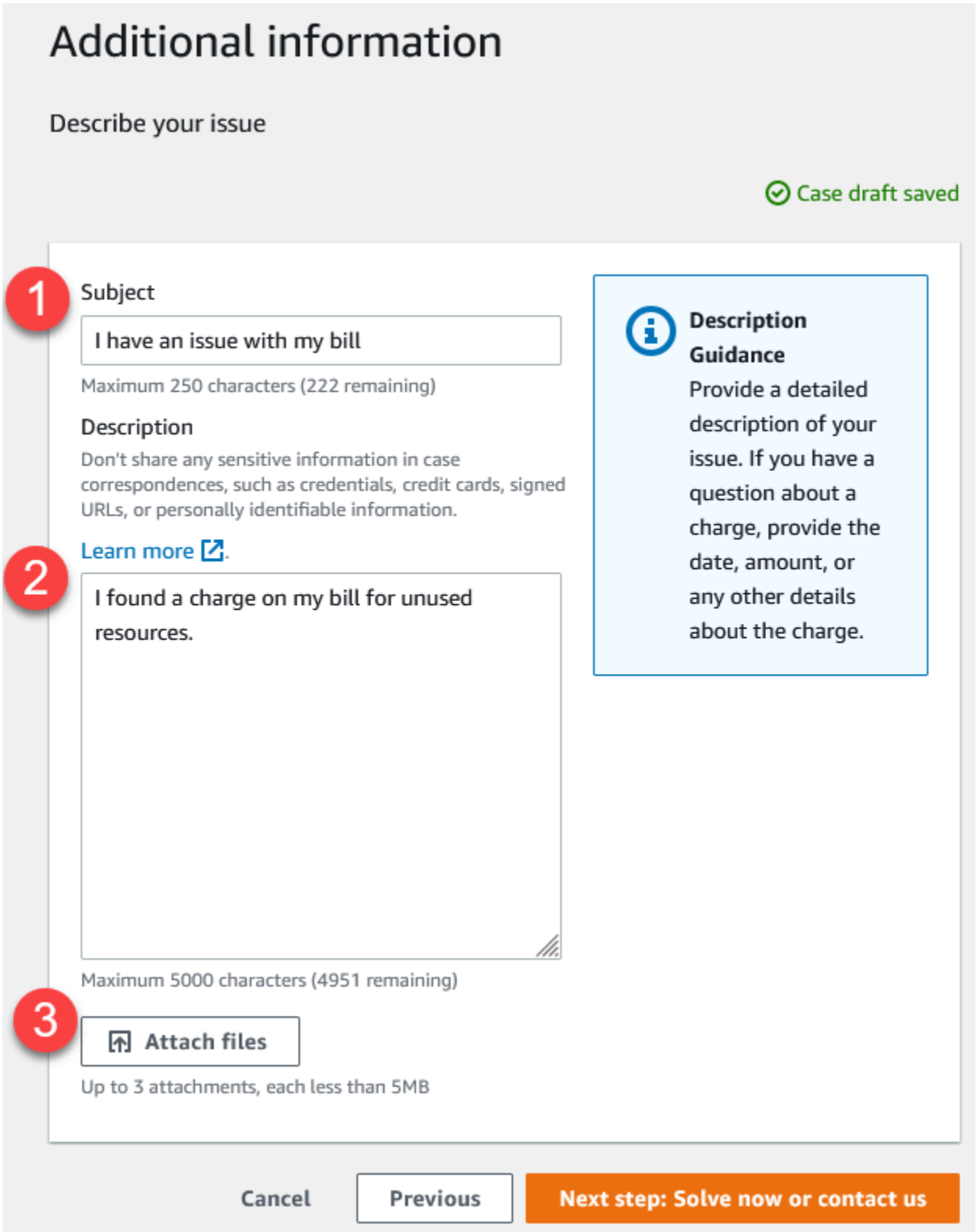
> **Note**
>
> 如果您拥有“基本”支持计划，则无法创建技术支持案例。

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）。

   响应时间是指来自的第一次响应 Amazon Web Services 支持. 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 选择初始支持案例严重性级别。

   > **Note**
   >
   > 根据您所选择的类别，系统可能会提示您提供更多信息。

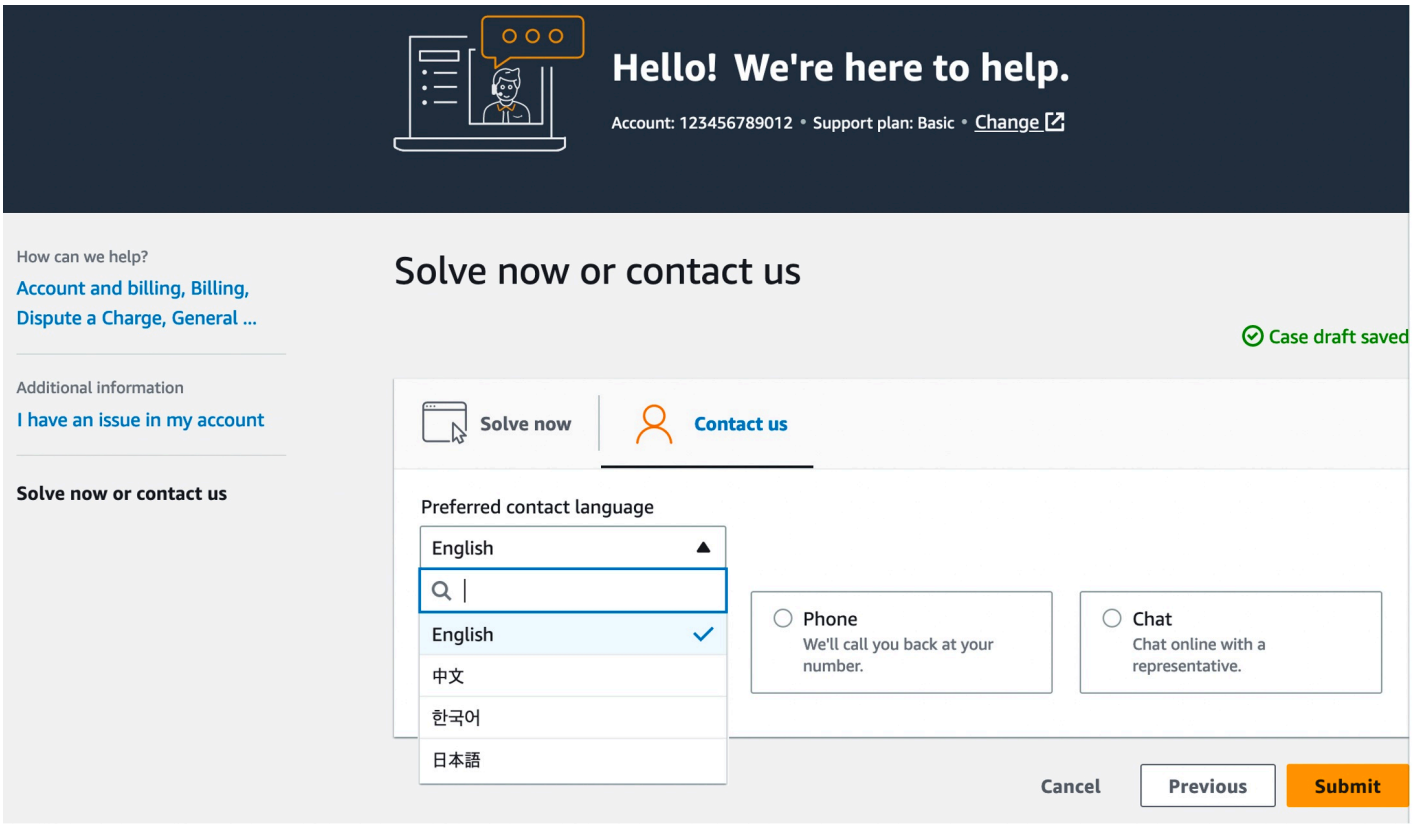
在指定案例类型和分类后，可以指定描述以及希望与您联系的方式。



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。这是您提供给的最重要的信息 Amazon Web Services 支持。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。
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。您最多可以附加三个文件。每个文件最大可为 5 MB。

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。您的支持计划将以您的首选语言显示自定义的联系选项。
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，则可以获得如下日语支持：

- 如果您需要非技术支持案例的客户服务，或者您有开发人员支持计划并需要技术支持，则可以在日本的工作时间内提供日语支持，该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 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划，则可以全天候提供日语技术支持。

如果您选择中文作为支持案例的首选联系语言，则可以获得如下中文支持：

- 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（GMT+8）提供支持，节假日和周末除外。
- 如果您有开发人员支持计划，则在我的账户中设置的工作时间内提供中文技术支持，该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。对于跨多个时区的国家/地区，工作时间可能不尽相同。
- 如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划，则可以全天候提供中文技术支持。

如果您选择韩语作为支持案例的首选联系语言，则可以获得如下韩语支持：

- 如果您需要非技术支持案例的客户服务，则可以在韩国的工作时间内提供韩语支持，该工作时间定义为韩国标准时间（GMT+9）上午 09:00 至下午 06:00，节假日和周末除外。
- 如果您有开发人员支持计划，则在我的账户中设置的工作时间内提供韩语技术支持，该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。对于跨多个时区的国家/地区，工作时间可能不尽相同。
- 如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划，则可以全天候提供韩语技术支持。

旧版体验：更新、解决和重新审理您的案例

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)）。

当您的问题更新后，您会收到一封电子邮件，其中包含通信内容以及指向该问题的 Support Center 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 Amazon Web Services 账户 提交支持案例的人。如果您以 Amazon 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 Cent Amazon Web Services 支持 er 的访问权限。
> - 如果您未在几天内回复 Amazon Web Services 支持 问题，则会自动解决问题。
> - 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。

主题

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。

> **Note**
>
> 如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则可以重新分配支持案例的严重性级别，以反映紧急程度和业务影响的变化。如果您没有上述任一支持计划，则无法更新案例的严重性。有关更多信息，请参阅选择初始支持案例严重性级别和更改支持案例的严重性级别。

更新现有的支持案例

1. 登录到 Amazon Support Center Console。

> **Tip**
>
> 在中 Amazon Web Services 管理控制台，您还可以选择问号图标
> ( )，
> 然后选择 Su pport Center。

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 Amazon Support Center Console。

> **Tip**
>
> 在中 Amazon Web Services 管理控制台，您还可以选择问号图标 ()，然后选择 Su pport Center。

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**
>
> 如果您的 Amazon Web Services 支持 问题已为您解决，则可以使用反馈链接提供有关您的体验的更多信息 Amazon Web Services 支持。

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。
> - 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 Amazon Support Center Console。

> **Tip**
>
> 在中 Amazon Web Services 管理控制台，您还可以选择问号图标 ()，然后选择 Su pport Center。

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

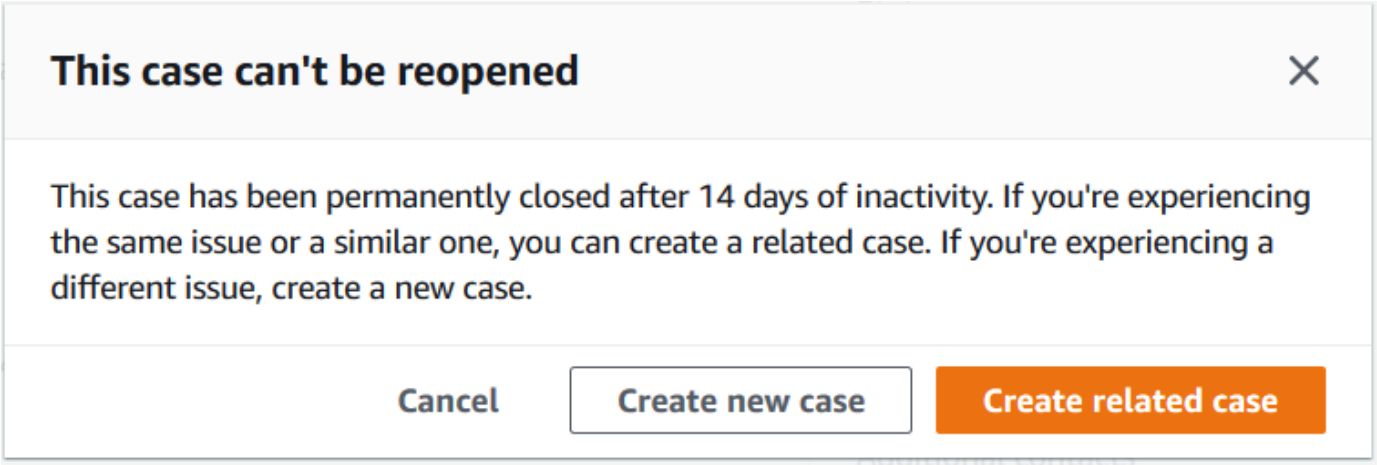
14 天处于不活动状态后，您将无法重新打开已解决的案例。如果您遇到与已解决案例相关的类似问题，您可以创建相关案例。此相关案例将包括指向先前解决的案例的链接，以便客服可以查看之前的案例详细信息和通信。如果您遇到的问题不同，我们建议您创建新案例。

要创建相关案例

1. 登录到 Amazon Support Center Console。

> **Tip**
>
> 在中 Amazon Web Services 管理控制台，您还可以选择问号图标 ()，然后选择 Su pport Center。

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）。

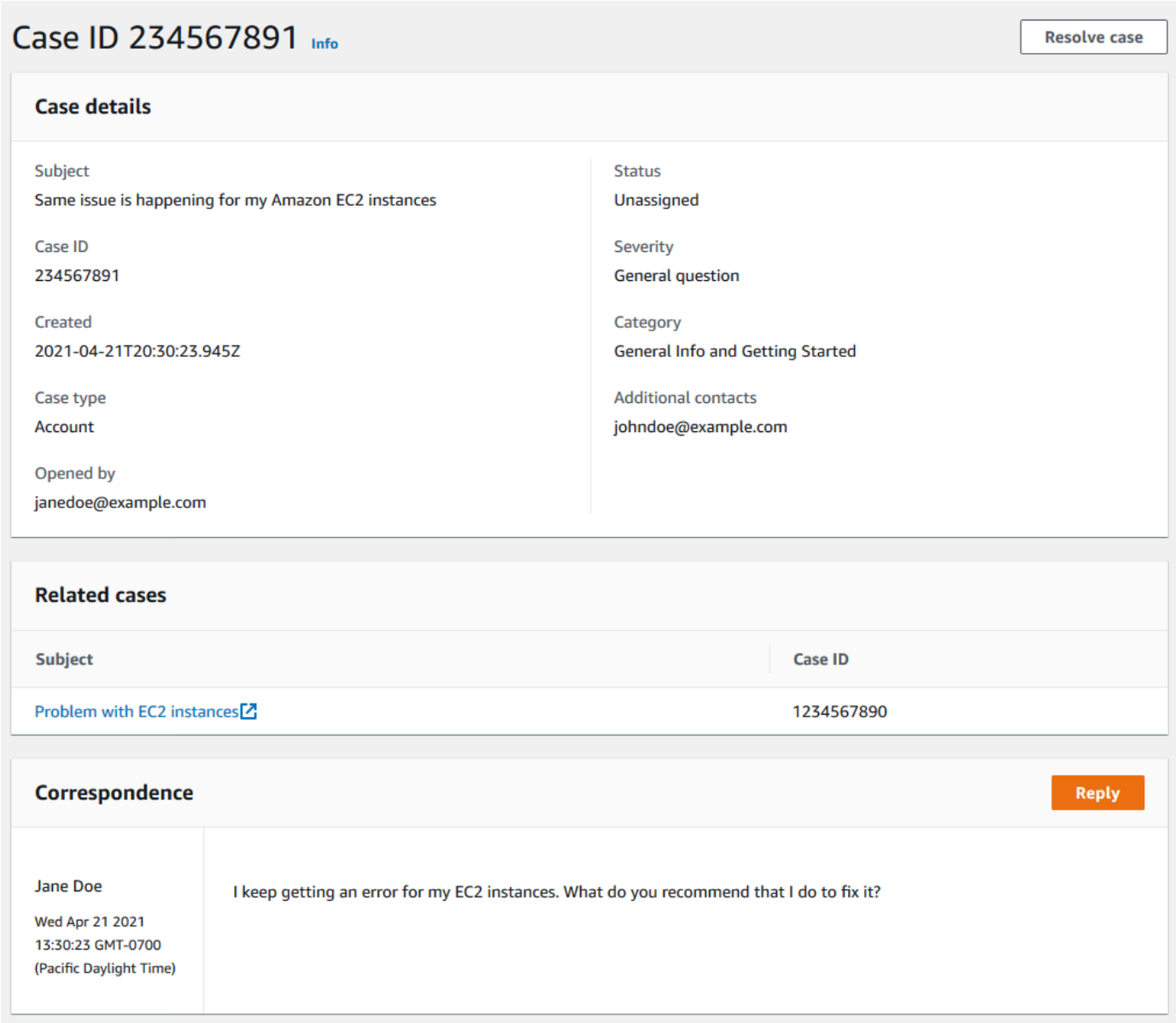


5. 按照同样的步骤创建您的案例。请参阅创建支持案例。

> **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。

Amazon Web Services 支持 与 Amazon SDK 一起使用

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

SDK 文档
Amazon CLI
适用于 Java 的 Amazon SDK
适用于 JavaScript 的 Amazon SDK
适用于 .NET 的 Amazon SDK
适用于 PHP 的 Amazon SDK
Amazon Tools for PowerShell
适用于 Python (Boto3) 的 Amazon SDK
适用于 Ruby 的 Amazon SDK
适用于 SAP ABAP 的 Amazon SDK

关于支持中心控制台 API

支持中心控制台 API 可增强您使用支持中心控制台的体验。支持中心控制台 API 提供的功能示例包括：

- 您能够创建并更新支持案例的草稿
- 支持中心控制台能够显示您账户的当前状态
- 支持中心控制台能够显示所选服务和类别的动态帮助

有关支持中心控制台 API 所提供的操作的完整列表，请参阅为支持中心控制台 API 操作添加 IAM 策略中的表格。

> **Important**
>
> 要继续使用支持中心控制台 API 中包含的功能，您必须在 2026 年 6 月 1 日之前将支持中心控制台操作添加到您的 Amazon Identity and Access Management 策略中。创建 IAM 策略后，请更新 Amazon Web Services 支持 托管策略以包含 `support-console:*` 操作。有关更多信息，请参阅 为支持中心控制台 API 操作添加 IAM 策略。

主题

为支持中心控制台 API 操作添加 IAM 策略

在 2026 年 6 月 1 日之前，您必须为支持中心控制台 API 操作创建 Amazon Identity and Access Management 策略。如果您未在 2026 年 6 月 1 日之前创建这些策略，将会收到 `AccessDenied` 错误。

要将这些操作添加到您的 IAM 策略中，请参阅Amazon Identity and Access Management 用户指南中的创建 IAM 策略（控制台）。

下表汇总了控制台操作。

> **Note**
>
> 这些操作仅适用于控制台。无法在 Amazon SDK 或 Amazon CLI 中使用。

操作	访问级别	描述
GetAccountState	READ	授予控制台显示当前账户状态的权限。
GetAccountGovCloudEnabled	READ	授予确定您的账户是否已启用 GovCloud 的权限。
GetCaseDraft	READ	授予控制台显示您之前创建的工单草稿的权限。
CreateCaseDraft	WRITE	授予创建或更新给定案例类型的案例草稿的权限。
DeleteCaseDraft	WRITE	授予删除给定案例类型的案例草稿的权限。
GetBanner	READ	授予控制台显示在影响客户的事件期间所显示 Amazon Web Services 支持 横幅的权限。
DescribeDynamicHelp	READ	授予控制台显示所选服务和类别的动态帮助资源的权限。
CreateContact	WRITE	授予控制台为所选联系人类型创建经过身份验证的联系人的权限。
CheckSubscription	READ	授予控制台验证您的账户是否有权访问所选产品的权限。
GetQuestionnaire	READ	授予控制台显示客户反馈问卷的权限。

操作	访问级别	描述
SaveFeedback	WRITE	授予保存问卷反馈的权限。

> **Note**
>
> 如果您有自定义 VPN 配置，则您的 IAM 策略必须允许在 aws.sourceIP 条件下使用支持中心控制台 API 端点。如果不允许使用支持中心控制台 API 端点，您的 ClientIp 地址将无法正确转发到 API。下表按 Amazon Web Services 区域列出了支持中心控制台 API 端点。
>
> | Amazon Web Services 区域 | 支持中心控制台 API 端点 |
> | --- | --- |
> | `https://api.us-east-1.prod.support-console.support.aws.dev` | 美国东部（弗吉尼亚州北部） |
> | `https://api.us-west-2.prod.support-console.support.aws.dev` | 美国西部（俄勒冈州） |
> | `https://api.eu-west-1.prod.support-console.support.aws.dev` | 欧洲地区（爱尔兰） |

测试支持中心控制台 API 调用

要验证对控制台的 API 调用是否正常工作，请打开 Amazon Support Center Console。如果调用失败，则会看到列出错误的横幅。

您可以使用 Amazon CloudTrail 调试对支持中心控制台进行的 API 调用。API 调用的 CloudTrail 事件会显示您是否缺少 IAM 策略。您还可以通过将浏览器的 IP 地址与 CloudTrail 事件中的客户端 IP 地址进行比较来调查 IP 地址转发问题。

要查看呼叫中心控制台调用的 CloudTrail 事件，请完成以下步骤：

1. 登录到 Amazon Web Services 管理控制台，然后通过以下网址打开 CloudTrail 控制台：https://console.aws.amazon.com/cloudtrail。
2. 在导航窗格中，选择事件历史记录。您会看到一个筛选后的事件列表，最新的事件显示在最前面。事件的默认筛选条件是只读的，设置为 false。要清除筛选条件，请选择筛选条件右侧的 X。
3. 选择事件源 support-console.amazonaws.com。在事件详细信息页面上，您可以查看事件详细信息、任何引用的资源以及事件记录。

关于 Amazon Web Services 支持 API

通过该 Amazon Web Services 支持 API，可以访问Amazon 支持中心中的某些功能。

API 提供两组不同的操作：

- 支持案例管理 操作用于管理 Amazon 支持案例从创建到解决的整个生命周期
- 要访问 Amazon Trusted Advisor 检查的 Amazon Trusted Advisor 操作

> **Note**
>
> 您必须有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划才能使用 Amazon Web Services 支持 API。有关更多信息，请参阅 Amazon Web Services 支持。

有关提供的操作和数据类型的更多信息 Amazon Web Services 支持，请参阅 Amazon Web Services 支持 API 参考。

主题

- 支持案例管理
- Amazon Trusted Advisor
- 端点
- Support in Amazon SDKs

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。您最多可以附加三个文件。每个文件最大可为 5 MB
- 解决您的案例

Amazon Web Services 支持 API 支持支持案例管理操作的 CloudTrail 日志记录。有关更多信息，请参阅 使用 Amazon CloudTrail 记录 Amazon Web Services 支持 API 调用。

有关演示如何管理支持案例整个生命周期的代码示例，请参阅 Amazon Web Services 支持 使用代码示例 Amazon SDKs...

Amazon Trusted Advisor

您可以使用这些 Trusted Advisor 操作来执行以下任务：

- 获取 Trusted Advisor 支票的名称和标识符
- 要求对您的 Amazon 账户和资源进行 Trusted Advisor 检查
- 获取 Trusted Advisor 检查结果的摘要和详细信息
- 刷新 Trusted Advisor 支票
- 获取每张 Trusted Advisor 支票的状态

Amazon Web Services 支持 API 支持对 Trusted Advisor 操作进行 CloudTrail 日志记录。有关更多信息，请参阅 Amazon Trusted AdvisorCloudTrail 日志记录中的 信息。

您可以使用 Amazon Ev CloudWatch ents 来监控您的检查结果是否有变化 Trusted Advisor。有关更多信息，请参阅 使用 Amazon 监控 Amazon Trusted Advisor 检查结果 EventBridge。

有关演示如何使用这些 Trusted Advisor 操作的 Java 代码示例，请参阅使用 Trusted Advisor 即 Web 服务。

端点

Amazon Web Services 支持 是一项全球服务。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，如果您使用中国（北京）端点创建案例，则可以使用中国（宁夏）端点为同一案例添加往来记录。

您可以为 Amazon Web Services 支持 API 使用以下终端节点：

- 中国（北京）– https://support.cn-north-1.amazonaws.com.cn
- 中国（宁夏）– https://support.cn-northwest-1.amazonaws.com.cn

Important

- 如果您调用该CreateCase操作来创建测试支持案例，那么我们建议您添加主题行，例如 TEST Case-请忽略。完成测试支持案例后，请调用ResolveCase操作来解决该问题。
- 要调用 Amazon Web Services 支持 API 中的 Amazon Trusted Advisor 操作，必须使用中国（北京）终端节点。目前，中国（宁夏）终端节点不支持 Trusted Advisor 这些操作。

有关 Amazon 终端节点的更多信息，请参阅中的Amazon Web Services 支持 终端节点和配额Amazon Web Services 一般参考。

Support in Amazon SDKs

Amazon Command Line Interface (Amazon CLI) 和 Amazon 软件开发套件 (SDKs) 包括对 Amazon Web Services 支持 API 的支持。

要查看支持 Amazon Web Services 支持 API 的语言列表，请选择操作名称，例如 CreateCase，然后在 “另请参阅” 部分中选择您的首选语言。

Amazon Web Services 支持 计划

Amazon 根据您的业务需求提供以下 Amazon Web Services 支持 计划供您选择。

- Basic
- 开发者版
- 商业
- Enterprise On-Ramp
- Amazon 企业 Support

> **Important**
>
> 您的 Amazon Web Services 支持 计划中不提供新计划 Amazon Web Services 区域。您现有的开发者支持、业务支持、企业支持或企业入门计划仍然有效。

主题

Amazon Web Services 支持 计划的特点

Basic Support 为账户和账单问题以及服务配额增加提供帮助。其他计划提供了许多技术支持案例，这些案例包括 pay-by-the-month定价且没有长期合同。

所有 Amazon 客户都可以自动全天候使用 Basic Support 的以下功能：

- One-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
- Building-block 架构支持：有关如何同时使用 Amazon 产品、功能和服务的指南
- 支持无限数量的支持案例，具有权限的所有用户均可打开。

此外，拥有商业、企业或企业入口计划的客户还可以使用以下功能：

- 用例指南 — 使用哪些 Amazon 产品、功能和服务来最好地支持您的特定需求。
- Amazon Trusted Advisor— 的一项功能 Amazon Web Services 支持，它可以检查客户环境并确定节省资金、填补安全漏洞以及提高系统可靠性和性能的机会。您可以访问所有 Trusted Advisor 支票。
- 用于与 Support Center 进行交互的 Amazon Web Services 支持 API 和 Trusted Advisor. 您可以使用 Amazon Web Services 支持 API 自动执行支持案例管理和 Trusted Advisor 操作。
- 第三方软件支持 — 亚马逊弹性计算云 (Amazon EC2) 实例操作系统和配置方面的帮助。此外，还可以帮助提高上最受欢迎的第三方软件组件的性能 Amazon。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 Amazon Identity and Access Management (IAM) 用户可以提交技术支持案例。

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 Amazon Web Services 支持 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。
- 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Amazon Web Services 支持和比较 Amazon Web Services 支持 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。

> **Note**
>
> 如果您与 Amazon 合作伙伴合作并想进一步了解合作伙伴主导的支持，请参阅Amazon Partner-Led Support

什么是 Amazon 统一运营

Amazon Unified Operations 将久经考验的专业知识与人工智能驱动的见解相结合，有助于降低运营和安全风险，更快地解决问题，并帮助您从一开始就架构更具弹性的云解决方案，从而加快最关键的云计划。指定的 Amazon 专家通过您首选的协作渠道充当团队的延伸，包括进行工作量审查、提供战略指导以及通过深入的情境知识优化绩效。通过全天候安全和性能监控，我们可以及早发现和缓解事件，同时减少警报量。针对重大事件的五分钟情境感知响应可进一步缩短解决时间，并有助于保持最佳运营绩效。

Amazon 统一运营定价

Amazon 统一运营定价基于您的具体要求和工作负载复杂性。有关详细定价信息，请参阅Amazon Web Services 支持 套餐定价。

目录

统一运营的好处

统一运营具有多项主要优势。

- 指定 Amazon 专家：您的 Amazon 团队包括指定的技术客户经理 (TAMs)、 Amazon 领域专家工程师以及高级账单和账户专家。你的 Amazon 团队可以与 Slack 或 Microsoft Teams 等协作工具集成。
- 深入的技术指导：您的 Amazon 团队通过针对特定应用程序的深入研究、就绪性评估、指导性测试支持以及针对您的环境量身定制的自定义运行手册，帮助您增强弹性。您的 Amazon 团队提供以工作量为中心的财务管理，并在战略上使成本与您的业务目标保持一致。
- 迁移、活动和启动支持：与指定的 Amazon 工程师一起加速关键的云迁移和业务活动，他们将主动帮助降低风险，指导您从规划到执行。为预定事件提供实时协助，提高迁移速度并成功启动。
- 全天候主动监控工作负载：从您的现有和第三方工具中加入应用程序 Amazon 和基础设施级别的警报，以检测预警信号并与您的团队一起推动主动缓解。
- 针对关键业务系统停机问题，在 5 分钟内与 Amazon 事件经理接触：在出现警报、工作负载警报或关键业务系统停机问题后 5 分钟内获得事件管理工程师的主动支持。
- 针对@@ 特定情境的案例响应：联系情境感知支持工程师，推动事件解决。为您的工作流程定制了运行手册和事件响应手册，可根据您的特定业务需求简化问题诊断和解决方案。
- 安全指导和支持：通过自动分类和调查主动监控安全事件，并全天候 Amazon 联系客户事件响应团队，为 Amazon 环境中的安全事件做好准备、响应和恢复。

统一运营小组

Amazon Unified Operations 汇集了一支由专业专家组成的指定团队，他们共同为你的云之旅提供支持。每个职位都经过精心设计，旨在全面涵盖云环境的技术、财务、运营和安全方面。从战略指导到技术支持，从财务优化到快速事件响应，这些专家是您团队的延伸，全天候提供服务，以确保您的云运营高效、安全地运行。

目录

技术客户经理

您指定的云策略师技术客户经理 (TAM) 负责协调整体参与并推动业务成果。 TAMs 领导战略规划，进行季度业务审查，提供弹性指导，并在专业团队之间进行协调，以确保您的云计划取得成功。他们是您进行升级和战略决策的主要联系人。

领域专家工程师

领域专家工程师 (DSE) 是一位技术专家，他对您的特定工作负载架构有深刻的了解，并且 Amazon Web Services 服务. DSEs 进行关键工作负载审查，创建技术文档，制定故障排除指南，并提供持续的技术咨询。他们分析事件以防止再次发生，并保持全球知识共享，以确保支持质量始终如一。

高级账单和账户专家

您的高级账单和账户专家 (SBAS) 是指定的财务优化专家，可帮助平衡绩效与成本。他们管理成本优化策略，监督预留实例和储蓄计划组合，进行财务业务审查，并提供详细的支出分析，以最大限度地提高您的云投资效率。

事件管理工程师

事件管理工程师 (IME) 是负责协调重大事件解决方案的快速响应专家。 IMEs 提供 5 分钟的响应时间，在事件发生期间协调技术团队，管理利益相关者的沟通。在发生事件期间， IMEs 对事件处理和响应有

效性进行实时评估，他们应要求记录事件的顺序、做出的决策和即时结果。在事件仍在发生期间，他们观察和评估应对协议的执行情况、团队协调以及现有行动手册的应用情况。

移民专家

按需专家指导关键过渡，例如启动和迁移。他们验证架构，制定详细的执行计划，在事件期间提供实时监控，并进行事后分析以捕获经验并优化 future 运营。

Amazon 客户事件响应小组

Amazon 客户事件响应小组 (CIRT) 是安全专家，为安全事件提供全天候专业协助。他们监控安全发现，在检测到的几分钟内提供指导性响应，并通过专家调查支持和最佳实践指导来增强您的安全运营能力。

专家 Support 工程师

Speciality Support Engineers (SSE) 是经验丰富的技术专家，他们使用高级情境工具来提供精确的支持解决方案。他们利用人工智能驱动的系统和深厚的技术知识来快速了解您的环境并解决复杂的技术挑战。

统一运营生命周期

Unified Operations Support 计划包含不同的阶段，从入职前到持续改进，可帮助您充分利用云环境。本主题涵盖每个阶段的要点。

目录

统一运营入职前

在入职前阶段，从你 Amazon 那里收集启动入职流程所需的信息，包括以下信息：

环境发现和技术验证

- 了解您的工作负载架构和密钥 Amazon Web Services 服务。
- 您的未来规划需求，例如迁移或活动。
- 先决条件，例如您的 Amazon Web Services 账户 和 Amazon Web Services 区域清单。
- 您的特定业务需求。

统一运营入职

入职启动仪式

- 认识团队（客户和 Amazon 分配的资源）。

入职研讨会

- 识别关键工作负载。
- 对工作负载进行深入的架构审查。
- 查看角色和职责（RACI 审查， Amazon 以及您的角色和职责）。
- 查看事件和变更管理工作流程 (ITSM)。
- 通信协议-工具和流程、上报路径、待命时间表
- 识别并定义关键警报（在 Amazon CloudWatch、您的第三方 APM 或自定义监控工具中）。
- 为关键警报构建运行手册。

服务入门

- 您的 Amazon Web Services 账户 入职培训. Amazon 安全事件响应
- 进入快速事件管理的关键警报。

统一运营活动前或迁移规划

Amazon 统一运营中的活动前或迁移计划包括以下关键要素。

- 情境收集：工作负载发现和架构。
- 运营准备情况审查 (ORR)：根据 Amazon 最佳实践和操作手册进行系统评估，以便在潜在问题影响事件之前将其识别出来。

- 风险评估：识别、列出潜在风险和缓解计划。
- 查看事件：保护切换或迁移事件支持。

统一运营事件迁移或切换

统一运营中的事件迁移或切换包括以下关键要素。

- 通@@ 往解决方案的实时桥梁： Amazon 专家加入您的沟通渠道，在关键业务时期监控事件并解决问题。
- 全天候全面支持： Round-the-clock专家协助，即时指导资源扩展需求。
- Amazon 工程：直接与了解您业务的工程师合作，提供量身定制的解决方案。

上线或活动后的统一运营

Unified Operations 中的上线后或活动后流程包括以下关键要素：

- 衍生参与和活动特定资源。
- 进行活动回顾。
- 根据学习内容更新运行手册和文档。
- 进行回顾以确定需要改进的领域。

统一运营工作负载事件管理

工作负载事件管理包括以下关键要素：

- Amazon Web Services 支持 案例创建。
- 与您和 Amazon 事件管理工程师 (IME) 合作，进行情境感知事件管理。
- 加入或创建事件桥接呼叫。
- 监测 Amazon Web Services 服务 健康状况和大规模事件 (LSE)。
- 快速恢复关键应用程序或工作负载。

事件发生后的统一行动

重大事件的事后分析由指定的领域专家工程师 (DSE) 进行。DSE 在解决问题后采用更广泛的分析方法，进行全面的根本原因分析，以确定流程或工具中的任何差距。DSE 通过更新响应手册、推荐预防措施和提出架构改进建议，将见解转化为可行的改进，以帮助防止将来发生类似事件。

统一运营持续改进

持续改进包括以下关键要素：

- 更新关键工作负载审查，提出 Amazon 针对具体服务的建议和弹性指导。
- 持续审查新旧案例，并针对已确定的技术问题提供故障排除指南。
- 应用课程并监督实施和测试。
- 讨论技术问题、配置、过去和即将推出的项目和里程碑。
- 通过风险评估和性能优化来审查新功能实施计划。
- 进行月度或季度业务评估 (MBR/QBR)。

统一运营入门

本主题讨论加入 Amazon 统一运营的步骤。

目录

统一操作入门：先决条件

加入 Amazon 统一运营需要以下物品

已签署的 Amazon 统一运营合同。欲了解更多信息，请联系您的 Amazon 销售代表。

- 已确定的业务需求，例如迁移、现代化、事件、目标正常运行时间等。
- 您的工作负载清单。
- 您的 Amazon Web Services 账户 和关联的清单 Amazon Web Services 区域。
- 确定应用程序、架构、运营和安全团队的利益相关者。

统一运营入门：加入关键警报以实现快速事件管理

为了帮助您快速通知您重大事件，请完成以下步骤，将警报加入 Amazon 事件检测和响应

1. 定义和配置您的关键警报，以实现快速事件管理。有关详细信息，请参阅《事件检测和响应用户指南》中的 “事件检测和响应” 中的定义和配置警报。

   a. 有关使用 Amazon 设置警报的步骤 CloudWatch，请参阅《事件检测和响应用户指南》中的 “事件检测和响应” 中的定义和配置警报。有关各种关键警报类型的 Amazon 建议 Amazon Web Services 服务，请参阅事件检测和响应 (IDR)。如果您想自动 Amazon 为已标记的 Amazon 资源创建关键 Amazon 警报，请联系您的 Amazon 统一运营团队。

   b. 要重定向或接收来自直接与 Amazon EventBridge 集成的第三方 APM 工具（例如、等）的关键警报 DataDog NewRelic，请参阅《Amazon 事件检测和响应用户指南》中的 “从 APMs 与亚马逊直接集成的警报” EventBridge 中获取与亚马逊直接集成的警报。您必须部署一组 Amazon 资源（Amazon Lambda 和 Amazon EventBridge 事件总线规则）来转换警报（事件）并将其重定向到 Amazon 事件检测和响应。您的 Amazon 统一运营团队可以帮助提供安装这些资源的 Amazon CloudFormation 模板。

   c. 通过未与 Amazon 直接集成的第三方 APM 工具从您的自定义监控工具中重定向或接收关键警报。 EventBridge有关更多信息，请参阅Amazon 事件检测和响应用户指南中的使用 webhook 从 EventBridge中获取警报， APMs 无需与 Amazon 直接集成。您必须部署一组 Amazon 资源（API Gateway Amazon Lambda 函数和 Amazon EventBridge 事件总线规则）来转换警报（事件）并将其重定向到 Amazon 事件检测和响应。您的 Amazon 统一运营团队可以帮助提供安装这些资源的 Amazon CloudFormation 模板。

2. 提供工作负载架构详细信息、联系人信息以及有关关键警报缓解措施的运行手册信息。为此，请完成以下步骤：

   - 下载并填写每个关键工作负载或应用程序Amazon 的事件检测和响应工作负载入职调查表，以及与每个独特工作负载相关的警报摄取调查表。

这些问卷中的信息可帮助 Amazon 团队制定事件补救操作手册。通过本操作手册，可以采取适当的措施，在关键警报导致业务停机之前对其进行快速故障排除和修复。有关示例和示例信息，请参阅Amazon 事件检测和响应中的工作负载入和警报摄取问卷。

3. 为 Amazon 事件检测和响应提供机载关键警报的访问权限

   a. 在 Amazon Web Services 账户 运行关键工作负载时部署AWSServiceRoleForHealth_EventProcessor服务相关角色 (SLR)，由 Amazon 事件管理团队进行监控。有关更多信息，请参阅为 Amazon 事件检测和响应提供警报接收权限。

   > **Note**
   >
   > 为了帮助你完成大规模的入职培训 Amazon Web Services 账户， Amazon 可以为你提供一个 Amazon Command Line Interface 脚本来快速跟踪这款 SLR 的配置。

   b. （可选）如果您的警报在 Amazon CloudWatch 中，请确保用于警报测试（上线前）的 Amazon Identity and Access Management 用户或角色在运行关键工作负载的用户或角色中拥有 `cloudwatch:SetAlarmState` IAM 权限。 Amazon Web Services 账户 这是入职后的警报测试（比赛日）所必需的。有关更多信息，请参阅 “Amazon 事件检测和响应” 中的 “测试已加载的工作负载”。

4. 创建 Amazon Web Services 支持 案例以订阅工作负载，以实现快速事件管理。请注意，您的 Amazon Web Services 账户 入站快速事件管理已自动启用，这意味着您可以通过 Support Center Console、或 Amazon SDK 向统一运营事件检测和响应队列提出案例 Amazon Command Line Interface，以便快速采取行动。 Amazon 要主动监控出站 Amazon Web Services 支持 案例并创建事件，请为您的关键工作量创建 Amazon Web Services 支持 案例。为此，请完成以下步骤：

   a. 登录 Amazon Support Center Console，选择 “创建案例”，然后选择 “技术支持”。
   b. 对于 “服务”，选择 “事件检测和响应”。
   c. 对于类别，选择载入新工作负载。
   d. 对于 “严重性”，选择 “一般指导”。
   e. 附上您在上一步中填写的工作量和警报调查表。

统一运营入门：如何请求 5 分钟的事件响应

Amazon 统一运营为您的关键事件提供 5 分钟的事件响应。要请求 5 分钟的入站回复，您可以通过支持互动创建支持案例，也可以使用旧版支持案例创建方法。创建案例时，请务必输入以下信息，以确保您的问题在 5 分钟内得到答复：

1. 对于案例类型，请选择技术。
2. 对于服务，选择Amazon 事件检测和响应。
3. 对于类别，选择活动事件。
4. 对于严重性，选择关键业务系统停机。
5. 在描述中，包括以下信息

    a. 技术信息

        - 工作负载名称
        - 受影响的 Amazon 资源 ARN

    b. 商业信息

        - 业务影响描述
        - （可选）客户桥详情

统一运营入门：规划域名覆盖范围

Amazon Unified Operations 通过基于域的覆盖方法提供专业知识。每个域名都由 Amazon 域名专家团队提供支持，他们提供以下服务：

- 与您的特定技术领域相匹配的@@ 专业知识。
- 在工作日内，通过你首选的协作工具（Slack 或 Microsoft Teams）持续提供可用性。
- 关于架构、最佳实践和优化机会@@ 的主动指导。
- 通过深厚的领域知识和对工作负载的熟悉度来@@ 增强事件响应。
- 由协调@@ 一致的团队而不是个人保持一致的体验。

这种域覆盖方法使 Amazon 专家能够深入了解您的关键工作负载，同时为您的技术堆栈提供全面的支持。

要选择域，组织保留从 23 个 Amazon 域中选择的决策权，并在做出决策时考虑以下因素：

- 主要 Amazon Web Services 服务 运行关键工作负载
- 关键 Amazon Web Services 服务 依赖项（例如亚马逊 EC2、亚马逊 EKS 或 Amazon RDS）
- 需要全天候支持（迁移、发布）的重大活动计划在 3-6 个月内完成

这些信息与您的技术客户经理的指导相结合，可以精确地调整领域专业知识与您的特定组织需求，从而帮助您保持对关键任务工作负载的最佳支持。

统一运营入门：注册您的账户以进行主动安全事件管理

Unified Operations Amazon 安全事件响应 使您有权帮助您快速做好准备，应对账户接管、数据泄露和勒索软件攻击等安全事件，并从中恢复。 Amazon 安全事件响应 对调查结果进行分类、上报事件并管理关键案例，同时还允许访问 Amazon 客户事件响应小组 (CIRT)，以调查受影响的资源。此访问权限可帮助您有效地缓解和解决安全事件，从而最大限度地减少对运营的影响。要加入此服务功能，请完成以下步骤：

1. 为其创建集中式 Amazon Web Services 账户 Amazon 安全事件响应。 Amazon Web Services 账户 这将用于配置您要监控 Amazon Web Services 账户 的所有其他内容、管理您的事件响应团队以及创建和查看安全事件。我们建议您将此账户与您用于其他安全服务（例如 Amazon GuardDuty 和）的账户保持一致 Amazon Security Hub CSPM。您可以使用Amazon Organizations管理账户或 Amazon Organizations 委托管理员账户作为安全事件响应成员账户。有关更多信息，请参阅《Amazon 安全事件响应 用户指南》中的选择会员账户。

   a. 选择基本的会员详细信息。有关更多信息，请参阅《Amazon 安全事件响应 用户指南》中的设置成员资格详细信息。

   b. 选择您想要将账户与之关联的方式 Amazon Organizations。有关更多信息，请参阅《Amazon 安全事件响应 用户指南》 Amazon Organizations中的 “将账户与关联”。

   c. （可选）您可以选择启用主动响应和警报分类工作流程，以便在组织内部监控和调查由 Amazon GuardDuty 和 Amazon Security Hub CSPM 集成生成的警报。有关更多信息，请参阅《Amazon 安全事件响应 用户指南》中的设置主动响应和警报分类工作流程。

2. （可选）启用对潜在安全事件的主动遏制。 Amazon 可以执行遏制操作以快速减轻影响，例如隔离受感染的主机或轮换凭证。要开启此功能，必须先向服务授予必要的权限。为此，请部署 Ste p Functions StackSet。

统一运营入门：您的 Amazon 期望

为了使统一运营实现最大价值，我们建议采用以下协作方法：

团队参与度

- 确定团队中的主题专家，以便在入职和持续参与期间与 Amazon 工程师合作。
- 参加最初的探索电话会议和随后的会议，以分享架构细节和操作要求。
- 建立定期接触点以审查架构更新或工作负载变化。

运营集成

- 在您的账户中配置关键警报，以实现有效的事件管理。
- 执行 Amazon 专家提出的建议行动项目，
- 参加比赛日练习，验证事件响应流程。

此协作框架可帮助您最大限度地提高统一运营的价值，实现正常运行时间目标，降低运营风险，并获得针对任务关键型工作负载的全面支持。

统一运营入门：您可以从中获得什么 Amazon

当您加入统一运营时，您可以期待以下内容 Amazon。

- 提供一支在您的工作负载领域和服务方面具有深厚技术专业知识的指定 Amazon 专家团队。
- 提供主动指导、持续优化和持续改进建议，以提高工作负载性能和弹性，加快迁移和现代化之路。
- 帮助提供快速的事件响应，情境感知工程师可在重大事件发生后 5 分钟内投入工作。
- 在整个应用程序生命周期中提供全面支持，从设计和迁移到生产发布和长期运营。
- 通过自动分类、减少误报和举报潜在安全事件来主动监控安全威胁。
- 协助解决问题并共同缓解 Amazon 您发现的安全事件。

更改 Amazon Web Services 支持 计划

您可以使用 Amazon Web Services 支持 计划控制台来更改您的支持计划 Amazon Web Services 账户。要更改您的支持计划，您必须拥有 Amazon Identity and Access Management(IAM) 权限。有关更多信息，请参阅管理对 Amazon Web Services 支持 套餐的访问权限和AmazonAmazon Web Services 支持 计划的托管策略。

更改您的支持计划

1. 在计划 https://console.aws.amazon.com/support//主页登录 Amazon Web Services 支持 计划控制台。
2. （可选）要比较支持计划，请在Amazon Web Services 支持 计划页面上，选择比较所有 Amazon Web Services 支持 计划和功能。
3. （可选）要查看支持计划的预估成本，请选择定价计算器。在定价计算器中，选择支持等级，输入预计 Amazon 每月花费的预估金额，然后选择计算。
4. 要降级 Enterprise Support 计划，请联系您的技术客户经理 (TAM)。

要降级 Business Support+ 计划，请在 “管理支持计划” 页面上，选择 “基本 Amazon Web Services 支持 计划” 部分的 “查看降级”。

要升级到 En Amazon terprise Suppor Amazon t 或统一运营计划，请选择 “联系销售人员”。

要从基本版升级到 Amazon 商业支持+计划 Amazon Web Services 支持，请完成以下步骤：

a. 在 “ Amazon 业务支持+” 部分中选择 “开始”。

b. 如果您已加入 Amazon Organizations 并启用了所有功能模式，则可以为整个组织订阅 Business Support+。有关全功能模式的信息，请参阅《Amazon Organizations 用户指南》Amazon Organizations中的 “使用为组织启用所有功能”。要在组织级别注册，请选择我的组织单选按钮。查看套餐详情和定价，然后选中复选框以同意订阅条款。只有贵组织的管理账户才能订阅整个组织。

   或者，要在账户级别注册，请选择 “我的账户” 单选按钮，然后选中该复选框以同意订阅条款。

c. 选择 “确认升级” 以完成您的 Amazon 商业支持+计划订阅。

> **Note**
>
> 在您为整个组织订阅 Amazon 商业支持+后，在该组织内创建的任何新帐户都将自动订阅 Amazon 商业支持+。如果之前在组织级别订阅了 B Amazon usiness Support+ 的账户离开组织，则该账户将降级为基本支持计划。

> **Note**
>
> 如果您注册了付费支持计划，则需要至少订阅一个月的 Amazon Web Services 支持。有关更多信息，请参阅 Amazon Web Services 支持 FAQs。

相关信息

有关 Amazon Web Services 支持 计划的更多信息，请参阅Amazon Web Services 支持 FAQs。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 Amazon Billing 用户指南中的关闭账户。

配置促销计划到期通知

您可以使用 Amazon 用户通知服务 配置通知，以便在支持计划的促销期即将结束时收到提醒。您可以订阅通过电子邮件 Amazon Console Mobile Application、或您选择的其他聊天渠道接收通知。

配置促销支持计划到期通知

1. 在 Amazon Web Services 管理控制台 中打开用户通知：
   a. 选择顶部导航栏中的铃铛图标。
   b. 选择通知中心。
   c. 在导航窗格中，选择通知配置。
   d. 选择创建通知配置。
   e. 至少选择一个配置中心。有关更多信息，请参阅在 Amazon 用户通知服务中使用通知中心存储、处理和复制通知。
2. 在事件规则中，输入以下信息：
   - 在 Amazon Web Services 服务 名称中，输入支持计划。
   - 在事件类型中，输入支持计划促销到期。
   - 对于区域，选择您想要接收通知的来源 Amazon Web Services 区域 。对于此选项，请选择美国东部（弗吉尼亚州北部）、美国东部（俄亥俄州）、美国西部（北加利福尼亚）以及美国西部（俄勒冈州）。
3. 配置聚合设置以降低通知频率。建议将聚合设置为在 5 分钟内接收。
4. 配置您希望接收通知的传递通道。如果您未选择配送渠道，则可以通过选择 Amazon Web Services 管理控制台 导航栏中的铃铛图标来查看通知。

有关创建用户配置通知的详细说明，请参阅《 Amazon 用户通知服务 用户指南》中的步骤 1：创建通知配置。

查看促销计划通知

您的通知将发送到您在配置期间选择的传递通道。您也可以通过选择控制台导航栏中的铃铛图标来查看通知。当有新通知时，铃铛图标会显示红色徽章。

有关查看通知的更多信息，请参阅《Amazon 用户通知服务 用户指南》中的步骤 2：查看通知。

开发人员、企业和企业入口服务终止支持

> **Important**
>
> 此信息 Amazon Web Services 区域 仅适用于商业广告。

有关过渡到新计划的信息，请参阅以下与您的计划相关的信息和Amazon Web Services 支持 常见问题解答。

> **Note**
>
> 开发者支持、业务支持和企业入门服务仍将在该 Amazon GovCloud (US) 地区提供。

开发者 Amazon Web Services 支持 计划终止支持

终止支持通知：开发者支持将于 2027 年 1 月 1 日停止。拥有 Developer Support 的客户可以继续使用其现有计划或选择在 2027 年 1 月 1 日之前的任何时候升级到 Business Support+。Business Support + 提供基于人工智能的帮助，了解您的运营背景，可全天候联系 Amazon 专家，每个账户每月最低费用为29美元。有关更多信息，请参阅 “商业支持+” 计划详情。

商业 Amazon Web Services 支持 计划终止支持

终止支持通知：Business Support 将于 2027 年 1 月 1 日停止。拥有 Business Support 的客户可以继续使用其现有计划或选择在 2027 年 1 月 1 日之前的任何时候升级到 Business Support+。Business Support+ 提供基于人工智能的帮助，了解您的运营背景，可全天候联系 Amazon 专家，每个账户每月最低费用为29美元。有关更多信息，请参阅 “商业支持+” 计划详情

企业入口服务终止支持

终止支持通知：2027 年 1 月 1 日， Amazon 将停用 Enterprise On-Ramp。在 2026 年，Enterprise On-Ramp 客户将在合同续订期间或定期批量自动升级到 Amazon Enterprise Support。客户将在升级前一个月收到电子邮件通知。无需进一步操作。Enterprise Support 提供指定的 TAM 分配、15 分钟的响应时间，且 Amazon 安全事件响应 无需支付额外费用，所有费用都低于 5,000 美元（低于 15,000 美元）。有关更多信息，请参阅Amazon 企业 Amazon Web Services 支持 套餐详情。

Amazon Trusted Advisor

Trusted Advisor 借鉴了从为成千上万的 Amazon 客户提供服务中学到的最佳实践。 Trusted Advisor 检查您的 Amazon 环境，然后在有机会节省资金、提高系统可用性和性能或帮助填补安全漏洞时提出建议。

如果您有 Basic 或 Developer Support 计划，则可以使用 Trusted Advisor 控制台访问服务限制类别中的所有检查以及安全和容错类别中的选定检查。基本和开发人员支持计划不提供自动检查更新。您必须手动刷新 “安全” 类别中的 Trusted Advisor 支票。要手动刷新检查，请执行以下操作：

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 在要刷新的检查上选择刷新按钮。

如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则可以使用 Trusted Advisor 控制台和 Amazon Trusted Advisor API 访问所有 Trusted Advisor 支票。您还可以使用 Amazon E CloudWatch vents 来监控 Trusted Advisor 支票的状态。有关更多信息，请参阅 使用 Amazon 监控 Amazon Trusted Advisor 检查结果 EventBridge。

你可以在 Trusted Advisor 中访问 Amazon Web Services 管理控制台。有关控制控制 Trusted Advisor 台访问权限的更多信息，请参阅管理对的访问权限 Amazon Trusted Advisor。

有关更多信息，请参阅 Trusted Advisor。

主题

- 开始使用 Trusted Advisor 建议
- 开始使用 Trusted Advisor API
- 使用 Trusted Advisor 即 Web 服务
- 的组织视图 Amazon Trusted Advisor
- 查看由 Amazon Trusted Advisor ... 提供支持的支票 Amazon Config
- 在中查看 Amazon Security Hub CSPM 控件 Amazon Trusted Advisor
- 选择使用 Amazon Compute Optimizer 支 Trusted Advisor 票
- 开始使用 P Amazon Trusted Advisor riority
- Amazon Trusted Advisor 查看参考资料
- 更改日志 Amazon Trusted Advisor

开始使用 Trusted Advisor 建议

您可以使用 Trusted Advisor 控制台的 “ Trusted Advisor 建议” 页面查看您的检查结果， Amazon Web Services 账户 然后按照建议的步骤修复所有问题。例如， Trusted Advisor 可能会建议您删除未使用的资源以减少每月账单，例如亚马逊弹性计算云 (Amazon EC2) 实例。

您还可以使用 Amazon Trusted Advisor API 对 Trusted Advisor 支票执行操作。有关更多信息，请参阅 Amazon Trusted Advisor API 参考

主题

登录 Trusted Advisor 控制台

您可以在 Trusted Advisor 控制台中查看支票和每张检查的状态。

> **Note**
>
> 您必须具有 Amazon 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 管理对的访问权限 Amazon Trusted Advisor。

登录控制 Trusted Advisor 台

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 在 Trusted Advisor 建议页面上，查看每种检查类别的摘要：
   - 建议的操作（ 红色 ）- Trusted Advisor 建议检查的操作。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，这可能是您不希望支票评估的 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。

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-有关安全设置的建议，可使您的 Amazon 解决方案更加安全。
- 容错能力 — 有助于提高 Amazon 解决方案弹性的建议。这些检查突出显示了冗余不足和过度使用的资源。
- 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 Amazon 服务和资源的限制（也称为配额）。
- 卓越运营 — 可帮助您有效且大规模地运营 Amazon 环境的建议。

要查看检查类别

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
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：

- 建议的操作（红色）- Trusted Advisor 建议检查的操作。
- 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。

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. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
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 Amazon 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）。

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。

如果您有评估账户中项目（例如 Amazon 资源）的支票，则可以使用标签筛选器仅显示带有指定标签的项目。

要筛选您的检查

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
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. 如果您为 Amazon 资源（例如 Amazon EC2 实例或 Amazon CloudTrail 跟踪）添加了标签，则可以筛选结果，以便检查结果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

有关为添加标签的更多信息 Trusted Advisor，请参阅以下主题：

- Amazon Web Services 支持 启用标记功能 Trusted Advisor
- Amazon Web Services 一般参考 中的添加 Amazon 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。如果您有 Developer 或 Basic Support 套餐，则可以登录 Trusted Advisor 控制台刷新支票。如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则每周 Trusted Advisor 自动刷新账户中的支票。

刷新 Trusted Advisor 支票

1. 在 https://console.aws.amazon.com/trust edad Amazon Trusted Advisor visor 上导航到控制台。
2. 在 “ Trusted Advisor 建议” 或 “支票类别” 页面上，选择 “刷新所有支票”。

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 每天自动刷新一些检查几次，例如可靠性检查Amazon Well-Architected的高风险问题。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 Amazon Security Hub CSPM 为账户启用了控件，则无法使用 Trusted Advisor 控制台刷新 Security Hub CSPM 控件。有关更多信息，请参阅 刷新你的 Security Hub CSPM 调查结果。

下载检查结果

您可以下载支票结果，以便 Trusted Advisor 在您的账户中查看概览。您可以下载所有检查或指定检查的结果。

从 “ Trusted Advisor 推荐” 中下载检查结果

1. 在 https://console.aws.amazon.com/trust edad Amazon Trusted Advisor visor 上导航到控制台。
   - 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，为 Amazon 组织中的所有成员账户创建报告。有关更多信息，请参阅 的组织视图 Amazon Trusted Advisor。

Preferences（首选项）

在管理 Trusted Advisor页面上，您可以禁用 Trusted Advisor。

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。

在您的组织页面上，您可以使用启用或禁用可信访问权限 Amazon Organizations。这是 的组织视图 Amazon Trusted Advisor 功能和 Trusted Advisor Priority 所必需的。

设置通知首选项

指定谁可以接收每周检查结果的 Trusted Advisor 电子邮件和语言。您每周都会收到一封电子邮件通知，告知您的 “ Trusted Advisor 推荐” 支票摘要。

“ Trusted Advisor 推荐” 的电子邮件通知不包括 Trusted Advisor 优先级的结果。有关更多信息，请参阅 管理 Trusted Advisor 优先级通知。

要设置通知首选项

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。

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。您可以在 Amazon 账单与成本管理控制台的 “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

如果您使用设置帐户 Amazon Organizations，则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 的组织视图 Amazon Trusted Advisor。

禁用 Trusted Advisor

当您禁用此服务时， Trusted Advisor 不会对您的账户进行任何检查。任何尝试访问 Trusted Advisor 控制台或使用 API 操作的人都会收到一条访问被拒绝的错误消息。

要禁用 Trusted Advisor

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
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）。此操作将禁 Trusted Advisor 用您账户中的所有支票。
4. 然后，您可以手动从您的账户中删除该服务角色。有关更多信息，请参阅 删除 Trusted Advisor的服务关联角色。

相关信息

有关的更多信息 Trusted Advisor，请参阅以下主题：

- 我该如何开始使用 Trusted Advisor？
- Amazon Trusted Advisor 查看参考资料

开始使用 Trusted Advisor API

Amazon Trusted Advisor API 参考适用于需要有关 Trusted Advisor API 操作和数据类型的详细信息的程序员。此 API 提供对您的账户或 Amazon 组织内所有账户的 Trusted Advisor 推荐的访问权限。Trusted Advisor API 使用以 JSON 格式返回结果的 HTTP 方法。

> **Note**
>
> - 您必须有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划才能使用 Trusted Advisor API。
> - 如果您从没有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划的账户调用 Amazon Trusted Advisor API，则会收到拒绝访问的异常。有关更改支持计划的更多信息，请参阅 Suppor Amazon t。

您可以使用 Amazon Trusted Advisor API 获取支票列表及其描述、推荐和推荐资源。您也可以更新建议的生命周期。要管理建议，请使用以下 API 操作：

- 使用ListChecks、ListRecommendationsGetRecommendation、和 ListRecommendationResourcesAPI 操作查看推荐以及相应的账户和资源。
- 使用 UpdateRecommendationLifecycleAPI 操作更新由 Priority Trusted Advisor 管理的推荐的生命周期。
- 使用 BatchUpdateRecommendationResourceExclusionAPI 操作在 Trusted Advisor 结果中包含或排除一项或多项资源。
- ListOrganizationRecommendations、、GetOrganizationRecommendationListOrganizationRecommendatic和 UpdateOrganizationRecommendationLifecycleAPI 调用仅支持由 P Trusted Advisor riority 管理的推荐。这类建议也称为“优先建议”。如果您已激活 Trusted Advisor Priority，则可以通过管理账户或委托管理员账户查看和管理优先建议。如果未激活 Priority，则提出请求时会收到“访问被拒绝”异常。

有关更多信息，请参阅 Su Amazon pport 用户指南 Amazon Trusted Advisor 中的。

有关验证请求的信息，请参阅签名版本 4 签名流程。

使用 Trusted Advisor 即 Web 服务

借助 Amazon Web Services 支持 服务，您可以编写与 Amazon 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

以下 Java 代码段创建一个 Amazon Web Services 支持 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 DescribeTrustedAdvisorChecks API 操作，获取 Trusted Advisor 检查的列表及其相应的 `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 Amazon Web Services 支持 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 DescribeTrustedAdvisorCheckRefreshStatuses API 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 `getMillisUntilNextRefreshable` 实例中包含的对象来调用 `DescribeTrustedAdvisorCheckRefreshStatusesResult`。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 DescribeTrustedAdvisorCheckResult API 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 DescribeTrustedAdvisorChecks API 操作，以获取检查 ID。

以下 Java 代码段使用 `DescribeTrustedAdvisorChecksResult` 变量引用的 `result` 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 `DescribeTrustedAdvisorCheckResultResult` 的 `checkResult` 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。

显示 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。

```
// Show ResourceIds for flagged resources.
for (TrustedAdvisorResourceDetail flaggedResource :
    result1.getResult().getFlaggedResources())
{
    System.out.println(
        "The resource for this ResourceID has been flagged: " +
        flaggedResource.getResourceId());
}
```

的组织视图 Amazon Trusted Advisor

组织视图允许您查看您中所有账户的 Trusted Advisor 支票Amazon Organizations。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，您可以使用这些报告通过 IAM 使用检查来确定组织中的哪些账户正在使用 Amazon Identity and Access Management (IAM)，或者您是否有通过 Amazon S3 存储桶权限检查对亚马逊简单存储服务 (Amazon S3) Simple S3 存储桶执行的操作建议。

> **Note**
>
> 组织视图功能在中国区域中不可用。

主题

先决条件

您必须满足以下要求才能启用组织视图：

- 您的账户必须是 Amazon Organizations 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 Amazon Organizations 用户指南中的启用组织中的所有功能。
- 组织中的管理账户必须有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划。您可以从 Amazon Web Services 支持 中心或 Support plans 页面找到您的支持计划。请参阅比较 Amazon Web Services 支持 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。

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 已作为可信服务在您的组织中启用。有关更多信息，请参阅 Amazon Organizations 用户指南中的使用其他 Amazon 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。此角色包括代表您调用 Organizations Trusted Advisor 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 将服务关联角色用于 Trusted Advisor。

您可以从 Trusted Advisor 控制台启用组织视图。

要启用组织视图

1. 以管理员身份登录组织的管理账户，然后在 https://console.aws.amazon.com/trust edadviso Amazon Trusted Advisor r 上打开控制台。
2. 在导航窗格中的 Preferences（首选项）下，选择 Your organization（您的组织）。
3. 在 “通过以下方式启用可信访问” 下 Amazon 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。该 Amazon Web Services 支持 计划决定了哪些 Trusted Advisor 支票可用于账户。

刷新 Trusted Advisor 支票

在为组织创建报告之前，我们建议您刷新 Trusted Advisor 支票的状态。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。

如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划，则每周 Trusted Advisor 自动刷新账户中的支票。

> **Note**
>
> 如果您的组织中有拥有开发者或基本支持计划的账户，则这些账户的用户必须登录 Trusted Advisor 控制台才能刷新支票。您无法刷新组织管理账户中的所有账户的检查。

刷新 Trusted Advisor 支票

1. 在 https://console.aws.amazon.com/trust edad Amazon Trusted Advisor visor 上导航到控制台。
2. 在 Trusted Advisor 建议页面上，选择刷新所有检查。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，然后在 https://console.aws.amazon.com/trust edadviso Amazon Trusted Advisor r 上打开控制台。
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，该报告包括全部 Amazon Web Services 区域、支票类别、支票和资源状态。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 “区域”，指定 Amazon Web Services 区域 或选择 “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 Amazon Organizations，请选择要包含在报告中的组织单位 (OUs)。有关的更多信息 OUs，请参阅《Amazon 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 Amazon Web Services 区域
- 所有的安全和性能检查

在以下示例中，该报告包括支持小组组织单位和一个属于该组织的 Amazon 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，然后在 https://console.aws.amazon.com/trust edadviso Amazon Trusted Advisor r 上打开控制台。
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）。

下载组织视图报告

报告准备就绪后，从 Trusted Advisor 控制台下载。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，然后在 https://console.aws.amazon.com/trust edadviso Amazon Trusted Advisor r 上打开控制台。
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 使用以下颜色代码来表示检查结果：

- `Green`— Trusted Advisor 未检测到支票存在问题。
- `Yellow`— Trusted Advisor 检测支票可能存在的问题。
- `Red`— Trusted Advisor 检测到错误并建议检查操作。
- `Blue`— Trusted Advisor 无法确定支票的状态。

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 (Yw2K9puPzl) IDs 和 IAM 密钥轮换 (DqdJqYeRm5) 检查的和属性。

```
{
    "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
- 支 Trusted Advisor 票编号
- 资源 ID
- 报告的时间戳
- Trusted Advisor 支票的全名
- 支 Trusted Advisor 票类别
- 父组织单位 (OU) 或根账户的账户 ID

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，如果您没有在组织中使用亚马逊弹性计算云预留实例，则亚马逊 EC2 预留实例租赁到期检查将不会出现在您的报告中。
- 账户尚未刷新检查结果。当拥有基本或开发者支持计划的用户首次登录 Trusted Advisor 主机时，可能会发生这种情况。如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则用户从注册账户起最多可能需要一周的时间才能看到检查结果。有关更多信息，请参阅 刷新 Trusted Advisor 支票。
- 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 接口与诸如 Amazon Athena 之类的 Amazon 服务结合使用，对您的报告进行查询。您还可以使用 Amazon Quick Suite 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 Amazon 服务查看 Trusted Advisor 报告。

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 已作为可信服务在 Organizations 中删除。
- `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。

要禁用组织视图 Trusted Advisor

1. 登录组织的管理账户，然后在 https://console.aws.amazon.com/trust edadviso Amazon Trusted Advisor r 上打开控制台。
2. 在导航窗格中，选择首选项。
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，将 Trusted Advisor 不再汇总组织中其他 Amazon 账户的支票。但是，在您通过 IAM 控制台、IAM API 或 Amazon Command Line Interface (Amazon CLI) 将其删除之前，`AWSServiceRoleForTrustedAdvisorReporting`服务相关角色仍保留在组织的管理账户中。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 Amazon 服务来查询和可视化组织视图报告中的数据。有关更多信息，请参阅以下资源：
>
> - Amazon 管理和治理博客中的使用 Amazon Organizations大规模查看 Amazon Trusted Advisor 建议
> - 使用其他 Amazon 服务查看 Trusted Advisor 报告

使用 IAM 策略允许访问组织视图

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

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

JSON

```
{
    "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

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

JSON

```
{
    "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 Amazon CloudTrail 在账户中启用了以下角色，则日志条目中可能会显示以下角色：
>
> - `AWSServiceRoleForTrustedAdvisorReporting`— Trusted Advisor 用于访问组织中账户的服务相关角色。
> - `AWSServiceRoleForTrustedAdvisor`— Trusted Advisor 用于访问组织中服务的服务相关角色。
>
> 有关服务关联角色的更多信息，请参阅将服务关联角色用于 Trusted Advisor。

使用其他 Amazon 服务查看 Trusted Advisor 报告

按照本教程使用其他 Amazon 服务上传和查看您的数据。在本主题中，您将创建一个用于存储报告的亚马逊简单存储服务 (Amazon S3) 存储桶和 Amazon CloudFormation 一个用于在账户中创建资源的模

板。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 Quick Suite 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 Amazon 管理和治理博客中的使用 Amazon Organizations 大规模查看 Amazon 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 Amazon Identity and Access Management (IAM) 用户身份登录。
- 使用美国东部（弗吉尼亚北部）Amazon Web Services 区域 快速设置您的 Amazon 服务和资源。
- 创建 Quick Suite 账户。有关更多信息，请参阅《Amazon Quick Suite 用户指南》中的 Quick Suite 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. 登录 Amazon Web Services 管理控制台 到 https://console.aws.amazon.com/。
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. 打开 Amazon S3 控制台，网址为 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 “创建文件夹”，输入名称**folder1**，然后选择 “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 Amazon CloudFormation创建资源

将报告上载到 Amazon S3 后，请将以下 YAML 模板上载到 Amazon CloudFormation。此模板告诉您要为您的账户创建 Amazon CloudFormation 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 Amazon Lambda、和创建资源 Amazon Glue。

要使用创建您的资源 Amazon CloudFormation

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. 在 https://console.aws.amazon.com/cloudformation 上打开 Amazon CloudFormation 控制台。
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 “我确认 Amazon CloudFormation 可能会创建 IAM 资源” 复选框。
15. 选择创建堆栈。

    创建堆栈约需 5 分钟时间。
16.

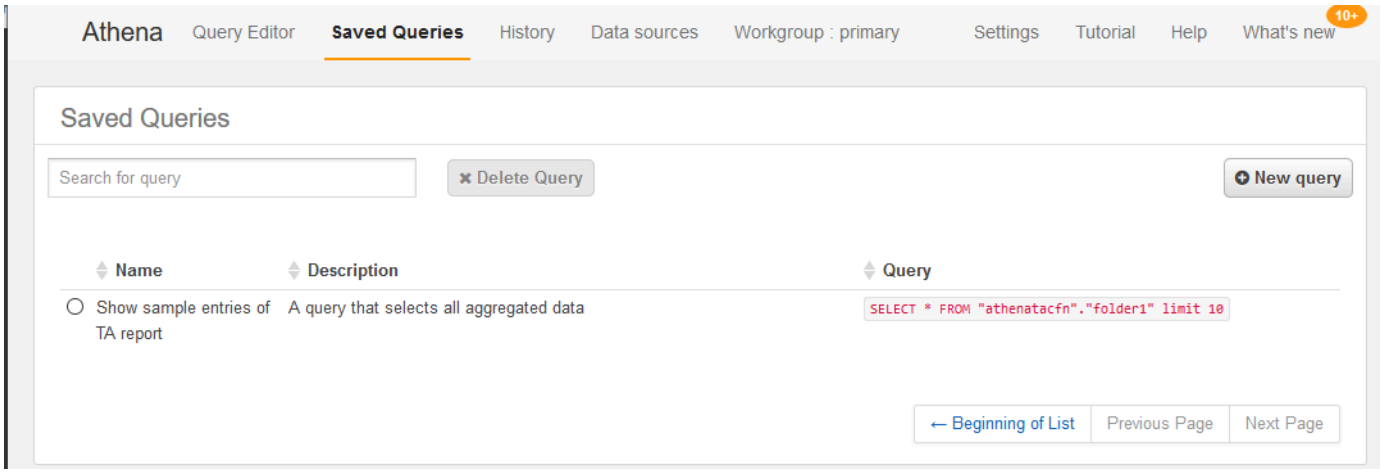
查询 Amazon Athena 中的数据

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）。



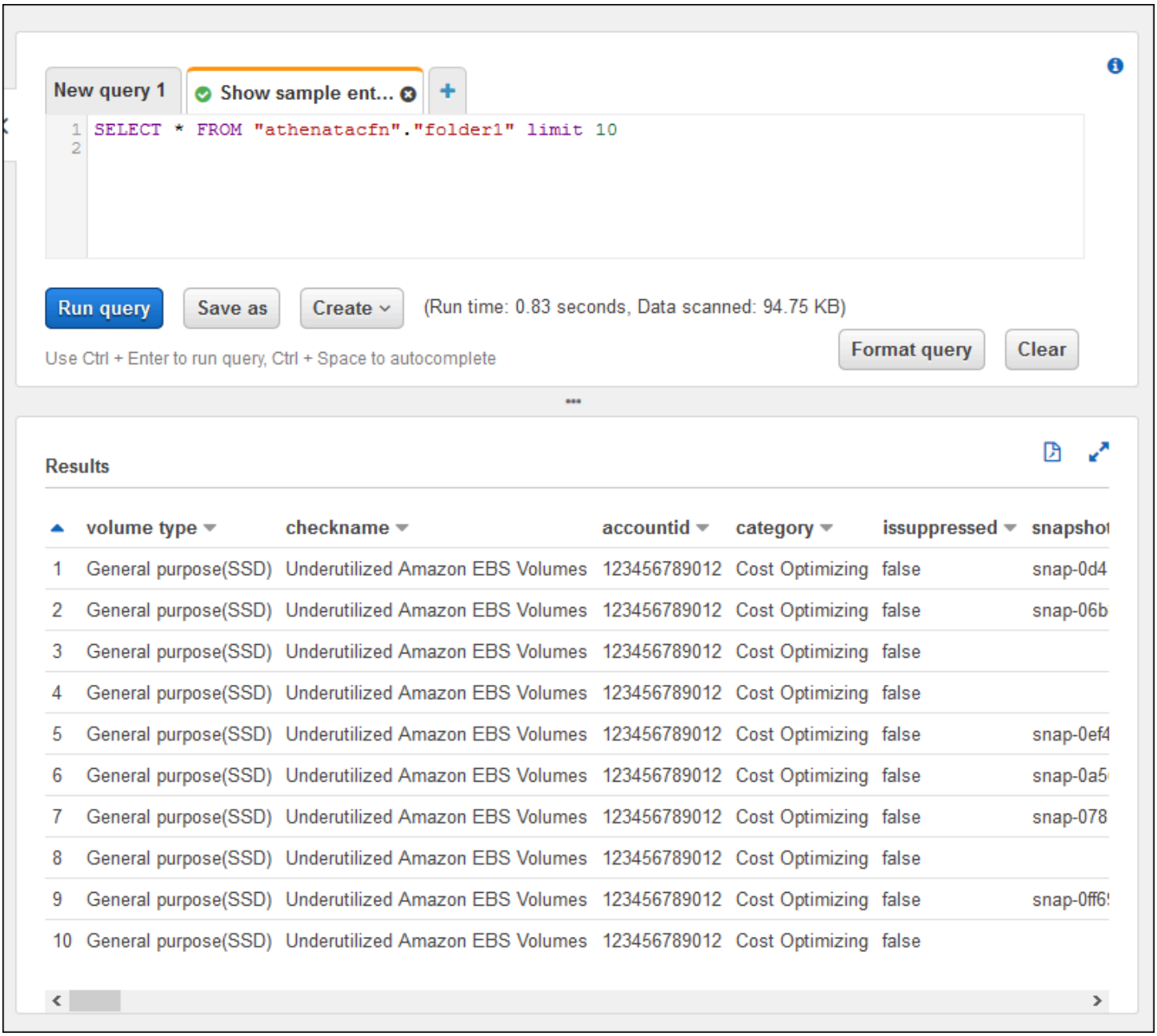
查询应与以下内容类似。

```
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。



	volume type	checkname	accountid	category	issuppressed	snapshot
1	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0d4
2	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-06b
3	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
4	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
5	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ef4
6	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0a5
7	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-078
8	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	
9	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	snap-0ff6
10	General purpose(SSD)	Underutilized Amazon EBS Volumes	123456789012	Cost Optimizing	false	

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。

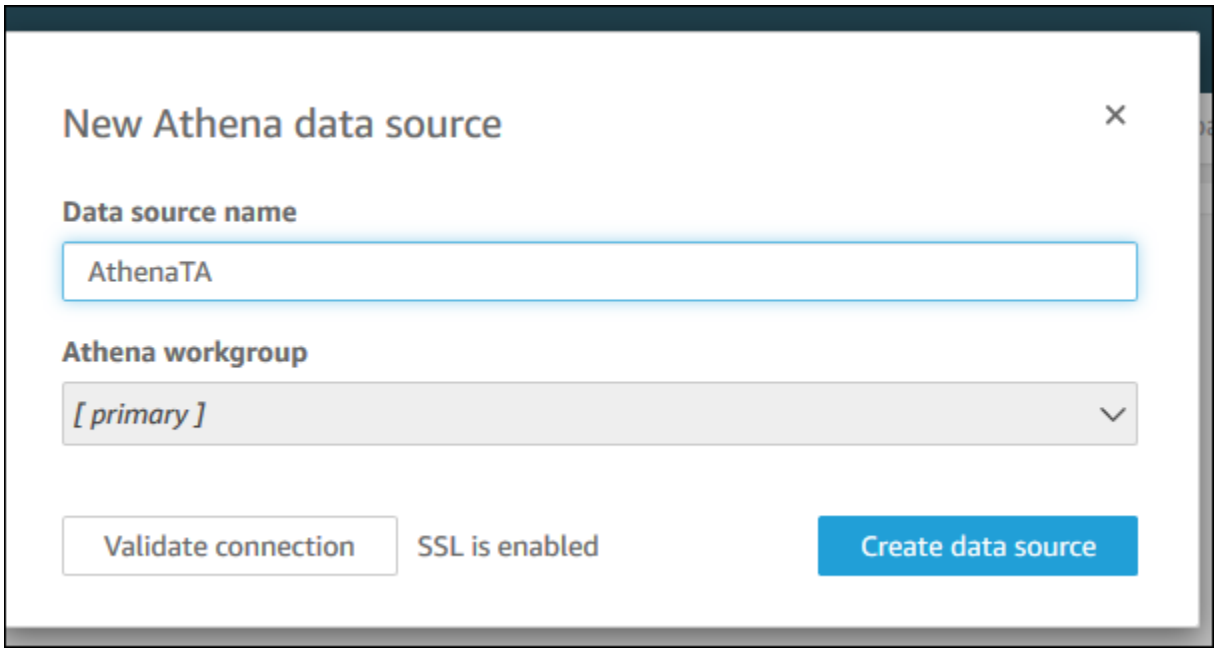
在 Quick Suite 中创建控制面板

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

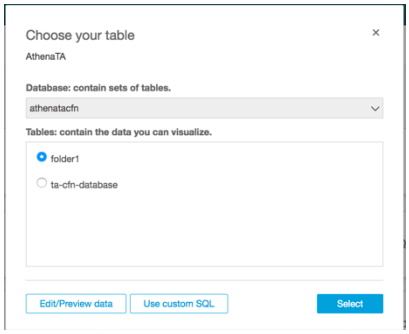
> **Note**
>
> 您必须使用美国东部（弗吉尼亚北部）区域。

要在 Quick Suite 中创建控制面板

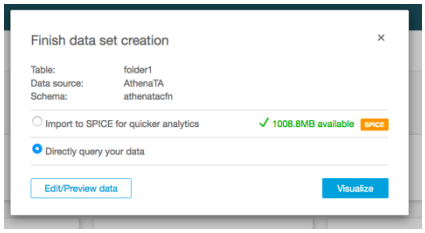
1. 导航到 Quick Suite 控制台，然后登录您的账户。
2. 选择 New analysis（新的分析）、New dataset（新数据集），然后选择 Athena。
3. 在 New Athena data source（新 Athena 数据源）对话框中，输入数据源名称，例如 AthenaTA，然后选择 Create data source（创建数据源）。



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）。



您现在可以在 Quick Suite 中创建控制面板。有关更多信息，请参阅《Amazon Quick Suite 用户指南》中的使用控制面板。

Example：Quick Suite 控制面板

以下示例仪表板显示有关 Trusted Advisor 检查的信息，例如：

- 受影响的账户 IDs
- Amazon 各地区摘要
- 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 Quick Suite 可以使用 Athena。有关更多信息，请参阅《Amazon Quick Suite 用户指南》中的无法连接到 Amazon Athena。

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

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 Amazon Glue 控制台查看架构，并快速确定报告中是否有重复的列。

要查找重复列

1. 打开 Amazon Glue 控制台，网址为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 “架构” 下查看 “列名” 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 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. 如果您还没有，请刷新您组织中账户的 Trusted Advisor 支票。请参阅刷新 Trusted Advisor 支票。
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。本教程中，您必须使用 JSON 文件。
3. 登录 Amazon Web Services 管理控制台 并打开 Amazon S3 控制台，网址为https://console.aws.amazon.com/s3/。
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 Amazon 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。

> **Note**
>
> 如果您对本教程仍有问题，您可以在 Amazon Web Services 支持 中心创建技术支持案例。

查看由 Amazon Trusted Advisor ... 提供支持的支票 Amazon Config

Amazon Config 是一项针对所需设置持续评估、审核和评估您的资源配置的服务。 Amazon Config 提供托管规则，这些规则是预定义的、可自定义的合规性检查， Amazon Config 用于评估您的 Amazon 资源是否符合常见的最佳实践。

Amazon Config 控制台将引导您完成托管规则的配置和激活。您还可以使用 Amazon Command Line Interface (Amazon CLI) 或 Amazon Config API 传递定义托管规则配置的 JSON 代码。您可以自定义托管规则的行为以满足您的需求。您可以自定义规则的参数，以便定义您的资源为符合规则而必须具备的属性。要了解有关启用的更多信息 Amazon Config，请参阅Amazon Config 开发者指南。

Amazon Config 托管规则支持对所有类别 Trusted Advisor 进行一组检查。启用某些托管规则后，相应的 Trusted Advisor 检查将自动启用。要查看哪些 Trusted Advisor 检查由特定的 Amazon Config 托管规则提供支持，请参阅Amazon Trusted Advisor 查看参考资料。

拥有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划的客户可以使用 Amazon Config 强化支票。如果您启用 Amazon Config 并拥有其中一个 Amazon Web Services 支持 计划，则会自动看到由相应已部署的 Amazon Config 托管规则支持的推荐。

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

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

我刚刚启用了录制和管理规则 Amazon Config，但我没有看到相应的 Trusted Advisor 检查。

Amazon Config 规则生成评估结果后，您可以近乎实时 Trusted Advisor 地看到结果。如果您遇到与此功能有关的问题，请在 Amazon Web Services 支持 Center 内创建技术支持案例。

我两次部署了同一个 Amazon Config 托管规则，我会看到什么 Trusted Advisor？

对于您安装的每个托管规则，您会在 Trusted Advisor 检查结果中看到单独的条目。

我关闭了 Amazon Config 在某个 Amazon 地区录制的功能。我会在里面看到 Trusted Advisor什么？

如果您 Amazon Config 在某个 Amazon 区域中关闭了资源记录，则 Trusted Advisor 不再接收相应托管规则的数据并在该区域进行检查。根据记录器保留策略 Amazon Config ，现有的托管规则结果会一

直保留， Trusted Advisor 直到 Amazon Config 到期。如果您删除托管规则，则 Trusted Advisor 支票数据通常会近乎实时地删除。

在中查看 Amazon Security Hub CSPM 控件 Amazon Trusted Advisor

启用 Amazon Security Hub CSPM 后 Amazon Web Services 账户，您可以在控制 Trusted Advisor 台中查看您的安全控制措施及其发现。您可以使用 Security Hub CSPM 控件来识别账户中的安全漏洞，就像使用 Trusted Advisor 检查一样。您可以查看支票的状态、受影响的资源列表，然后按照 Security Hub CSPM 的建议来解决您的安全问题。您可以使用此功能在一个方便的位置查找来自 Trusted Advisor 和 Security Hub CSPM 的安全建议。

注意

- 您可以从 Trusted Advisor中查看 Amazon 基础安全最佳实践安全标准中的控件，但类别为 “恢复” > “弹性” 的控件除外。有关受支持控件的列表，请参阅《Amazon Security Hub CSPM 用户指南》中的 Amazon 基础安全最佳实践控件。

  有关 Security Hub CSPM 类别的更多信息，请参阅控制类别。
- Trusted Advisor 在 2024 年 9 月 26 日之前上线的 Security Hub CSPM 控制措施。2024 年 9 月 26 日之后发布的控件尚未上线。 Trusted Advisor你可以在 Sec urity Hub CSPM 日志中找到在该日期之后发布的控件。

主题

先决条件

要启用 Security Hub CSPM 与的集成，您必须满足以下要求： Trusted Advisor

- 您必须有此功能的 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划。您可以从 Amazon Web Services 支持 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 Amazon Web Services 支持 套餐。
- 你必须在中 Amazon Config 为你想要的 Securit Amazon Web Services 区域 y Hub CSPM 控件启用资源记录。有关更多信息，请参阅启用和配置 Amazon Config。
- 您必须启用 Security Hub CSPM 并选择Amazon 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《Amazon Security Hub CSPM 用户指南》中的设置 Amazon Security Hub CSPM。

> **Note**
>
> 如果您已经满足了这些先决条件，则可以跳到 查看你的 Security Hub CSPM 调查结果。

关于 Amazon 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。个人会员账户无需联系 Amazon Web Services 支持 即可启用此功能。但是，组织中的成员帐户如果想在中查看自己的发现，则必须启用 Security Hub CSPM。 Trusted Advisor

如果要为特定的成员账户禁用此集成，请参阅为 Amazon Organizations 账户禁用此功能。

查看你的 Security Hub CSPM 调查结果

为您的账户启用 Security Hub CSPM 后，您的 Security Hub CSPM 发现最多可能需要 24 小时才能显示在控制台的 “安全” 页面上。 Trusted Advisor

要查看你的 Security Hub CSPM 调查结果，请访问 Trusted Advisor

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 S our ce，您可以选择Amazon Security Hub CSPM筛选 Security Hub CSPM 控件。

3. 选择 Security Hub CSPM 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 Amazon Trusted Advisor 还是 Amazon Security Hub CSPM。对于 Security Hub CSPM 控件，你可以找到控件 ID。
- Alert Criteria（提示标准）– 控件的状态。例如，如果 Security Hub CSPM 检测到重要问题，则状态可能为 “红色：严重” 或 “高”。
- 建议的操作-使用 Security Hub CSPM 文档链接查找修复问题的推荐步骤。
- S@@ ecurity Hub CSPM 资源 — 您可以在账户中找到 Security Hub CSPM 检测到问题的资源。

> **注意**
>
> - 您必须使用 Security Hub CSPM 将资源排除在搜索结果之外。目前，你无法使用 Trusted Advisor 控制台从 Security Hub CSPM 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 CSPM 的这种集成。您可以查看在整个组织中发现的 Security Hub CSPM 控制措施，然后创建和下载报告。有关更多信息，请参阅 的组织视图 Amazon Trusted Advisor。

刷新你的 Security Hub CSPM 调查结果

启用安全标准后，Security Hub CSPM 最多可能需要两个小时才能找到您的资源的结果。然后，该数据最多可能需要 24 小时才能显示在 Trusted Advisor 控制台中。如果您最近启用了Amazon 基础安全最佳实践 v1.0.0 安全标准，请稍后再次检查控制台。 Trusted Advisor

> **Note**
>
> - 每个 Security Hub CSPM 控件的刷新计划都是周期性的，或者是触发更改的。目前，你无法使用 Trusted Advisor 控制台或 Amazon Web Services 支持 API 刷新 Security Hub CSPM 控件。有关更多信息，请参阅运行安全检查的计划。
> - 如果要将资源排除在搜索结果之外，则必须使用 Security Hub CSPM。目前，你无法使用 Trusted Advisor 控制台从 Security Hub CSPM 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。

禁用 Security Hub CSPM Trusted Advisor

如果您不想让 Security Hub CSPM 信息显示在控制台中，请按照以下步骤操作。 Trusted Advisor 此过程仅禁用 Security Hub CSPM 与的集成。 Trusted Advisor它不会影响你使用 Security Hub CSPM 的配置。您可以继续使用 Security Hub CSPM 控制台来查看您的安全控制措施、资源和建议。

禁用 Security Hub CSPM 集成

1. 联系Amazon Web Services 支持并请求禁用 Security Hub CSPM 与的集成。 Trusted Advisor

   Amazon Web Services 支持 禁用此功能后，Security Hub CSPM 将不再向发送数据。 Trusted Advisor您的 Security Hub CSPM 数据将从中删除。 Trusted Advisor
2. 要重新启用此集成，请联系 Amazon Web Services 支持。

为 Amazon Organizations 账户禁用此功能

如果您已经完成了管理帐户的先前程序，则系统会自动从组织中的所有成员帐户中删除 Security Hub CSPM 集成。组织中的具体成员账户无需单独联系 Amazon Web Services 支持 。

如果您是组织中的成员帐户，则可以联系 Amazon Web Services 支持 以仅从您的帐户中删除此功能。

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

我在控制台中看不到 Security Hub CSPM 的调查结果 Trusted Advisor

确认您是否已完成以下步骤：

- 您有 B Amazon usiness Support+、E Amazon nterprise Suppor Amazon t 或统一运营计划。
- 您在与 Security Hub CSPM 相同的区域 Amazon Config 内启用了资源记录。
- 您启用了 Security Hub CSPM 并选择了Amazon 基础安全最佳实践 v1.0.0 安全标准。
- Security Hub CSPM 的新控件 Trusted Advisor 将在两到四周内作为办理登机手续的形式添加。请参阅说明。

有关更多信息，请参阅先决条件。

我 Amazon Config 正确配置了 Security Hub CSPM，但我的发现仍然缺失

Security Hub CSPM 最多可能需要两个小时才能找到您的资源的调查结果。然后，该数据最多可能需要 24 小时才能显示在 Trusted Advisor 控制台中。请稍后重新检查 Trusted Advisor 控制台。

> **注意**
>
> - 只有您在基础安全最佳实践安全标准中发现的控件才会显示在 “ Amazon 基础安全最佳实践” 安全标准中，但类别为 “恢复” > “弹性” 的控件 Trusted Advisor 除外。
> - 如果 Security Hub CSPM 存在服务问题，或者 Security Hub CSPM 不可用，则您的发现最多可能需要 24 小时才能显示出来。 Trusted Advisor请稍后重新检查 Trusted Advisor 控制台。

我想禁用特定的 Security Hub CSPM 控件

Security Hub CSPM 会自动将你的数据发送到。 Trusted Advisor 如果您禁用 Security Hub CSPM 控件或不再有该控件的资源，则您的发现结果将不会出现在中。 Trusted Advisor

您可以登录 Sec urity Hub CSPM 控制台并验证您的控件是启用还是禁用。

如果您禁用 Security Hub CSPM 控件或禁用 Amazon 基础安全最佳实践安全标准的所有控件，则您的发现将在接下来的五天内存档。这五天的归档期仅为近似值且仅尽力而为，并不能保证。当您的发现存档时，它们会从中删除 Trusted Advisor。

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

我想找到我排除的 Security Hub CSPM 资源

在 Trusted Advisor 控制台中，您可以选择您的 Security Hub CSPM 控件名称，然后选择 “排除的项目” 选项。此选项显示 Security Hub CSPM 中禁止的所有资源。

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。您无法从控制台中禁用 Security Hub CSPM 资源。 Trusted Advisor 为此，请使用 Sec urity Hub CSPM 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 Amazon 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 Amazon 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 Amazon Web Services 支持。

在 Security Hub CSPM 检查中，我看到同一个受影响的资源有多个 Amazon Web Services 区域

有些 Amazon Web Services 服务 是全球性的，并非特定于某个地区，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。

对于评估全球服务资源的 Security Hub CSPM 检查，您可能会看到多个受影响资源的项目。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 CSPM， Amazon Config 这样同一资源就不会出现多个区域。有关更多信息，请参阅您可能希望禁用的Amazon 基础最佳实践控件。

我关闭了 Security Hub CSPM 或者 Amazon Config 在某个区域中

如果您在中停止使用 Amazon Config 或禁用 Security Hub CSPM 的资源记录 Amazon Web Services 区域，则将 Trusted Advisor 不再接收该区域中任何控件的数据。 Trusted Advisor 在 7-9 天内移除你的 Security Hub CSPM 发现的内容。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 CSPM。

要为您的账户禁用此功能，请参阅 禁用 Security Hub CSPM Trusted Advisor。

我的控件已存档在 Security Hub CSPM 中，但我还能在 Security Hub CSPM 中看到调查结果 Trusted Advisor

当查找结果的`RecordState`状态更改`ARCHIVED`为时， Trusted Advisor 会从您的账户中删除该 Security Hub CSPM 控件的查找结果。您可能还会在 Trusted Advisor 7-9 天内看到搜索结果，然后再将其删除。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 CSPM 调查结果

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

选择使用 Amazon Compute Optimizer 支 Trusted Advisor 票

Compute Optimizer 服务可以分析 Amazon 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。使用 Compute Optimizer，您可以在支票中查看相同的建议。 Trusted Advisor

您可以选择加入您的 Amazon Web Services 账户 唯一账户，也可以选择加入属于组织的所有成员账户 Amazon Organizations。有关更多信息，请参阅《Amazon 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。然后，最多可能需要 48 小时才能查看以下检查 Trusted Advisor 的结果：

成本优化

- Amazon EBS 过度预调配卷
- Amazon Lambda 内存大小过度配置的函数

性能

- Amazon EBS 预调配不足的卷
- Amazon Lambda 内存大小的函数配置不足

> **注意**
>
> - 这些检查的结果每天至少会自动刷新一次，并且不允许刷新请求。更改可能需要几个小时才能显示。您可以使用 Trusted Advisor 控制台将资源排除在自

动刷新的支票之外。除了 Trusted Advisor Priority 推荐资源之外，您可以使用BatchUpdateRecommendationResourceExclusion该 API 将资源排除在任何支票之外。

- Trusted Advisor 已经有未充分利用的 Amazon EBS 卷和过度利用的 Amazon EBS 磁性卷检查。

  在您选择使用 Compute Optimizer 后，我们建议您改用新的 Amazon EBS 超额配置卷，改用 Amazon EBS 预配置不足的卷检查。

相关信息

有关更多信息，请参阅以下主题：

- 《Amazon Compute Optimizer 用户指南》中的查看 Amazon EBS 卷建议
- 《Amazon Compute Optimizer 用户指南》中的查看 Lambda 函数建议
- 《Amazon Lambda 用户指南》中的配置 Lambda 函数内存
- 在@@ 亚马逊 EC2 用户指南中请求修改您的 Amaz on EBS 卷

开始使用 P Amazon Trusted Advisor riority

Trusted Advisor Priority 可帮助您保护和优化自己 Amazon Web Services 账户 以遵循 Amazon Web Services 最佳实践。借助 P Trusted Advisor riority，您的 Amazon Web Services 账户 团队可以主动监控您的账户，并在为您发现机会时创建按优先顺序排列的建议。

例如，您的账户团队可以识别您的 Amazon 账户根用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 “优先级” 页面上显示为有效的 Trusted Advisor 优先级建议。然后您可以按照建议解决。

Trusted Advisor 优先建议来自以下两个来源：

- Amazon Web Services 服务 — 诸如 Trusted Advisor Amazon Security Hub CSPM、和 Well-Architect Amazon ed 之类的服务会自动创建推荐。您的客户团队会与您共享这些建议，以便这些推荐显示在 “ Trusted Advisor 优先级” 中。
- 您的客户团队 – 您的客户团队可以手动创建建议。

Trusted Advisor 优先级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 Pri Trusted Advisor ority 来查找组织中所有成员账户的推荐。

主题

先决条件

您必须满足以下要求才能使用 P Trusted Advisor riority：

- 您必须有 E Amazon nterprise Supp Amazon ort 或统一运营计划。
- 您的账户必须属于已启用 Amazon Organizations中所有功能的组织。有关更多信息，请参阅《Amazon Organizations 用户指南》中的启用企业中的所有功能。
- 您的组织必须已启用对的可信访问权限 Trusted Advisor。要启用可信访问权限，请以管理账户身份登录。在 Trusted Advisor 控制台中打开您的组织页面。
- 您必须登录自己的 Amazon 账户才能查看针对您的账户的 Trusted Advisor 优先级推荐。
- 您必须登录到组织的管理账户或委派管理员账户，才能查看组织的汇总建议。有关如何注册委派管理员账户的说明，请参阅 注册委派管理员。
- 您必须具有 Amazon Identity and Access Management (IAM) 权限才能访问 Trusted Advisor 优先级。有关如何控制对 Priority 的 Trusted Advisor 访问权限的信息，请参阅管理对的访问权限 Amazon Trusted Advisor和Amazon Web Services 的托管策略 Amazon Trusted Advisor。

启用 Trusted Advisor 优先级

请要求您的客户团队为您启用此功能。您必须制定 Amazon 统一运营计划，并且是贵组织的管理账户所有者。如果控制台中的 “ Trusted Advisor 优先级” 页面显示您需要使用进行可信访问 Amazon Organizations，请选择 “启用可信访问权限” Amazon Organizations。想要了解更多信息，请参阅先决条件部分。

查看优先建议

在您的账户团队为您启用 P Trusted Advisor riority 后，您可以查看针对您的 Amazon 账户的最新推荐。

查看优先建议

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 在 Trusted Advisor Priority 页面上，您可以查看以下项目：

   如果您使用的是 Amazon Organizations 管理或委派管理员帐户，请切换到 “我的帐户” 选项卡。

   - 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. 在有效选项卡上，有效的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 Amazon Web Services 服务您的 Amazon Web Services 账户 团队或计划中的服务活动。
     - 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、受其影响的资源以及建议操作。然后，您可以确认或忽略相应的建议。

查看组织中所有账户 Amazon 中按优先顺序排列的建议

管理账户和 P Trusted Advisor riority 授权的管理员都可以查看整个组织中汇总的推荐。

> **Note**
>
> 成员账户无权访问汇总的建议。

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 在 Trusted Advisor Priority 页面上，确保您位于我的组织选项卡上。
3. 要查看针对一个账户的推荐，请在从您的组织中选择一个账户下拉列表中选择一个账户。或者，您可以查看所有账户的建议。

   在我的组织选项卡上，您可以查看以下项目：

   - 所需操作：整个组织中正在等待响应或正在处理的建议的数量。
   - 概述：显示以下项目：
     - 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。
     - 解决建议所需的平均时间。
4. 在有效选项卡下，有效的优先建议部分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。此项可以是检查名称，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 Amazon Web Services 服务您的 Amazon Web Services 账户 团队或计划中的服务活动。

- 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。

5. 选择建议，以查看其他详细信息、受影响的账户和资源以及建议的操作。然后，您可以确认或忽略相应的建议。

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. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 如果您使用的是 Amazon Organizations 管理或委派管理员帐户，请切换到“我的帐户”选项卡。
3. 在 Trusted Advisor Priority 页面中的 Active（活动）选项卡下，选择一个建议名称。
4. 在详细信息部分，您可以查看建议的操作以解决建议。
5. 在受影响的资源部分中，您可以查看受影响的资源并按状态进行筛选。
6. 选择确认。
7. 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）。正在处理或等待回复的建议将显示在“ Trusted Advisor 优先级”页面的“活动”选项卡中。
8. 按照建议的操作解决建议。有关更多信息，请参阅 解决建议。

确认针对 Amazon 组织中所有账户的推荐

管理账户或 Trusted Advisor 委派管理员可以确认针对所有受影响账户的建议。

> **Note**
>
> 成员账户无权访问汇总的建议。

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 在 Trusted Advisor Priority 页面上，确保您位于我的组织选项卡上。
3. 在有效选项卡中，选择建议名称。

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）。
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。
7. 要查看建议的详细信息，请选择建议名称。

   在详细信息部分，您可以查看有关建议的以下信息：

   - 建议概述和详细信息部分涵盖了要完成的建议操作。

     状态摘要，显示所有受影响账户的建议。
   - 在受影响的账户部分中，您可以查看所有账户中受影响的资源。您可以按账号和状态进行筛选。
   - 在受影响的资源部分中，您可以查看所有账户中受影响的资源。您可以按账号和状态进行筛选。

忽略建议

您还可以忽略建议。也就是说，您会确认建议，但您不会处理该建议。如果建议与您的账户无关，您可以忽略该建议。例如，如果您计划删除某 Amazon Web Services 账户 项测试，则无需按照建议的操作进行操作。

忽略建议的方法

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 如果您使用的是 Amazon Organizations 管理或委派管理员帐户，请切换到 “我的帐户” 选项卡。
3. 在 Trusted Advisor Priority 页面中的 Active（活动）选项卡下，选择一个建议名称。
4. 在建议详细信息页面上，查看有关受影响资源的信息。
5. 如果此建议不适用于您的账户，请选择忽略。
6. 在忽略建议对话框中，选择您不处理该建议的原因。
7. （可选）输入注释，详细说明您忽略该建议的原因。如果您选择其他，则必须在备注部分输入说明。
8. 选择忽略。建议状态更改为 “已驳回”，并显示在 “ Trusted Advisor 优先级” 页面的 “已关闭” 选项卡中。

驳回针对组织中所有账户 Amazon 的推荐

管理账户或 Priority 的委 Trusted Advisor 托管理员可以驳回其所有账户的推荐。

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 在 “ Trusted Advisor 优先级” 页面上，确保您位于 “我的组织” 选项卡上。
3. 在有效选项卡中，选择建议名称。
4. 如果此建议不适用于您的账户，则选择忽略。
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）输入注释，详细说明您忽略该建议的原因。如果您选择其他，则必须在注释部分输入说明。
7. 选择忽略。建议状态将变为已忽略。该建议显示在 “ Trusted Advisor 优先级” 页面的 “已关闭” 选项卡中。

> **Note**
>
> 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驳回了该建议。

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”。

解决建议

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 在 “ Trusted Advisor 优先级” 页面上，确保您位于 “我的组织” 选项卡上。
3. 在 Trusted Advisor Priority 页面上，选择建议，然后选择 Resolve（解决）。

4. 在解决建议对话框中，选择解决。已解决的建议显示在 “ Trusted Advisor 优先级” 页面的 “已关闭” 选项卡下。 Trusted Advisor Priority 会通知您的客户团队您已解决该建议。

解决针对 Amazon 组织中所有账户的推荐

管理账户或 P Trusted Advisor riority 授权管理员可以解决其所有账户的推荐。

> **Note**
>
> 成员账户无权访问汇总的建议。

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 如果您使用的是 Amazon Organizations 管理或委派管理员帐户，请切换到 “我的帐户” 选项卡。
3. 在有效选项卡中，选择建议名称。
4. 如果该建议不适用于您的账户，请选择解析。
5. 在解决建议对话框中，选择解决。已解决的建议显示在 “ Trusted Advisor 优先级” 页面的 “已关闭” 选项卡下。 Trusted Advisor Priority 会通知您的客户团队您已解决该建议。

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. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 如果您使用的是 Amazon Organizations 管理或委派管理员帐户，请切换到 “我的帐户” 选项卡。
3. 在 Trusted Advisor Priority 页面，选择 Closed（已关闭）选项卡。
4. 在关闭的建议下，选择已忽略的建议，然后选择重新打开。
5. 在重新打开建议对话框中，说明重新打开建议的原因。
6. 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，然后选择查看注释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。

7. 按照建议详细信息中的步骤操作。

重新打开针对 Amazon 组织中所有账户的推荐

管理账户或 P Trusted Advisor riority 授权管理员可以为其所有账户重新打开推荐。

> **Note**
>
> 成员账户无权访问汇总的建议。

1. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
2. 在 “ Trusted Advisor 优先级” 页面上，确保您位于 “我的组织” 选项卡上。
3. 在关闭的建议下，选择已忽略的建议，然后选择重新打开。
4. 在重新打开建议对话框中，说明重新打开建议的原因。
5. 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。

6. 按照建议详细信息中的步骤操作。

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. 在家中 Trusted Advisor 登录https://console.aws.amazon.com/trustedadvisor/主机。
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。授权的管理员账户可以在 “ Trusted Advisor 优先级” 中查看、确认、解决、驳回和重新打开建议。

注册账户后，必须向委派的管理员授予访问 Trusted Advisor Prior Amazon Identity and Access Management ity 所需的权限。有关更多信息，请参阅管理对的访问权限 Amazon Trusted Advisor和Amazon Web Services 的托管策略 Amazon Trusted Advisor。

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。您必须登录到组织的管理账户，才能注册或取消注册委派管理员。

注册委派管理员

1. 以管理帐户身份在https://console.aws.amazon.com/trustedadvisor/家中登录主 Trusted Advisor 机。
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。不再是管理员授权的账户将不会收到来自 P Trusted Advisor riority 的电子邮件通知。

取消注册委派管理员

1. 以管理帐户身份在https://console.aws.amazon.com/trustedadvisor/家中登录主 Trusted Advisor 机。
2. 在导航窗格中的 Preferences（首选项）下，选择 Your organization（您的组织）。
3. 在委派管理员下，选择账户，然后选择注销。
4. 在此对话框中，选择 Deregister（注销）。

管理 Trusted Advisor 优先级通知

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托管理员，他们也可以将其账户设置为接收 P Trusted Advisor riority 电子邮件通知。

Trusted Advisor 优先电子邮件通知不包括个人账户的检查结果，与每周的 “ Trusted Advisor 推荐” 通知是分开的。有关更多信息，请参阅 设置通知首选项。

> **Note**
>
> 只有管理账户或授权管理员才能设置 Trusted Advisor 优先级电子邮件通知。

管理您的 Trusted Advisor 优先级通知

1. 以管理或委派管理员帐户在https://console.aws.amazon.com/trustedadvisor/家中登录 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. 对于收件人，选择希望其接收电子邮件通知其他联系人。您可以在 Amazon 账单与成本管理 控制台的 “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 从该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 优先级

请联系您的客户团队并让他们为您禁用此功能。禁用此功能后，您的 Trusted Advisor 控制台中将不再显示按优先顺序排列的推荐。

如果您禁用 P Trusted Advisor riority 然后稍后再次启用，您仍然可以查看您的账户团队在您禁用 Trusted Advisor Priority 之前发送的推荐。

Amazon Trusted Advisor 查看参考资料

您可以在以下参考资料中 Trusted Advisor 查看所有支票 IDs 的名称、描述和内容。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。

如果您有 B Amazon usiness Support+、En Amazon terprise Support 或 Amazon 统一运营计划，也可以使用 Amazon Trusted Advisor API 和 Amazon Command Line Interface (Amazon CLI) 来访问您的支票。有关更多信息，请参阅以下主题：

- 开始使用 Trusted Advisor API

> **Note**
>
> 如果您有 Basic Support 或 Developer Support 计划，则可以使用 Trusted Advisor 控制台访问该服务限制类别中的所有检查以及安全和容错类别中的以下检查：
>
> - Amazon S3 存储桶权限

- 安全组 – 不受限制的特定端口

> **Note**
>
> 您可以在中国区域中使用以下检查。

成本优化

您可以使用以下成本优化类别检查。

检查名称

- 闲置的负载均衡器
- 未关联的弹性 IP 地址

闲置的负载均衡器

说明

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）。

> **Note**
>
> 此检查会报告按标准标记的所有资源以及评估的资源总数，包括 OK 资源。资源表仅列出已标记的资源。

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。请参阅使用您的负载均衡器注册您的 Amazon EC2 实例或删除您的负载均衡器。

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

- Region
- 负载均衡器名称
- Reason
- 预估每月节省

未关联的弹性 IP 地址

说明

检查是否存在与正在运行的亚马逊弹性计算云 (EIPsAmazon EC2) 实例无关的弹性 IP 地址 ()。

EIPs 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，通过将公有 IP 地址重新映射到账户中的另一个实例来 EIPs 掩盖实例或可用区的故障。针对与正在运行的实例无关的 EIP，将收取名义费用。

> **Note**
>
> 此检查会报告按标准标记的所有资源以及评估的资源总数，包括 0K 资源。资源表仅列出已标记的资源。

检查 ID

Z4AUBRNSmz

提醒条件

黄色：分配的弹性 IP 地址 (EIP) 未与正在运行的 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

- Region
- IP 地址

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 DynamoDB Auto Scaling 未启用
- Amazon EBS 优化未启用
- Amazon EBS 预置 IOPS (SSD) 卷附件配置
- Amazon EBS 预调配不足的卷
- CPU 利用率高 Amazon EC2 实例
- 应用于实例的大量 EC2 安全组规则
- 一个 EC2 安全组中有大量规则
- 过度使用的 Amazon EBS 磁性介质卷

Amazon DynamoDB Auto Scaling 未启用

说明

检查您的 Amazon DynamoDB 表和全局二级索引是否启用了自动扩缩或按需。

Amazon DynamoDB Auto Scaling 使用 Application Auto Scaling 服务代表您动态调整预置的吞吐能力，以响应实际的流量模式。这将允许表或全局二级索引增大其预置的读取和写入容量以处理突发流量，而不进行限制。当工作负载减少时，Application Auto Scaling 可以减少吞吐量，这样您就无需为未使用的预置容量付费。

您可以使用 Amazon Config 规则中的参数调整检查配置。

有关更多信息，请参阅使用 DynamoDB Auto Scaling 自动管理吞吐能力。

> **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。
> 对于企业、企业入口或企业客户，您可以使用 BatchUpdateRecommendationResourceExclusionAPI 在 Trusted Advisor 结果中包含或排除一项或多项资源。

检查 ID

c18d2gz136

来源

Amazon Config 托管规则： dynamodb-autoscaling-enabled

提醒条件

黄色：未为您的 DynamoDB and/or 表全局二级索引启用自动缩放。

Recommended Action（建议的操作）

除非您已经有一种机制可以根据您的工作负载要求自动扩展 DynamoDB and/or 表和全局二级索引的预配置吞吐量，否则请考虑为您的 Amazon DynamoDB 表启用自动扩展。

有关更多信息，请参阅将 d ynamoDB Amazon Web Services 管理控制台 与 auto scalingp 配合使用。

其他资源

使用 DynamoDB Auto Scaling 自动管理吞吐能力

报告列

- Status

- Region
- 资源
- Amazon Config 规则
- 输入参数
- 上次更新时间

Amazon EBS 优化未启用

说明

检查您的亚马逊 EC2 实例是否启用了亚马逊 EBS 优化。

Amazon EBS 优化的实例使用优化的配置堆栈，为来自您的实例的 Amazon EBS I/O. This optimization provides the best performance for your Amazon EBS volumes by minimizing contention between Amazon EBS I/O 和其他流量提供额外的专用容量。

有关更多信息，请参阅 Amazon EBS 优化的实例。

> **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。
> 对于企业、企业入口或企业客户，您可以使用 BatchUpdateRecommendationResourceExclusionAPI 在 Trusted Advisor 结果中包含或排除一项或多项资源。

检查 ID

`c18d2gz142`

来源

Amazon Config 托管规则： ebs-optimized-instance

提醒条件

黄色：未在支持的亚马逊 EC2 实例上启用 Amazon EBS 优化。

Recommended Action（建议的操作）

在支持的实例上开启 Amazon EBS 优化。

有关更多信息，请参阅在启动时启用 EBS 优化。

其他资源

Amazon EBS 优化的实例

报告列

- Status
- Region
- 资源
- Amazon Config 规则
- 输入参数
- 上次更新时间

Amazon EBS 预置 IOPS (SSD) 卷附件配置

说明

检查挂载到未经 EBS 优化的亚马逊 EBS 优化的亚马逊弹性计算云 (Amazon EC2) 实例的预配置 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：可进行 EBS 优化的 Amazon EC2 实例附带预配置 IOPS (SSD) 卷，但该实例未经过过 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

- Status
- 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

说明

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。
> 对于企业、企业入口或企业客户，您可以使用 BatchUpdateRecommendationResourceExclusionAPI 在 Trusted Advisor 结果中包含或排除一项或多项资源。

检查 ID

`C0r6dfpM04`

提醒条件

黄色：回顾期间预置不足的 EBS 卷。为了确定卷是否配置不足，我们会考虑所有默认 CloudWatch 指标（包括 IOPS 和吞吐量）。用于识别资源不足的 EBS 卷的算法遵循 Amazon Web Services 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 选择使用 Amazon Compute Optimizer 支 Trusted Advisor 票。

报告列

- Status
- Region
- 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

CPU 利用率高 Amazon EC2 实例

说明

检查过去 14 天内任何时候运行的亚马逊弹性计算云 (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。

> **Note**
>
> 此检查会报告按标准标记的所有资源以及评估的资源总数，包括 OK 资源。资源表仅列出已标记的资源。

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

- 监控亚马逊 EC2
- 实例元数据和用户数据
- 《亚马逊 CloudWatch 用户指南》
- Amazon A EC2 uto 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

说明

检查是否有大量安全组规则的 EC2 实例。如果实例具有大量规则，性能可能会降低。

> **Note**
>
> 此检查会报告按标准标记的所有资源以及评估的资源总数，包括 OK 资源。资源表仅列出已标记的资源。

检查 ID

j3DFqYTe29

提醒条件

黄色： EC2-VPC 实例有超过 50 条安全组规则。

黄色： EC2-Classic 实例有超过 100 条安全组规则。

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

EC2 安全组

报告列

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

一个 EC2 安全组中有大量规则

说明

检查每个亚马逊弹性计算云 (Amazon EC2) 安全组中是否有过多的规则。

如果安全组具有大量规则，则性能可能会降低。

> **Note**
>
> 此检查会报告按标准标记的所有资源以及评估的资源总数，包括 OK 资源。资源表仅列出已标记的资源。

检查 ID

`tfg86AVHAZ`

提醒条件

黄色：Amazon EC2-VPC 安全组有超过 50 条规则。

黄色：Amazon EC2-Classic 安全组有 100 多条规则。

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，请参阅您的 EC2 实例的 Amazon EC2 安全组。

其他资源

- 亚马逊 EC2 安全组

报告列

- Region
- 安全组名称
- 组 ID
- 说明
- 实例计数
- - VPC ID
- 出站规则总数

过度使用的 Amazon EBS 磁性介质卷

说明

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

磁卷专为具有中等或突发 input/output (I/O) 要求的应用程序而设计，无法保证 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 用户指南

报告列

- Status
- Region
- 卷 ID
- 卷名
- 超过的天数
- 最大每日中值
- 出站规则总数

安全性

您可以使用以下安全类别检查。

> **Note**
>
> 如果您为启用了 Security Hub CSPM Amazon Web Services 账户，则可以在控制台中查看您的发现。 Trusted Advisor 有关信息，请参阅在中查看 Amazon Security Hub CSPM 控件 Amazon Trusted Advisor。
> 您可以查看 Amazon 基础安全最佳实践安全标准中的所有控件，但类别为 “恢复” > “弹性” 的控件除外。有关受支持控件的列表，请参阅《Amazon Security Hub CSPM 用户指南》中的 Amazon 基础安全最佳实践控件。

检查名称

- Amazon S3 存储桶权限
- ELB 侦听器安全
- 经典负载均衡器安全组
- IAM 密码策略
- 安全组 – 不受限制的特定端口
- 安全组 – 不受限制的访问

Amazon S3 存储桶权限

说明

检查 Amazon Simple Storage Service (Amazon S3) 中具有开放访问权限或允许任何经过身份验证的用户访问的存储桶。 Amazon

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

- 红色：存储桶 ACL 允许所有人或任何经过身份验证的 Amazon 用户进行列表 Upload/Delete 访问或访问权限，并且未启用 “阻止公共访问” 设置。
- 红色：存储桶策略允许公共访问，但未启用 “阻止公共访问” 设置。

- 红色： Trusted Advisor 无权查看政策，或者由于其他原因无法评估策略。
- 黄色：存储桶策略允许公开访问，但是 “限制公共存储桶” 设置已开启，仅允许该账户的授权用户进行访问。
- 黄色：存储桶合规，但未启用完整的阻止公共访问保护。
- 绿色：存储桶合规且已启用完全屏蔽公共访问保护。

> **Note**
>
> 启用 “阻止公共访问忽略公共访问” 后，不会评估公共 ACLs ACL 授权。

推荐操作

如果存储桶允许开放访问，请确定是否确实需要开放访问。例如，要托管静态网站，您可以使用 Amazon CloudFront 来提供托管在 Amazon S3 上的内容。请参阅《亚马逊 CloudFront 开发者指南》中的限制对 Amazon S3 来源的访问。如有可能，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

为 Amazon S3 存储桶配置阻止公共访问设置

报告列

- Status
- 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

ELB 侦听器安全

说明

检查带有侦听器的经典负载均衡器，这些负载均衡器不使用推荐的安全配置进行加密通信。Amazon 建议您使用安全协议（HTTPS 或 SSL）、 up-to-date安全策略以及安全的密码和协议。当您为前端连接（客户端到负载均衡器）使用安全协议时，客户端与负载均衡器之间的请求会被加密。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 Amazon 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

- 红色：负载均衡器的任何侦听器均未配置安全协议 (HTTPS)。
- 黄色：负载均衡器 HTTPS 侦听器配置了包含弱加密算法的安全策略。
- 黄色：负载均衡器 HTTPS 侦听器未配置推荐的安全策略。
- 绿色：负载均衡器至少有一个 HTTPS 侦听器，并且所有 HTTPS 侦听器都配置了推荐的策略。

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

- Status
- Region
- 负载均衡器名称
- 负载均衡器端口
- Reason

经典负载均衡器安全组

说明

检查负载均衡器是否配置了允许访问未针对负载均衡器配置的端口的安全组。

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。
- 绿色：与负载均衡器关联的 Amazon VPC 安全组的入站规则不允许访问未在负载均衡器的侦听器配置中定义的端口。

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
- 迁移 Classic Load Balancer
- 配置经典负载均衡器

报告列

- Status
- Region
- 负载均衡器名称
- 安全组 IDs
- Reason

IAM 密码策略

说明

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 Amazon 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

- 绿色：密码策略已启用，推荐内容要求已启用。
- 黄色：密码策略已启用，但至少有一项内容要求未启用。

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。

要访问 Amazon Web Services 管理控制台，IAM 用户需要密码。作为最佳实践， Amazon 强烈建议您使用联合身份验证，而不是创建 IAM 用户。联合身份验证允许用户使用其现有的公司凭证登录 Amazon Web Services 管理控制台。使用 IAM Identity Center 创建用户或联合用户，然后在账户中承担 IAM 角色。

要了解有关身份提供者和联合身份验证的更多信息，请参阅《IAM 用户指南》中的身份提供者和联合身份验证。要了解有关 IAM Identity Center 的更多信息，请参阅 IAM Identity Center 用户指南。

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

安全组 – 不受限制的特定端口

说明

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、数据丢失）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 地址入站规则。 Amazon 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，并且可以被排除。有关更多信息，请参阅 Trusted Advisor 常见问题。
>
> > **Note**
> >
> > 此检查会报告按标准标记的所有资源以及评估的资源总数，包括 OK 资源。资源表仅列出已标记的资源。

检查 ID

`HCP4007jGY`

提醒条件

- 绿色：安全组对端口 80、25、443 或 465 提供不受限制的访问。
- 红色：安全组附加到资源，对端口 20、21、22、1433、1434、3306、3389、4333、5432 或 5500 提供不受限制的访问。
- 黄色：安全组对任何其他端口提供不受限制的访问。
- 黄色：安全组未附加到任何资源，并且提供不受限制的访问。

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。

检查并删除未使用的安全组。您可以使用 Amazon Firewall Manager 大规模集中配置和管理安全组。有关更多信息 Amazon Web Services 账户，请参阅Amazon Firewall Manager 文档。

考虑使用 Systems Manager 会话管理器对 SSH（端口 22）和 RDP（端口 3389）访问实例。 EC2 使用会话管理器，您无需在安全组中启用端口 22 和 3389 即可访问您的 EC2 实例。

其他资源

- 亚马逊 EC2 安全组

  TCP 和 UDP 端口号列表
- 无类域间路由
- 使用会话管理器
- Amazon Firewall Manager

报告列

- Status
- Region
- 安全组名称
- 安全组 ID
- 协议
- 起始端口
- 终止端口
- 关联

安全组 – 不受限制的访问

说明

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、数据丢失）的机会。

> **Note**
>
> 此检查仅评估您创建的安全组及其 IPv4 地址入站规则。由创建的安全组 Amazon Directory Service 会被标记为红色或黄色，但它们不构成安全风险，可以排除在外。有关更多信息，请参阅 Trusted Advisor 常见问题。

> **Note**
>
> 此检查会报告按标准标记的所有资源以及评估的资源总数，包括 OK 资源。资源表仅列出已标记的资源。

检查 ID

1iG5NDGVre

提醒条件

- 绿色：安全组规则有一个后缀为 /0 的源 IP 地址，该规则适用于端口 25、80 或 443。
- 黄色：安全组规则有一个后缀为 /0 的源 IP 地址，用于 25、80 或 443 以外的端口，且安全组已附加到资源。
- 红色：安全组规则有一个后缀为 /0 的源 IP 地址，且该规则针对 25、80 或 443 以外的端口，同时安全组未附加到资源。

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。

检查并删除未使用的安全组。您可以使用 Amazon Firewall Manager 大规模集中配置和管理安全组。有关更多信息 Amazon Web Services 账户，请参阅Amazon Firewall Manager 文档。

考虑使用 Systems Manager 会话管理器对 SSH（端口 22）和 RDP（端口 3389）访问实例。 EC2 使用会话管理器，您无需在安全组中启用端口 22 和 3389 即可访问您的 EC2 实例。

其他资源

- 亚马逊 EC2 安全组
- 无类域间路由
- 使用会话管理器
- Amazon Firewall Manager

报告列

- Status
- Region

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

容错能力

您可以使用以下容错类别检查。

检查名称

- Amazon EBS 快照
- Amazon ElastiCache 多可用区集群
- Amazon MemoryDB 多可用区集群
- Amazon RDS 备份
- Amazon S3 存储桶日志记录
- Auto Scaling 组运行状况检查
- Auto Scaling 组资源
- ELB 连接耗尽
- 负载均衡器优化

Amazon EBS 快照

说明

检查 Amazon EBS 卷（可用或正在使用）的快照的存在时间。即使复制了 Amazon EBS 卷，也可能会发生故障。快照会保存到 Amazon S3 中，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。

要自动创建 EBS 快照，您可以考虑使用 Amazon Backup 或 Amazon Data Lifecycle Manager。

其他资源

Amazon Elastic Block Store（Amazon EBS）

Amazon EBS Snapshots

Amazon Backup

Amazon Data Lifecycle Manager

报告列

- Status
- Region
- 卷 ID
- 卷名
- 快照 ID
- 快照名称
- 快照期限
- 卷附件
- Reason

Amazon ElastiCache 多可用区集群

说明

检查在单个可用区 (AZ) 中部署的 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。

在多个区域部署通过异步复制到不同可用区的只读副本来 AZs 增强 ElastiCache 集群的可用性。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。
> 对于企业、企业入口或企业客户，您可以使用 BatchUpdateRecommendationResourceExclusionAPI 在 Trusted Advisor 结果中包含或排除一项或多项资源。

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。

推荐操作

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，请参阅使用多可用区最大限度地缩短 ElastiCache (Redis OSS) 中的停机时间。

报告列

- Status
- Region
- 集群名称
- 上次更新时间

Amazon MemoryDB 多可用区集群

说明

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。

在多个区域部署通过异步复制到不同可用区中的只读副本来 AZs 增强 MemoryDB 集群的可用性。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。
> 对于企业、企业入口或企业客户，您可以使用 BatchUpdateRecommendationResourceExclusionAPI 在 Trusted Advisor 结果中包含或排除一项或多项资源。

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

- Status
- Region
- 集群名称
- 上次更新时间

Amazon RDS 备份

说明

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。备份可降低数据意外丢失的风险并允许 point-in-time恢复。

> **Note**
>
> 此检查会报告按标准标记的所有资源以及评估的资源总数，包括 OK 资源。资源表仅列出已标记的资源。

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

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

Amazon S3 存储桶日志记录

说明

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，因此 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 Trusted Advisor 想检查日志记录状态，请将该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。

如果日志传送者没有目标的写入权限（未启用写入功能），请向日志传输 Upload/Delete 组授予权限。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

- Status
- Region

- 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

Auto Scaling 组运行状况检查

说明

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。如果不使用 Elastic Load Balancing 运行状况检查，Auto Scaling 只能对亚马逊弹性计算云 (Amazon EC2) 实例的运行状况采取行动。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 A EC2 uto Scaling 用户指南

报告列

- Status

- Region
- 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

说明

检查与启动配置、启动模板和自动扩缩组关联的资源的可用性。

指向不可用资源的 Auto Scaling 组无法启动新的亚马逊弹性计算云 (Amazon EC2) 实例。正确配置后，Auto Scaling 会使亚马逊 EC2 实例的数量在需求高峰期间无缝增加，并在需求平静期间自动减少。指向不可用资源的 Auto Scaling 组和启动 configurations/launch 模板无法按预期运行。

> **Note**
>
> 此检查会报告按标准标记的所有资源以及评估的资源总数，包括 OK 资源。资源表仅列出已标记的资源。

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。
- 红色：启动模板与已删除的亚马逊机器映像（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或目标组，然后将其关联到自动扩缩组；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 创建新的启动配置或启动模板版本，然后将其与自动扩缩组关联。有关如何创建新的启动配置的信息，请参阅 Amazon A EC2 uto Scaling 用户指南中的创

建启动配置。有关如何创建启动模板的信息，请参阅 Amazon A EC2 uto Scaling 用户指南中的为 Auto Sc aling 组创建启动模板。

> **Note**
>
> 出于安全考虑，检查结果不包括使用启动模板中的 Amazon Systems Manager 参数引用的任何资源。

如果您的启动模板包含包含亚马逊系统映像 (AMI) ID 的 Amazon Systems Manager 参数，请查看启动模板以确保参数引用有效的 AMI ID，或者在 Amazon Systems Manager 参数存储中进行适当的更改。有关更多信息，请参阅 Amazon A EC2 uto Scaling 用户指南 IDs中的使用 Amazon Systems Manager 参数代替 AMI。

其他资源

- Auto Scaling 疑难解答：亚马逊 EC2 AMIs
- 对 Auto Scaling 进行问题排查：负载均衡器配置
- Amazon A EC2 uto Scaling 用户指南
- 使用 Amazon Systems Manager 参数代替 AMI IDs

报告列

- Status
- Region
- 自动扩缩组名
- 启动类型
- 资源类型
- 资源名称

ELB 连接耗尽

说明

检查没有启用连接耗尽的经典负载均衡器。

如果未启用连接耗尽功能，并且您从经典负载均衡器注销 Amazon EC2 实例，则经典负载均衡器会停止将流量路由到该实例并关闭连接。启用连接耗尽后，经典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处理活动请求。

检查 ID

7qGXsKIUw

提醒条件

- 黄色：经典负载均衡器未启用连接耗尽。
- 绿色：经典负载均衡器已启用连接耗尽。

Recommended Action（建议的操作）

为经典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

- Status
- Region
- 负载均衡器名称
- Reason

负载均衡器优化

说明

检查您的负载均衡器配置。

为了帮助提高使用 Elastic Load Balancing 时亚马逊弹性计算云 (Amazon EC2) 的容错级别，我们建议在一个地区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：向负载均衡器注册的 Amazon EC2 实例在可用区之间的分布不均匀。（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

- Status
- Region
- 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

服务限制

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中的利用率或限制 Amazon Web Services 区域。

Recommended Action（建议的操作）

如果您预计超出服务限制，请直接从服务配额控制台请求增加。如果服务配额还不支持您的服务，则可以在支持中心打开支持案例。

报告列

- Status
- 服务
- Region
- 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

- DynamoDB 读取容量
- DynamoDB 写入容量
- EBS 活动快照
- EBS 通用型 SSD (gp2) 卷存储
- EBS 通用型 SSD (gp3) 卷存储
- EBS 磁介质（标准）卷存储
- EBS 预调配 IOPS SSD (io1) 卷聚合 IOPS
- EBS 预置 IOPS SSD (io1) 卷存储
- EC2 预留实例租约
- EC2-VPC 弹性 IP 地址
- ELB 经典负载均衡器

- VPC
- VPC 互联网网关

DynamoDB 读取容量

说明

检查使用量是否超过每个 Amazon Web Services 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

说明

检查使用量是否超过每个 Amazon Web Services 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

说明

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 通用型 SSD (gp2) 卷存储

说明

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

说明

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

说明

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 预调配 IOPS SSD (io1) 卷聚合 IOPS

说明

检查使用量是否超过 EBS 预调配 IOPS SSD (io1) 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

说明

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

EC2 预留实例租约

说明

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

亚马逊 EC2 配额

EC2-VPC 弹性 IP 地址

说明

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 经典负载均衡器

说明

检查使用量是否超过 ELB 经典负载均衡器配额的 80%。

检查 ID

`iK7O00l7J9`

其他资源

Elastic Load Balancing 配额

VPC

说明

检查使用量是否超过 VPC 配额的 80%。

检查 ID

`jL7PP0l7J9`

其他资源

VPC 配额

VPC 互联网网关

说明

检查使用量是否超过 VPC 互联网网关配额的 80%。

检查 ID

`kM7QQ0l7J9`

其他资源

VPC 配额

更改日志 Amazon Trusted Advisor

有关 Trusted Advisor 支票的最新更改，请参阅以下主题。

> **Note**
>
> 如果您使用 Trusted Advisor 控制台或 Amazon Web Services 支持 API，则已弃用的支票不会出现在检查结果中。如果您使用已弃用的支票，例如在 Amazon Web Services 支持 API 操作或代码中指定支票 ID，则会收到 API 调用错误。请删除这些检查以避免错误。

有关可用检查的更多信息，请参阅 Amazon Trusted Advisor 查看参考资料。

更改日期	检查名称	更改描述
2025 年 12 月 18 日	更新了 Amazon S3 存储桶版本控制	添加了新的警报标准： • 黄色： Trusted Advisor 无权验证版本控制
2025年12月17日	更新了 Amazon S3 存储桶权限	更新了警报条件部分。
2025 年 11 月 21 日	更新 Application Load Balancer 安全组	更新了 Application Load Balancer 安全组警报和建议。

更改日期	检查名称	更改描述
2025 年 11 月 17 日	在Amazon Web Services 区域 检查描述中更新了Amazon STS 全局端点的使用情况	更新了 Amazon Web Services 区域 检查描述中的 Amazon STS 全局端点使用情况，以阐明何时刷新检查结果。
2025 年 10 月 15 日	更新了多个检查描述	已在多个检查描述中添加注释，注明该检查会报告按标准标记的所有资源以及评估的资源总数，包括 0K 资源。资源表仅列出已标记的资源。
2025 年 10 月 10 日	更新了检查参考	已更新检查参考，以显示所有可用的检查。
2025 年 9 月 11 日	l4dfs2q4c5：使用已弃用运行时的函数 Amazon Lambda	已更新黄色提醒条件，注明包含至少 180 天内即将弃用的运行时。
2025 年 8 月 19 日	Pfx0RwqBli：亚马逊 S3 存储桶权限	提醒条件已更新：Trusted Advisor 无权检查策略或 ACL，或者出于其他原因无法评估策略或 ACL 从黄色更改为红色。
2025 年 7 月 3 日	Pfx0RwqBli：亚马逊 S3 存储桶权限	提醒条件已更新，以体现所有黄色和红色提醒对应的判定条件。
2025 年 7 月 3 日	c1dfprch15：带有 Ubuntu LTS 的 EC2 亚马逊实例已终止标准支持	已更新注释，注明此检查每天至少刷新一次。

更改日期	检查名称	更改描述
2025 年 7 月 2 日	c1dvkm4z6b：处于屏蔽模式的亚马逊 ECS 驱动程序 AWSLogs	Amazon ECS 将 awslogs 驱动程序日志配置参数模式的默认设置从 `blocking` 更改为 `non-blocking` 。黄色状态描述已更新，以反映此更改。
2025 年 7 月 2 日	7 注意DAFEmo事项：根账户的 MFA	新增了信息，说明可集中删除成员账户的根用户凭证，无需再管理根用户凭证的 MFA。
2025 年 6 月 9 日	c1z7kmr17n：针对数据库集群存储的 Amazon Aurora 成本优化建议	新检查
2025 年 6 月 9 日	c15m0mgld3：全球终端节点的使用情况 Amazon STSAmazon Web Services 区域	更新的支票：此支票现在适用于所有 Amazon Web Services 支持 计划。
2025 年 4 月 30 日	• n420c450f2：备用域名 CloudFront • n425c450f2：IAM 证书存储区中的 CloudFront 自定义 SSL 证书	添加了一条注释，表明此检查适用于传统的 Amazon CloudFront 分配。
2025 年 4 月 30 日	n415c450f2：标头转发和缓存命中率 CloudFront	添加了一条注释，表明此检查适用于传统的 Amazon CloudFront 分配。
2025 年 4 月 2 日	c1dfprch02：Amazon EFS 吞吐量模式优化	此检查的描述已更改。有关更多信息，请参阅终止支持微软 Windows Server 的亚马逊 EC2 实例。

更改日期	检查名称	更改描述
2025 年 4 月 2 日	Qsdfp3A4L4：带有微软 Windows Server 的亚马逊 EC2 实例终止支持	此检查的描述已更改。有关更多信息，请参阅 Amazon EFS 吞吐量模式优化。

较早的更新

以下 Amazon Security Hub CSPM 检查已被弃用：

检查名称	检查 ID
S3.10 - 启用了版本控制的 S3 通用存储桶应具有生命周期配置	Hs4Ma3G211
S3.11 - S3 通用存储桶应已启用事件通知	Hs4Ma3G212
CodeBuild.5- CodeBuild 项目环境不应启用特权模式	Hs4Ma3G218
CloudFormation.1- CloudFormation 堆栈应与亚马逊简单通知服务 (SNS) Simple Notification Service 集成	Hs4Ma3G245
SNS.2 - 发送到主题的通知消息应启用传输状态日志记录	Hs4Ma3G263
Athena.1 - Athena 工作组应进行静态加密	Hs4Ma3G294

更新了自动扩缩组资源检查

Trusted Advisor 2024 年 12 月 23 日更新了以下支票。

检查名称	检查类别	检查 ID
Auto Scaling 组资源	容错能力	8CNsSllI5v

此检查的描述已更新，新增了启动配置和启动模板的相关内容。

新增了提醒条件 `Red: A launch template is associated with a deleted Amazon Machine Image (AMI).`。

有关更多信息，请参阅 Auto Scaling 组资源。

新增了 1 项检查

Trusted Advisor 2024 年 11 月 22 日增加了 1 张新支票：

- 8604e947f2 - 应用程序负载均衡器安全组

更新了 3 项检查

Trusted Advisor 2024 年 11 月 7 日更新了 3 张支票：

- b92b83d667 - ELB 目标不均衡
- 8 CNs slli5v-Auto Scaling 组资源
- wuy7g1zxQL-亚马逊可用区域余额 EC2

新增了 4 项检查

Trusted Advisor 2024 年 10 月 11 日增加了 4 张新支票：

- 07602fcad6 - IAM Access Analyzer - 外部访问权限
- 528d6f5ee7 - GWLB - 端点可用区
- c2vlfg0jp6 - 非活动的 VPC 接口端点
- c2vlfg0k35 - 非活动的网关负载均衡器端点

更新了 3 项检查

Trusted Advisor 2024 年 10 月 2 日更新了 3 张支票：

- 检查 ID 7040ea389a 已从成本优化支柱移至容错能力支柱
- 已更新支票 ID 7 DAFEmo Dos
- 更新了检查 ID Cmsvnj8db2

新增了 9 项新检查

Trusted Advisor 2024 年 8 月 23 日新增了 9 张支票：

- c2vlfg0p86 - [IAM] - SAML 2.0 身份提供者
- 7040ea389a - Network Firewall 端点跨可用区数据传输
- c2vlfg0bfw - 低利用率 Network Firewall
- c2vlfg0gqd - Network Firewall 多可用区
- c2vlfg0p1w - 应用程序负载均衡器目标组加密协议
- c2vlfg022t - [NAT 网关] - 未充分利用的资源
- c243hjzrhn-单机架部署 Amazon Outposts
- b92b83d667 - ELB 目标不均衡
- 90046ff5b5 - MSK 可用性仅限于两个可用区

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

更新了 1 项安全检查并新增了 1 项安全检查

Trusted Advisor 2024 年 8 月 22 日更新了 1 项卓越运营检查：

- c1fd6b96l4

Trusted Advisor 在 2024 年 8 月 22 日增加了 1 次安全检查：

- c2vlfg0f4h

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

更新了 6 项安全检查

Trusted Advisor 2024 年 8 月 20 日更新了 6 项安全检查：

- nNauJisYIT
- c9D319e7sG
- a2sec6 ILx
- HCP4007jgy

- 1lg5 NDGVre
- Yw2K9puPzl

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

更新了 1 项容错能力检查

Trusted Advisor 2024 年 8 月 12 日更新了 1 个容错检查和 1 个安全检查：

- VPN 隧道冗余
- 需要升级 Amazon RDS 引擎次要版本

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

更新了 9 项检查

Trusted Advisor 在 2024 年 7 月 21 日更新了 9 张支票：

- 7q GXs KIUw
- ZRxQlPsb6c
- N425c450f2
- 7 个注意DAFEmo事项
- Pfx0 RwqBli
- H7 lgTzj TYb
- C056F80cR3
- Yw2K9puPzl
- xSqX82fQu

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

移除了 5 项检查并新增了 1 项检查

Trusted Advisor 2024 年 5 月 15 日弃用了 3 个容错检查、1 个性能检查和 1 个安全检查：

- IAM 使用

- ELB 跨区域负载均衡
- 过度使用的 Amazon EBS 磁性介质卷
- 应用于实例的大量 EC2 安全组规则
- EC2 安全组中有大量规则

Trusted Advisor 2024 年 5 月 15 日增加了 1 项新的安全检查：

- Amazon S3 服务器访问日志已启用

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

移除了容错能力检查

Trusted Advisor 2024 年 4 月 25 日弃用了 3 个容错检查：

- Amazon Direct Connect 连接冗余
- Amazon Direct Connect 位置冗余
- Amazon Direct Connect 虚拟接口冗余

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

新的容错能力检查

Trusted Advisor 在 2024 年 2 月 29 日添加了 1 个容错检查：

- NLB - 私有子网中面向互联网的资源

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

更新了容错能力检查和安全检查

Trusted Advisor 2024 年 3 月 28 日增加了 1 项新的容错检查并修改了 1 项现有容错检查和 1 项安全检查：

- 添加了 Amazon Resilience Hub 应用程序组件检查
- 更新了支持 Amazon Lambda vPC 的功能，但没有多可用区冗余

- 使用已弃用的运行时更新了 Amazon Lambda 函数

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

新的容错能力检查

Trusted Advisor 在 2024 年 1 月 31 日添加了 1 个容错检查：

- Amazon Direct Connect 位置弹性

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

更新了容错能力检查

Trusted Advisor 2024 年 1 月 8 日修订了 1 项容错检查：

- Amazon RDS innodb_flush_log_at_trx_commit 参数不是 1

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

更新了安全检查

Trusted Advisor 2023 年 12 月 21 日修改了 1 张安全检查：

- Amazon Lambda 使用已弃用运行时的函数

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

新的安全和性能检查

Trusted Advisor 2023 年 12 月 20 日新增了 2 项安全检查和 2 项新的性能检查：

- Amazon EFS 客户端未使用 data-in-transit加密
- Amazon Aurora 数据库集群的读取工作负载预调配不足
- Amazon RDS 实例的系统容量预调配不足
- 带有 Ubuntu LTS 的亚马逊 EC2 实例已终止标准支持

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

新的安全检查

Trusted Advisor 2023 年 12 月 15 日增加了 1 张新的安全检查：

- Amazon Route 53 中直接指向 S3 存储桶的不匹配 CNAME 记录

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

新的容错能力和成本优化检查

Trusted Advisor 2023 年 12 月 7 日添加了 2 个新的容错检查和 1 个新的成本优化检查：

- Amazon DocumentDB 单可用区集群
- Amazon S3 未完成的分段上传中止配置
- Amazon ECS Amazon日志驱动程序处于屏蔽模式

有关更多信息，请参阅Amazon Trusted Advisor 查看参考资料。

Trusted Advisor 检查删除

检查名称	检查类别	检查 ID
EBS 卷应连接到实例 EC2	安全性	Hs4Ma3G119
S3 存储桶应启用服务器端加密	安全性	Hs4Ma3G167
CloudFront 发行版应启用源访问身份	安全性	Hs4Ma3G195

与集 Trusted Advisor 成的更新 Amazon Security Hub CSPM

Trusted Advisor 2022 年 11 月 17 日进行了以下更新。

如果您禁用 Security Hub CSPM 或禁 Amazon Config 用 Trusted Advisor 了 Amazon Web Services 区域，那么现在会 Amazon Web Services 区域 在 7-9 天内删除您对此的控制结果。以前，从中删除 Security Hub CSPM 数据的时间范围 Trusted Advisor 为 90 天。

有关更多信息，请参阅 问题排查 主题中的以下章节：

- 我关闭了 Security Hub CSPM 或者 Amazon Config 在某个区域中
- 我的控件已存档在 Security Hub CSPM 中，但我还能在 Security Hub CSPM 中看到调查结果 Trusted Advisor

更新到控制 Trusted Advisor 台

Trusted Advisor 2022 年 11 月 16 日添加了以下更改。

控制台中的控制 Trusted Advisor 面板现在是 “ Trusted Advisor 推荐”。 Trusted Advisor 建议页面仍然显示检查结果以及关于您 Amazon Web Services 账户每个类别的可用检查。

此名称更改仅更新 Trusted Advisor 控制台。您可以像往常一样继续使用 Trusted Advisor 控制台和 Amazon Web Services 支持 API 中的 Trusted Advisor 操作。

有关更多信息，请参阅 开始使用 Trusted Advisor 建议。

将 Security Hub CSPM 支票添加到 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 CSPM控件。此版本支持 Amazon 基础安全最佳实践安全标准中的所有控件，但类别：恢复 > 弹性中的控件除外。有关更多信息，请参阅 在中查看 Amazon Security Hub CSPM 控件 Amazon Trusted Advisor。

有关受支持控件的列表，请参阅《Amazon Security Hub CSPM 用户指南》中的 Amazon 基础安全最佳实践控件。

添加了来自的支票 Amazon Compute Optimizer

Trusted Advisor 2022 年 5 月 4 日添加了以下支票。

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`
Amazon Lambda 内存大小过度配置的函数	成本优化	`COr6dfpM05`
Amazon Lambda 内存大小的函数配置不足	性能	`COr6dfpM06`

你必须选择 Compute Optimizer，这样这些支票才能从你的 Lambda 和 Amazon EBS 资源中接收数据。 Amazon Web Services 账户 有关更多信息，请参阅 选择使用 Amazon Compute Optimizer 支 Trusted Advisor 票。

更新了对 Amazon Direct Connect的检查

Trusted Advisor 2022 年 3 月 29 日更新了以下支票。

检查名称	检查类别	检查 ID
Amazon Direct Connect 连接冗余	容错能力	`0t121N1Ty3`
Amazon Direct Connect 位置冗余	容错能力	`8M012Ph3U5`
Amazon Direct Connect 虚拟接口冗余	容错能力	`4g3Nt5M1Th`

- Region（区域）列的值现已显示 Amazon Web Services 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，表格中仅显示 Trusted Advisor 建议您进行调查的资源。这些资源旁边拥有一个警告图标 ( )。

更新了 Amazon OpenSearch 服务的支票名称

Trusted Advisor 2021 年 9 月 8 日更新了Amazon OpenSearch Service Reserved Instance Optimization支票的名称。

检查建议、类别和 ID 是相同的。

检查名称	检查类别	检查 ID
Amazon OpenSearch 服务预留实例优化	成本优化	7ujm6yhn5t

> **Note**
>
> 如果您使用 Trusted Advisor 亚马逊 CloudWatch 指标，则此检查的指标名称也会更新。有关更多信息，请参阅 创建 Amazon CloudWatch 告警以监控 Amazon Trusted Advisor 指标。

增加了 Amazon Elastic Block Store 卷存储的检查

Trusted Advisor 2021 年 6 月 8 日添加了以下支票。

检查名称	检查类别	检查 ID
EBS 通用型 SSD (gp3) 卷存储	服务限制	dH7RR0l6J3

添加了支票 Amazon Lambda

Trusted Advisor 2021 年 3 月 8 日添加了以下支票。

检查名称	检查类别	检查 ID
Amazon Lambda 超时时间过长的函数	成本优化	L4dfs2Q3C3
Amazon Lambda 错误率高的函数	成本优化	L4dfs2Q3C2
Amazon Lambda 使用已弃用运行时的函数	安全性	L4dfs2Q4C5
Amazon Lambda 不带多可用区冗余的启用 VPC 的功能	容错能力	L4dfs2Q4C6

有关如何在 Lambda 中使用这些检查的更多信息，请参阅Amazon Lambda 开发人员指南中的查看推荐 Amazon Trusted Advisor 的工作流程示例。

Trusted Advisor 检查删除

Trusted Advisor 2021 年 3 月 8 日删除了中国（北京）地区的以下支票。

检查名称	检查类别	检查 ID
EC2 弹性 IP 地址	服务限制	aW9HH0l8J6

更新了 Amazon Elastic Block Store 的检查

Trusted Advisor 2021 年 3 月 5 日，为了进行以下检查，将亚马逊 EBS 交易量的单位从千兆字节 (GiB) 更新为 tebibyte (TiB)。

> **Note**
>
> 如果您使用 Trusted Advisor 亚马逊 CloudWatch 指标，则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 Amazon CloudWatch 告警以监控 Amazon Trusted Advisor 指标。

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	服务限制	gH5CC0e3J9	冷 HDD (sc1) 卷存储 (TiB)
EBS 通用型 SSD (gp2) 卷存储	服务限制	dH7RR0l6J9	通用型 SSD (gp2) 卷存储 (TiB)
EBS 磁介质（标准）卷存储	服务限制	cG7HH0l7J9	磁介质（标准）卷存储 (TiB)
EBS 预置 IOPS SSD (io1) 卷存储	服务限制	gI7MM0l7J9	预置 IOPS (SSD) 存储 (TiB)

检查名称	检查类别	检查 ID	更新了的 CloudWatch 指标 ServiceLimit
EBS 吞吐量优化型 HDD (st1) 卷存储	服务限制	wH7DD0l3J9	吞吐量优化型 HDD (st1) 卷存储 (TiB)

Trusted Advisor 检查删除

> **Note**
>
> Trusted Advisor 2020 年 11 月 18 日删除了以下支票。

2020 年 11 月 18 日删除的检查	检查类别	检查 ID
EC2适用于 EC2 Windows 实例的 Config 服务	容错能力	V77i0LlBqz
ENA适用于 EC2 Windows 实例的驱动程序版本	容错能力	TyfdMXG69d
NVMe适用于 EC2 Windows 实例的驱动程序版本	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
EBS 活动卷	服务限制	fH7LL0l7J9

Amazon Elastic Block Store 对您可以预置的卷数量不再有相应的限制。

您可以使用 S Amazon ystems Manager Distribut or 或其他第三方工具监控您的亚马逊 EC2 实例并验证它们是否是最新的，也可以编写自己的脚本来返回 Windows 管理工具 (WMI) 的驱动程序信息。

Trusted Advisor 检查删除

Trusted Advisor 2020 年 2 月 18 日删除了以下支票。

检查名称	检查类别	检查 ID
Service Limits	性能	eW7HH0l7J9

安全性 Amazon Web Services 支持

云安全 Amazon 是重中之重。作为 Amazon 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方 Amazon 的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础架构。 Amazon 还为您提供可以安全使用的服务。作为的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用的合规计划 Amazon Web Services 支持，请参阅 vices 按合规计划划分的范围内的服务。
- 云端安全 — 您的责任由您 Amazon Web Services 服务 使用的内容决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用时如何应用分担责任模型 Amazon Web Services 支持。以下主题向您展示如何进行配置 Amazon Web Services 支持 以满足您的安全和合规性目标。您还将学习如何使用其他 Amazon Web Services 来帮助您监控和保护您的 Amazon Web Services 支持 资源。

主题

中的数据保护 Amazon Web Services 支持

分 Amazon 分担责任模型适用于中的数据保护 Amazon Web Services 支持。如本模型所述 Amazon ，负责保护运行所有内容的全球基础架构 Amazon Web Services 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 Amazon Web Services 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。

出于数据保护目的，我们建议您保护 Amazon Web Services 账户 凭证并使用 Amazon IAM Identity Center 或 Amazon Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 Amazon 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 Amazon CloudTrail。有关使用 CloudTrail 跟踪捕获 Amazon 活动的信息，请参阅《Amazon CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 Amazon 加密解决方案以及其中的所有默认安全控件 Amazon Web Services 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 Amazon 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://www.amazonaws.cn/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API Amazon Web Services 支持 或以其他 Amazon Web Services 服务 方式使用控制台 Amazon CLI、API 或时 Amazon SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

> **Important**
>
> 在通信中，切勿共享敏感信息，例如凭证、信用卡 URLs、签名或个人身份信息。

为您的手机 Amazon Web Services 支持 壳提供安全保障

创建支持案例时，您的支持案例中包含的信息归您所有。 Amazon 未经您的许可，不会访问您的 Amazon Web Services 账户 数据。 Amazon 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：

- Amazon Web Services 支持 使用`AWSServiceRoleForSupport`服务相关角色中定义的权限呼叫其他 Amazon Web Services 服务 人为您解决客户问题。有关更多信息，请参阅使用服务相关角色 Amazon Web Services 支持和Amazon 托管策略： AWSSupportServiceRolePolicy。

- 您可以查看在您的中发生 Amazon Web Services 支持 的 API 调用 Amazon Web Services 账户。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，请参阅使用记录 Amazon Web Services 支持 API 调用 Amazon CloudTrail。
- 您可以使用 Amazon Web Services 支持 API 来调用 `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。在案例创建后，您最多可以查看 24 个月的案例详情。有关更多信息，请参阅《Amazon Web Services 支持 API Reference》中的 DescribeCases。
- 您的支持案例遵循 Amazon Web Services 支持的合规性验证。
- 当您创建支持案例时， Amazon 无法访问您的帐户。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。 Amazon Web Services 支持 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Amazon Web Services 支持 FAQs。
- 您可以更改 Amazon Web Services 支持 套餐以获得账户所需的帮助。有关更多信息，请参阅比较 Amazon Web Services 支持 套餐和更改 Amazon Web Services 支持 套餐。

的身份和访问管理 Amazon Web Services 支持

Amazon Identity and Access Management (IAM) Amazon Web Services 服务 可帮助管理员安全地控制对 Amazon 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 Amazon Web Services 支持 资源。您可以使用 IAM Amazon Web Services 服务 ，无需支付额外费用。

主题

- Amazon Trusted Advisor的示例服务控制策略
- 对 Amazon Web Services 支持 身份和访问进行故障排除

受众

您的使用方式 Amazon Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅对 Amazon Web Services 支持 身份和访问进行故障排除）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅如何 Amazon Web Services 支持 与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅Amazon Web Services 支持 基于身份的策略示例）

使用身份进行身份验证

身份验证是您 Amazon 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 Amazon Web Services 账户根用户，或者通过担任 IAM 角色进行身份验证。

对于编程访问， Amazon 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的Amazon 签名版本 4。

Amazon 账户 root 用户

创建时 Amazon Web Services 账户，首先会有一个名为 Amazon Web Services 账户 root 用户的登录身份，该身份可以完全访问所有资源 Amazon Web Services 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关要求根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 Amazon 使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用 Amazon CLI 或 Amazon API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon 上运行的应用程序非常有用。 EC2有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用策略管理访问

您可以 Amazon 通过创建策略并将其附加到 Amazon 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 Amazon 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 Amazon 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

基于身份的策略

基于身份的策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

基于身份的策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

其他策略类型

Amazon 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)-在中指定组织或组织单位的最大权限 Amazon Organizations。有关更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。

- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《Amazon Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 Amazon 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 Amazon Web Services 支持 与 IAM 配合使用

在使用 IAM 管理访问权限之前 Amazon Web Services 支持，您应该了解哪些可用的 IAM 功能 Amazon Web Services 支持。要全面了解如何 Amazon Web Services 支持 和其他 Amazon 服务与 IAM 配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的Amazon 服务。

有关如何管理 Amazon Web Services 支持 使用 IAM 的访问权限的信息，请参阅管理访问权限 Amazon Web Services 支持。

主题

- Amazon Web Services 支持 基于身份的策略
- Amazon Web Services 支持 IAM 角色

Amazon Web Services 支持 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。 Amazon Web Services 支持 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 Amazon JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

正在执行的策略操作在操作前 Amazon Web Services 支持 使用以下前缀:`support:`. 例如，要授予某人通过 Amazon EC2 `RunInstances` API 操作运行亚马逊 EC2 实例的权限，您需要将

该ec2:RunInstances操作包含在他们的策略中。策略语句必须包括 Action 或 NotAction 元素。Amazon Web Services 支持 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 Amazon Web Services 支持 操作列表，请参阅 IAM 用户指南 Amazon Web Services 支持中的定义操作。

示例

要查看 Amazon Web Services 支持 基于身份的策略的示例，请参阅。Amazon Web Services 支持 基于身份的策略示例

Amazon Web Services 支持 IAM 角色

I AM 角色是您的 Amazon 账户中具有特定权限的实体。

将临时证书与 Amazon Web Services 支持

可以使用临时凭证进行联合身份验证登录，分派 IAM 角色或分派跨账户角色。您可以通过调用AssumeRole或之类的 Amazon STS API 操作来获取临时安全证书GetFederationToken。

Amazon Web Services 支持 支持使用临时证书。

服务关联角色

服务相关角色允许 Amazon 服务访问其他服务中的资源以代表您完成操作。服务关联角色显示在 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关联角色的权限。

Amazon Web Services 支持 支持服务相关角色。有关创建或管理 Amazon Web Services 支持 服务相关角色的详细信息，请参阅将服务关联角色用于 Amazon Web Services 支持。

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他服务中的资源以代表您完成操作。服务角色显示在 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。

Amazon Web Services 支持 支持服务角色。

Amazon Web Services 支持 基于身份的策略示例

默认情况下，IAM 用户和角色没有创建或修改 Amazon Web Services 支持 资源的权限。他们也无法使用 Amazon Web Services 管理控制台 Amazon CLI、或 Amazon API 执行任务。IAM 管理员必须创建 IAM 策略，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
- 使用 Amazon Web Services 支持 控制台
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略非常强大。它们决定是否有人可以在您的账户中创建、访问或删除 Amazon Web Services 支持 资源。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 Amazon 托管策略 — 要 Amazon Web Services 支持 快速开始使用，请使用 Amazon 托管策略为员工提供所需的权限。这些策略已在您的账户中提供，并由 Amazon维护和更新。有关更多信息，请参阅 IAM 用户指南中的使用 Amazon 托管策略的权限入门。
- 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 Amazon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 Amazon Web Services 支持 控制台

要访问 Amazon Web Services 支持 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您 Amazon 账户中 Amazon Web Services 支持 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。

为确保这些实体仍然可以使用 Amazon Web Services 支持 控制台，还要将以下 Amazon 托管策略附加到这些实体。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

对于仅调用 Amazon CLI 或 Amazon API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与您尝试执行的 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或使用 Amazon CLI 或 Amazon API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
```

```
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

使用服务关联角色

Amazon Web Services 支持 并 Amazon Trusted Advisor 使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是与 Amazon Web Services 支持 和 Trusted Advisor直接关联的独特 IAM 角色。在每个案例中，服务关联角色是预定义的角色。此角色包括代表您调用其他 Amazon 服务 Amazon Web Services 支持 或 Trusted Advisor 需要的所有权限。以下主题说明了服务相关角色的作用以及如何在 Amazon Web Services 支持 和 Trusted Advisor中使用它们。

主题

- 将服务关联角色用于 Amazon Web Services 支持
- 将服务关联角色用于 Trusted Advisor

将服务关联角色用于 Amazon Web Services 支持

Amazon Web Services 支持 工具通过 API 调用收集有关您的 Amazon 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计性，请 Amazon Web Services 支持 使用 Amazon Identity and Access Management (IAM) 服务相关角色。

`AWSServiceRoleForSupport`服务相关角色是直接链接到 Amazon Web Services 支持的独特 IAM 角色。此服务相关角色是预定义的，它包括代表您调用其他 Amazon 服务 Amazon Web Services 支持 所需的权限。

`AWSServiceRoleForSupport` 服务关联角色信任 `support.amazonaws.com` 服务来代入角色。

为了提供这些服务，角色的预定义权限 Amazon Web Services 支持 允许访问资源元数据，而不是客户数据。只有 Amazon Web Services 支持 工具才能担任此角色，该角色存在于您的 Amazon 账户中。

我们会编辑可能包含客户数据的字段。例如， Amazon Step Functions API 调GetExecutionHistory用的Input和Output字段对用户不可见 Amazon Web Services 支持。我们使用 Amazon KMS keys 加密敏感字段。这些字段已在 API 响应中被删除， Amazon Web Services 支持 代理不可见。

> **Note**
>
> Amazon Trusted Advisor 使用单独的 IAM 服务相关角色访问账户的 Amazon 资源，以提供最佳实践建议和检查。有关更多信息，请参阅 将服务关联角色用于 Trusted Advisor。

AWSServiceRoleForSupport服务相关角色允许客户通过 Amazon CloudTrail查看所有 Amazon Web Services 支持 API 调用。这有助于满足监控和审计要求，因为它提供了一种透明的方式来了解代表您 Amazon Web Services 支持 执行的操作。有关的信息 CloudTrail，请参阅《Amazon CloudTrail 用户指南》。

的服务关联角色权限 Amazon Web Services 支持

此角色使用AWSSupportServiceRolePolicy Amazon 托管策略。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 — Amazon 客户服务使用托管策略授予的权限来执行作为支持计划一部分的多项服务。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。
- 处理您 Amazon 账户的服务属性和使用情况数据 — Amazon Web Services 支持 可能会使用托管策略授予的权限来访问您 Amazon 账户的服务属性和使用数据。该政策 Amazon Web Services 支持 允许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。
- 维护您的账户及其资源的运行状况 —— Amazon Web Services 支持 使用自动化工具执行与运营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**
>
> Amazon Web Services 支持 每月自动更新一次AWSSupportServiceRolePolicy策略，以添加新 Amazon 服务和操作的权限。

有关更多信息，请参阅 Amazon 的托管策略 Amazon Web Services 支持。

为创建服务相关角色 Amazon Web Services 支持

您无需手动创建 AWSServiceRoleForSupport 角色。创建 Amazon 账户时，系统会自动为您创建和配置此角色。

> **Important**
>
> 如果您在开始支持服务相关角色 Amazon Web Services 支持 之前使用该角色，则在您的账户中 Amazon 创建了该AWSServiceRoleForSupport角色。有关更多信息，请参阅我的 IAM 账户中出现新角色。

编辑和删除的服务相关角色 Amazon Web Services 支持

您可以使用 IAM 编辑 AWSServiceRoleForSupport 服务关联角色的描述。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

该AWSServiceRoleForSupport角色是为您的账户 Amazon Web Services 支持 提供管理、运营和技术支持所必需的。因此，无法通过 IAM 控制台、API 或 Amazon Command Line Interface (Amazon CLI) 删除此角色。这将保护您的 Amazon 账户，因为您不会无意中删除管理支持服务所需的权限。

已加入 Amazon Organizations 并拥有企业 Amazon Web Services 支持 套餐的客户可以删除该AWSServiceRoleForSupport服务相关角色。删除此角色会限制 Amazon Web Services 支持 工程师访问您的资源，从而限制他们代表您执行操作的能力。有关更多信息，或者如需请求删除 AWSServiceRoleForSupport 服务关联角色，请联系您的技术客户经理 (TAM)。

有关 AWSServiceRoleForSupport 角色或其使用的更多信息，请联系 Amazon Web Services 支持。

将服务关联角色用于 Trusted Advisor

Amazon Trusted Advisor 使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是直接链接到 Amazon Trusted Advisor的唯一 IAM 角色。服务相关角色由预定义 Trusted Advisor，它们包括该服务代表您调用其他 Amazon 服务所需的所有权限。 Trusted Advisor 使用此角色来检查您的使用情况， Amazon 并提供改善 Amazon 环境的建议。例如， Trusted Advisor 分析您的亚马逊弹性计算云 (Amazon EC2) 实例使用情况，以帮助您降低成本、提高性能、容忍故障和提高安全性。

> **Note**
>
> Amazon Web Services 支持 使用单独的 IAM 服务相关角色访问您账户的资源，以提供账单、管理和支持服务。有关更多信息，请参阅 将服务关联角色用于 Amazon Web Services 支持。

有关支持服务关联角色的其他服务的信息，请参阅与 IAM 配合使用的Amazon 服务。查找在 Service-linked role（服务关联角色）列的值为 Yes（是）的服务。请选择是与查看该服务的服务关联角色文档的链接。

主题

- 的服务关联角色权限 Trusted Advisor
- 管理服务关联角色的权限
- 为 创建服务关联角色 Trusted Advisor
- 为 Trusted Advisor编辑服务关联角色
- 删除 Trusted Advisor的服务关联角色

的服务关联角色权限 Trusted Advisor

Trusted Advisor 使用两个与服务相关的角色：

- AWSServiceRoleForTrustedAdvisor— 此角色信任 Trusted Advisor 服务代替您访问 Amazon 服务的角色。角色权限策略允许对所有 Amazon 资源进行 Trusted Advisor 只读访问。此角色简化了 Amazon 账户的入门流程，因为您不必为添加必要的权限 Trusted Advisor。当您开设 Amazon 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。
- AWSServiceRoleForTrustedAdvisorReporting – 此角色信任 Trusted Advisor 服务来担任组织视图功能的角色。此角色可 Trusted Advisor 作为 Amazon Organizations 组织中的可信服务启用。 Trusted Advisor 启用组织视图时会为您创建此角色。

  有关附加策略的更多信息，请参阅 AWSTrustedAdvisorReportingServiceRolePolicy。

  您可以使用组织视图为组织中的所有账户创建 Trusted Advisor 检查结果报告。有关此特征的更多信息，请参阅的组织视图 Amazon Trusted Advisor。

管理服务关联角色的权限

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。以下示例使用 AWSServiceRoleForTrustedAdvisor 服务关联角色。

Example：允许 IAM 实体创建 AWSServiceRoleForTrustedAdvisor 服务关联角色

只有在禁用 Trusted Advisor 帐户、删除服务相关角色并且用户必须重新创建角色才能重新启用时，才需要执行此步骤。 Trusted Advisor

将以下语句添加到 IAM 实体的权限策略可创建服务关联角色。

```
{
    "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 服务关联角色的描述

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关联角色的描述。

```
{
    "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 服务关联角色

您可以将以下语句添加到 IAM 实体的权限策略来删除服务关联角色。

```
{
```

```
    "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 Amazon 托管策略（例如 AdministratorAccess）来提供对的完全访问权限 Trusted Advisor。

为 创建服务关联角色 Trusted Advisor

无需手动创建 AWSServiceRoleForTrustedAdvisor 服务关联角色。当您开设 Amazon 账户时，Trusted Advisor 会为您创建服务相关角色。

> **Important**
>
> 如果您在服务开始支持 Trusted Advisor 服务相关角色之前使用该服务，则 Trusted Advisor 已经在您的账户中创建了该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 服务关联角色， 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关联角色，可能会出现上述情况。在这种情况下，您可以使用 IAM 创建 AWSServiceRoleForTrustedAdvisor 服务关联角色，然后重新启用 Trusted Advisor。

启用 Trusted Advisor （控制台）

1. 使用 IAM 控制台或 IAM API 为创建服务相关角色。 Amazon CLI Trusted Advisor有关更多信息，请参阅创建服务关联角色。
2. 登录 Amazon Web Services 管理控制台，然后导航到 Trusted Advisor 控制台，网址为https://console.amazonaws.cn/trustedadvisor。

   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 “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编辑服务关联角色

由于多个实体可能引用该角色，因此无法更改服务关联角色的名称。但是，您可以使用 IAM 控制台或 IAM API 来编辑角色的描述。 Amazon CLI有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

删除 Trusted Advisor的服务关联角色

如果您不需要使用的功能或服务 Trusted Advisor，则可以删除该AWSServiceRoleForTrustedAdvisor角色。必须 Trusted Advisor 先禁用此服务相关角色，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。禁用后 Trusted Advisor，即禁用所有服务功能，包括离线处理和通知。此外，如果您 Trusted Advisor 为成员账户禁用，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节省成本的方法的 Trusted Advisor 支票。您无法访问 Trusted Advisor 控制台。API 调用 Trusted Advisor 返回拒绝访问错误。

您必须在 AWSServiceRoleForTrustedAdvisor 账户中重新创建服务关联角色，然后才能重新启用 Trusted Advisor。

必须先在控制台 Trusted Advisor 中禁用服务相关角色，然后才能删除AWSServiceRoleForTrustedAdvisor服务相关角色。

要禁用 Trusted Advisor

1. 登录 Amazon Web Services 管理控制台 并导航到 Trusted Advisor 控制台，网址为https://console.amazonaws.cn/trustedadvisor。
2. 在导航窗格中，选择首选项。
3. 在服务关联角色权限部分中，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。

禁用后 Trusted Advisor，所有 Trusted Advisor 功能都将被禁用，并且 Trusted Advisor 控制台仅显示禁用状态横幅。

然后，您可以使用 IAM 控制台 Amazon CLI、或 IAM API 删除名AWSServiceRoleForTrustedAdvisor为的 Trusted Advisor 服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

Amazon 的托管策略 Amazon Web Services 支持

Amazon 托管策略是由创建和管理的独立策略 Amazon。 Amazon 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， Amazon 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新 Amazon 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 Amazon 最有可能在启动新的 API 或现有服务可以使用新 Amazon Web Services 服务 的 API 操作时更新 Amazon 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

主题

Amazon 的托管策略 Amazon Web Services 支持

Amazon Web Services 支持 具有以下托管策略。

目录

Amazon 托管策略：AWSSupportAccess

Amazon Web Services 支持 使用AWSSupportAccess Amazon 托管策略。此政策通过 Amazon Web Services 支持 API 管理您的支持案例生命周期。中的增强功能 Amazon Support Center Console 是通过支持控制台 API 服务提供的。您可以将此策略附加到 IAM 实体。有关更多信息，请参阅 的服务关联角色权限 Amazon Web Services 支持。

要查看此策略的权限，请参阅《Amazon 托管式策略参考》中的 AWSSupportAccess。

Amazon 托管策略：AWSSupportServiceRolePolicy

Amazon Web Services 支持 使用AWSSupportServiceRolePolicy Amazon 托管策略。此托管策略附加到 AWSServiceRoleForSupport 服务关联角色。该策略允许服务关联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 的服务关联角色权限 Amazon Web Services 支持。

要查看此策略的权限，请参阅《Amazon 托管式策略参考》中的 AWSSupportServiceRolePolicy。

有关对策略的更改列表，请参阅 Amazon Web Services 支持Amazon 托管策略的更新 和 AWSSupportServiceRolePolicy 的权限更改。

Amazon Web Services 支持Amazon 托管策略的更新

查看 Amazon Web Services 支持 自这些服务开始跟踪这些更改以来的 Amazon 托管策略更新的详细信息。要获得有关此页面更改的自动提示，请订阅 文档历史记录 页面上的 RSS 源。

下表描述了自 2022 年 2 月 17 日以来 Amazon Web Services 支持 托管策略的重要更新。

Amazon Web Services 支持

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	向以下服务添加了 145 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： • Amazon Amplify — 解决与相关的问题 Amazon Amplify。 • Amazon AppSync — 调试与相关的问题 Amazon AppSync。	2025年12月8日

更改	描述	日期
	• Amazon Outposts — 调试与相关的问题 Amazon Outposts。 • Amazon 清洁室-用于解决与 Amazon 洁净室有关的问题。 • Amazon Compute Optimizer — 调试与相关的问题 Amazon Compute Optimizer。 • Amazon Connect – 调试与 Amazon Connect 相关的问题。 • Amazon DynamoDB – 调试与 Amazon DynamoDB 相关的问题。 • Amazon EMR – 排查与 Amazon EMR 相关的问题。 • Amazon Location Service — 解决与亚马逊定位服务相关的问题；。 • 亚马逊 GuardDuty -调试与亚马逊相关的问题 GuardDuty。 • Amazon Network Firewall — 调试与相关的问题 Amazon Network Firewall。 • Amazon HealthOmics — 解决与相关的问题 Amazon HealthOmics。 • Amazon Organizations — 调试与相关的问题 Amazon Organizations。	

更改	描述	日期
	• Amazon S3 – 调试与 Amazon S3 相关的问题。 • 亚马逊 S3 表-调试与亚马逊 S3 表相关的问题。 • 亚马逊 S3 向量 — 调试与亚马逊 S3 矢量相关的问题。 • 亚马逊 SageMaker AI — 用于解决与亚马逊 A SageMaker I 相关的问题。 • Amazon Security Hub CSPM — 解决与相关的问题 Amazon Security Hub CSPM。 • 亚马逊 SES — 调试与亚马逊 SES 相关的问题。 • Amazon Signer — 调试与相关的问题 Amazon Signer。 • Amazon STS — 解决与相关的问题 Amazon STS。	

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	向以下服务添加了 125 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： • 用于 IT 运营的人工智能 (AIOps) — 调试与 IT 运营人工智能相关的问题 (AIOps)。 • Amazon Backup gateway — 解决与相关的问题 Amazon Backup gateway。 • Amazon CloudFormation — 调试与相关的问题 Amazon CloudFormation。 • Amazon Cognito Identity – 调试与 Amazon Cognito Identity 相关的问题。 • Amazon Cognito – 排查与 Amazon Cognito 相关的问题。 • Amazon Backup — 调试与相关的问题 Amazon Backup。 • Amazon Directory Service — 调试与相关的问题 Amazon Directory Service。 • 亚马逊 EC2 -调试与亚马逊相关的问题 EC2。 • Amazon FIS — 解决与相关的问题 Amazon FIS。 • 亚马逊 FSx -解决与亚马逊相关的问题 FSx。	2025年9月30日

更改	描述	日期
	• Amazon Global Accelerator — 调试与相关的问题 Amazon Global Accelerator。 • Amazon 身份存储-调试与 Amazon 身份存储相关的问题。 • Amazon Web Services 开票 — 调试与相关的问题 Amazon Web Services 开票。 • Amazon Lake Formation — 解决与相关的问题 Amazon Lake Formation。 • Amazon Network Firewall — 调试与相关的问题 Amazon Network Firewall。 • Oracle Database@Amazon — 用于解决与 Oracle Database@ 相关的问题。Amazon • Amazon S3 – 调试与 Amazon S3 相关的问题。 • Amazon SES – 排查与 Amazon SES 相关的问题。 • Amazon IAM Identity Center — 解决与相关的问题 Amazon IAM Identity Center。	
AWSSupportAccess：对现有策略的更新	在 AWSSupportAccess 托管策略中添加了支持控制台 API 的权限。	2025 年 7 月 18 日

更改	描述	日期
AWSSupportServiceRolePolicy：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： • Amazon CloudFormation — 调试与相关的问题 Amazon CloudFormation。 • Amazon Config — 解决与相关的问题 Amazon Config。 • 亚马逊 OpenSearch 服务-调试与亚马逊 OpenSearch 服务相关的问题。 • Amazon Glue — 调试与相关的问题 Amazon Glue。 • Amazon IAM — 用于解决与 Amazon IAM 相关的问题。 • Amazon Pinpoint：解决与 Amazon Pinpoint 相关的问题。 • Amazon Outposts — 调试与相关的问题 Amazon Outposts。 • Amazon STS — 调试与相关的问题 Amazon STS。 有关更多信息，请参阅 AWSSupportServiceRolePolicy 的权限更改。	2025 年 7 月 15 日

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	向以下服务添加了 257 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： • Amazon App Runner — 调试与相关的问题 Amazon App Runner。 • Amazon AppSync — 解决与相关的问题 Amazon AppSync。 • Amazon Batch — 调试与相关的问题 Amazon Batch。 • Amazon Bedrock – 排查与 Amazon Bedrock 相关的问题。 • 亚马逊 CloudFront -调试与亚马逊相关的问题 CloudFront。 • Amazon CodePipeline — 解决与相关的问题 Amazon CodePipeline。 • Amazon Config — 解决与相关的问题 Amazon Config。 • Amazon Connect – 调试与 Amazon Connect 相关的问题。 • Amazon DataSync — 调试与相关的问题 Amazon DataSync。 • Amazon Direct Connect — 解决与相关的问题 Amazon Direct Connect。	2025 年 6 月 17 日

更改	描述	日期
	• 亚马逊 EC2 — 解决与亚马逊相关的问题 EC2。 • Amazon 故障注入服务-调试与 Amazon 故障注入服务相关的问题。 • Amazon Firewall Manager — 解决与相关的问题 Amazon Firewall Manager。 • Amazon Glue — 调试与相关的问题 Amazon Glue。 • 亚马逊 GuardDuty — 调试与亚马逊相关的问题 GuardDuty。 • EC2 Image Builder — 用于解决与 EC2 图像生成器相关的问题。 • Amazon IoT — 解决与相关的问题 Amazon IoT。 • Amazon IoT FleetWise — 调试与相关的问题 Amazon IoT FleetWise。 • Amazon CloudWatch 日志-用于调试与亚马逊 CloudWatch 日志相关的问题。 • AWS Elemental MediaLive — 调试与相关的问题 AWS Elemental MediaLive。 • 网络流量监测仪 - 排查与网络流量监测仪相关的问题。 • Amazon Network Manager — 解决与相关的问	

更改	描述	日期
	题 Amazon Network Manager。 • Amazon CloudWatch 可观测性管理服务-用于解决与亚马逊 CloudWatch 可观测性管理服务相关的问题。 • Amazon 并行计算服务-调试与 Amazon 并行计算服务相关的问题。 • Amazon Redshift Serverless – 排查与 Amazon Redshift Serverless 相关的问题。 • Amazon Redshift – 排查与 Amazon Redshift 相关的问题。 • Amazon Resilience Hub — 调试与相关的问题 Amazon Resilience Hub。 • Amazon Anywhere 身份和访问管理角色 — 随时随地调试与 Amazon 身份和访问管理角色相关的问题。 • Amazon S3 on Outposts – 排查与 Amazon S3 on Outposts 相关的问题。 • Amazon S3 – 排查与 Amazon S3 相关的问题。 • Amazon S3 表类数据存储服务 – 排查与 Amazon S3 表相关的问题。 • 亚马逊 SageMaker AI — 调试与亚马逊 A SageMaker I 相关的问题。	

更改	描述	日期
	• Amazon Security Hub CSPM — 调试与相关的问题 Amazon Security Hub CSPM。 • Amazon SQS – 调试与 Amazon SQS 相关的问题。 • Amazon Systems Manager Incident Manager — 解决与相关的问题 Amazon Systems Manager Incident Manager。 • Amazon Systems Manager 快速设置-调试与 Amazon Systems Manager 快速设置相关的问题。 • Amazon Systems Manager — 调试与相关的问题 Amazon Systems Manager。 • 亚马逊 WorkSpaces 瘦客户机-用于解决与亚马逊 WorkSpaces 瘦客户机相关的问题。 • Amazon Timestream – 调试与 Amazon Timestream 相关的问题。 • Amazon Telco Network Builder — 用于解决与 Amazon 电信网络生成器相关的问题。 • Amazon Transfer Family — 调试与相关的问题 Amazon Transfer Family。	

更改	描述	日期
	• Amazon VPC Lattice – 排查与 Amazon VPC Lattice 相关的问题。	
AWSSupportServiceRolePolicy：对现有策略的更新	为以下服务添加了 88 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： • Amazon Bedrock – 排查与 Amazon Bedrock 相关的问题。 • Amazon Connect – 调试与 Amazon Connect 相关的问题。 • 亚马逊 DataZone -调试与亚马逊相关的问题 DataZone。 • 亚马逊 EC2 — 解决与亚马逊相关的问题 EC2。 • Amazon EKS – 调试与 Amazon EKS 相关的问题。 • Amazon Glue — 解决与相关的问题 Amazon Glue。 • 适用于 Apache Flink 的亚马逊托管服务 – 排查与适用于 Apache Flink 的亚马逊托管服务相关的问题。 • Amazon Lambda — 调试与相关的问题 Amazon Lambda。	2024 年 11 月 25 日

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	向以下服务添加了 79 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： • Amazon OpenSearch Serverless — 用于解决与亚马逊 OpenSearch 无服务器相关的问题。 • Amazon AppConfig — 调试与相关的问题 Amazon AppConfig。 • Application Signals – 调试与 Application Signals 相关的问题。 • Amazon Athena – 排查与 Amazon Athena 相关的问题。 • 亚马逊 CloudWatch — 调试与亚马逊相关的问题 CloudWatch。 • Amazon DynamoDB – 排查与 Amazon DynamoDB 相关的问题。 • 亚马逊 EC2 — 解决与亚马逊相关的问题 EC2。 • Amazon IoT — 调试与相关的问题 Amazon IoT。 • Amazon Lambda — 解决与相关的问题 Amazon Lambda。	2024 年 10 月 8 日

更改	描述	日期
	• Amazon Launch Wizard — 解决与相关的问题 Amazon Launch Wizard。 • Amazon Security Hub CSPM — 调试与相关的问题 Amazon Security Hub CSPM。 • 亚马逊 WorkSpaces — 调试与亚马逊相关的问题 WorkSpaces。	

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	向以下服务添加了 79 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： • Amazon Web Services 账户 — 解决与相关的问题 Amazon Web Services 账户。 • Amazon Auto Scaling — 调试与相关的问题 Amazon Auto Scaling。 • Amazon Bedrock – 调试与 Amazon Bedrock 相关的问题。 • Amazon CodeConnections — 解决与相关的问题 Amazon CodeConnections。 • Amazon 截止日期云 — 调试与 Amazon 截止日期云相关的问题。 • Amazon Elastic Kubernetes Service – 排查与 Amazon Elastic Kubernetes Service 相关的问题。 • Elastic Load Balancing – 排查与 Elastic Load Balancing 相关的问题。 • Amazon 免费套餐-调试与 Amazon 免费套餐相关的问题。	2024 年 8 月 5 日

更改	描述	日期
	• Amazon Inspector – 排查与 Amazon Inspector 相关的问题。 • Amazon OpenSearch Ingestion — 用于解决与亚马逊 OpenSearch 摄取相关的问题。 • 亚马逊 WorkSpaces -调试与亚马逊相关的问题 WorkSpaces。 • Amazon X-Ray — 调试与相关的问题 Amazon X-Ray。	

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	为以下服务添加了 17 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： • Amazon CloudWatch 网络监视器-用于解决与网络监控服务相关的问题。 • Amazon CloudWatch 日志-用于调试与亚马逊 CloudWatch 日志相关的问题。 • Amazon Managed Streaming for Apache Kafka – 调试与 Amazon Managed Streaming for Apache Kafka 相关的问题。 • Amazon Managed Service for Prometheus – 排查与 Amazon Managed Service for Prometheus 相关的问题。	2024 年 3 月 22 日

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	向以下服务添加了 63 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： • Amazon 洁净室-用于解决与 Amazon 洁净室有关的问题。 • CodeConnections — 解决与相关的问题 CodeConnections。 • Amazon EKS – 调试与 Amazon EKS 相关的问题。 • Image Builder – 调试与 Image Builder 相关的问题。 • Amazon Inspector2 – 排查与 Amazon Inspector2 相关的问题。 • Amazon Inspector Scan – 调试与 Amazon Inspector Scan 相关的问题。 • Amazon CloudWatch 日志-用于解决与亚马逊 CloudWatch 日志相关的问题。 • Amazon Outposts — 解决与相关的问题 Amazon Outposts。 • Amazon RDS – 调试与 Amazon RDS 相关的问题。 • Amazon IAM Identity Center — 解决与相关的	2024 年 1 月 17 日

更改	描述	日期
	问题 Amazon IAM Identity Center。 • Amazon S3 Express – 调试与 Amazon S3 Express 相关的问题。 • Amazon Trusted Advisor — 解决与相关的问题 Amazon Trusted Advisor。	

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	向以下服务添加了 126 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： • Amazon Direct Connect — 解决与 Amazon Direct Connect 服务有关的问题。 • 亚马逊 SageMaker AI — 用于解决与亚马逊 A SageMaker I 服务相关的问题。 • 亚马逊 AppStream -调试与亚马逊相关的问题 AppStream。 • Amazon 资源探索器 — 调试与相关的问题 Amazon 资源探索器。 • Amazon Redshift Serverless – 排查与 Amazon Redshift Serverless 相关的问题。 • 亚马逊 ElastiCache — 调试与亚马逊相关的问题 ElastiCache。 • Amazon Comprehend – 排查与 Amazon Comprehend 相关的问题。 • 亚马逊 EC2 — 解决与亚马逊相关的问题 EC2。 • Amazon Elastic Kubernetes Service – 用于调试与 Amazon Elastic Kubernetes Service 相关的问题。	2023 年 12 月 6 日

更改	描述	日期
	• Amazon Elastic Disaster Recovery — 解决与相关的问题 Amazon Elastic Disaster Recovery。 • Amazon AppSync — 调试与相关的问题 Amazon AppSync。 • Amazon CloudWatch 日志-用于解决与亚马逊 CloudWatch 日志相关的问题。 • Amazon Health — 调试与 Amazon Health 服务相关的问题。 • Amazon Connect – 调试与 Amazon Connect 相关的问题。 • Amazon Snowball Edge — 解决与相关的问题 Amazon Snowball Edge。 • Amazon Health Imaging – 排查与 Amazon Health Imaging 相关的问题。	

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	为以下服务增加了 163 项新权限，以执行有助于排查与账单、管理和技术支持相关的客户问题的操作： • Amazon CloudFront — 用于解决与 CloudFront 服务相关的问题。 • 亚马逊 EC2 -解决与亚马逊 EC2 服务有关的问题。 • 亚马逊 AppStream -调试与亚马逊相关的问题 AppStream。 • Amazon WAF — 调试与 Amazon Web 应用程序防火墙相关的问题。 • Amazon Connect – 排查与 Amazon Connect 相关的问题。 • Amazon IoT — 调试与相关的问题 Amazon IoT。 • Amazon Route 53 – 排查与 Amazon Route 53 相关的问题。 • Amazon 已验证的访问权限-用于解决与 Amazon 已验证访问服务相关的问题。 • Amazon Simple Email Service – 调试与 Amazon Simple Email Service 相关的问题。	2023 年 10 月 27 日

更改	描述	日期
	• Amazon Elastic Beanstalk — 解决与相关的问题 Amazon Elastic Beanstalk。 • Amazon DynamoDB – 调试与 Amazon DynamoDB 相关的问题。 • Amazon EC2 Image Builder — 用于解决与 Amazon EC2 图像生成器相关的问题。 • Amazon Outposts — 调试与 Amazon Outposts 服务相关的问题。 • Amazon Glue — 调试与相关的问题 Amazon Glue。 • Amazon Directory Service — 解决与相关的问题 Amazon Directory Service。 • Amazon Elastic Disaster Recovery — 解决与相关的问题 Amazon Elastic Disaster Recovery。 • Amazon Step Functions — 调试与相关的问题 Amazon Step Functions。 • Amazon EMR – 排查与 Amazon EMR 相关的问题。 • Amazon Relational Database Service – 排查与 Amazon Relational Database Service 相关的问题。 • Amazon EC2 Systems Manager — 调试与亚马逊	

更改	描述	日期
	EC2 系统管理器相关的问题。	

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	为以下服务增加了 176 项新权限，以执行有助于排查与账单、管理和技术支持相关的客户问题的操作： • Amazon Glue — 解决与 Amazon Glue 服务有关的问题 • Amazon EMR – 排查与 Amazon EMR 服务相关的问题。 • Amazon Security Lake – 调试与 Amazon Security Lake 相关的问题。 • Amazon Systems Manager — 调试与 Systems Manager 服务相关的问题。 • Amazon Verified Permissions – 排查与 Amazon Verified Permissions 相关的问题。 • Amazon IAM 访问分析器 — 调试与 IAM 访问分析器服务相关的问题。 • Amazon Backup — 解决与相关的问题 Amazon Backup。 • Amazon Database Migration Service — 解决与 DMS 服务相关的问题。 • Amazon DynamoDB – 调试与 Dynamo DB 相关的问题。	2023 年 8 月 28 日

更改	描述	日期
	• Amazon Elastic Container Registry（Amazon ECR）– 排查与 Amazon Elastic Container Registry（Amazon ECR）相关的问题。 • Amazon Elastic Container Service – 调试与 Amazon Elastic Container Service 相关的问题。 • Amazon Elastic Kubernetes Service – 排查与 Amazon Elastic Kubernetes Service 相关的问题。 • Amazon EMR Serverless – 调试与 Amazon EMR Serverless Service 相关的问题。 • Amazon Identity and Access Management — 解决与相关的问题 Amazon Identity and Access Management。 • Amazon Network Firewall-用于解决与 Amazon 网络防火墙相关的问题。 • Amazon HealthOmics — 调试与相关的问题 Amazon HealthOmics。 • Amazon Quick Suite – 调试与 Amazon Quick Suite 相关的问题。 • Amazon Relational Database Service – 排	

更改	描述	日期
	查与 Amazon Relational Database Service 相关的问题。 • Amazon Redshift – 排查与 Amazon Redshift 相关的问题。 • Amazon Redshift Serverless – 调试与 Amazon Redshift Serverless 相关的问题。 • 亚马逊 SageMaker AI — 调试与亚马逊 A SageMaker I 相关的问题。	

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	为以下服务增加了 141 项新权限，以执行有助于排查与账单、管理和技术支持相关的客户问题的操作： • Lambda – 排查与 Lambda 服务相关的问题。 • Amazon Lex – 排查与 Amazon Lex 服务相关的问题。 • Amazon 传输-调试与传输服务相关的问题。 • Amazon Amplify — 调试与 Amplify 服务相关的问题。 • Amazon Pip EventBridge es — 用于解决与 Pipes 相关的权限和账单问题。 • 亚马逊 EventBridge -调试与亚马逊相关的问题 EventBridge • Amazon CloudWatch 日志-用于解决与亚马逊 CloudWatch 日志相关的问题。 • Amazon Systems Manager — 对与 Systems Manager 相关的问题进行故障排除。 • Amazon CloudWatch — 调试与之相关的问题 CloudWatch。 • 亚马逊 ElastiCache -解决与亚马逊相关的问题 ElastiCache。	2023 年 6 月 26 日

更改	描述	日期
	• Amazon Athena – 调试与 Athena 相关的问题。 • Amazon 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。 • Amazon EC2 — 调试与 EC2 服务相关的问题。 • Amazon Certificate Manager — 解决与 Certifice Manager 相关的问题。 • Amazon EventBridge 计划程序-用于解决与 EventBridge 计划程序相关的问题。 • Amazon OpenSearch 服务-用于解决与之相关的问题 OpenSearch。 • Amazon EventBridge 架构-调试与 EventBridge 架构相关的问题。 • Amazon 用户通知-用于解决与用户通知相关的问题。 • Amazon App CloudWatch lication Insights — 用于解决与 CloudWatch 应用程序见解相关的问题。 • Amazon DynamoDB – 排查与 DynamoDB 相关的问题。 • Amazon DocumentDB Elastic Clusters – 排查	

更改	描述	日期
	与 DocumentDB Elastic Clusters 相关的问题。	

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	为以下服务增加了 53 项新权限，以执行有助于排查与账单、管理和技术支持相关的客户问题的操作： • Auto Scaling – 排查与 Auto Scaling 服务相关的问题。 • 亚马逊 CloudWatch -解决与亚马逊相关的问题 CloudWatch。 • Amazon Compute Optimizer — 解决与 Compute Optimizer 相关的问题。 • Amazon CloudWatch Evicently — 解决与 Evidently 相关的问题。 • EC2 Image Builder — 用于解决与图像生成器服务相关的问题。 • Amazon IoT TwinMaker — 解决与相关的问题 Amazon IoT TwinMaker。 • Amazon CloudWatch 日志-用于解决与亚马逊 CloudWatch 日志相关的问题。 • Amazon Pinpoint：解决与 Amazon Pinpoint 相关的问题。 • Amazon OAM 链接 — 用于调试与 OAM 资源相关的问题。	2023 年 5 月 2 日

更改	描述	日期
	• Amazon Outposts — 解决与相关的问题 Amazon Outposts。 • Amazon RDS – 调试与 Amazon RDS 相关的问题。 • Amazon 资源探索器 — 解决与资源管理器相关的问题。 • Amazon CloudWatch RUM — 对 RUM 服务资源的配置进行故障排除。 • Amazon SNS – 排查与 Amazon SNS 相关的问题。 • Amazon CloudWatch Synthetics — 解决与 Sy CloudWatch nthetics 相关的问题。	

更改	描述	日期
AWSSupportServiceRolePolicy：对现有策略的更新	为以下服务增加了 52 项新权限，以执行有助于排查与账单、管理和技术支持相关的客户问题的操作： • Amazon Backup gateway — 解决与 Backup 网关相关的问题。 • Amazon S3 – 调试与 Amazon S3 相关的问题。 • Amazon Application Migration Service — 解决与应用程序迁移服务相关的问题。 • Amazon 洁净室-调试与 Amazon 洁净室有关的问题； • Amazon Systems Manager 适用于 SAP — 对与 SAP 相关的问题进行故障排除。Amazon Systems Manager • Amazon VPC Lattice – 调试与 Amazon VPC Lattice 相关的问题。	2023 年 3 月 16 日

更改	描述	日期
AWSSupportServiceRolePolicy：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 — Amazon Web Services 支持 允许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。 • Amazon CloudWatch Internet Monitor — 调试与互联网监控器相关的问题。 • 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。 • Amazon P EventBridge ipes — 解决与 EventBridge 管道有关的问题。 • 亚马逊互动视频服务-允许 Amazon Web Services 支持查询 Amazon IVS 资源以解决客户问题。 • 亚马逊 FSx — 允许开发工具 Amazon Web Services 支持 ，以支持亚马逊 FSx 数据存储库的导入和导出。	2023 年 1 月 10 日

更改	描述	日期
	• 亚马逊 GameLift 服务器-用于解决与亚马逊 GameLift 服务器相关的问题。 • Amazon Glue：解决与 Amazon 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。 • Amazon Network Manager — 解决与网络管理器有关的问题。 • 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。	

更改	描述	日期
	• Amazon HealthOmics — 解决与相关的问题 HealthOmics。 • Amazon Transcribe：调试与 Amazon Transcribe 相关的问题。	

更改	描述	日期
AWSSupportServiceRolePolicy：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： • Amazon Application Migration Service — 解决复制和启动问题。 • Amazon CloudFormation hooks — Amazon Web Services 支持 允许开发可以帮助解决问题的自动化工具。 • Amazon Elastic Kubernetes Service - 解决与 Amazon EKS 相关的问题。 • Amazon IoT FleetWise – 排查与 Amazon IoT FleetWise 相关的问题。 • Amazon Mainframe Modernization — 调试与相关的问题 Amazon Mainframe Modernization。 • Amazon Outposts — 帮助 Amazon Web Services 支持获取专用主机和资产列表。 • Amazon Private 5G – 排查与 Private 5G 相关的问题。 • Amazon Tiros - 调试与 Tiros 相关的问题。	2022 年 10 月 4 日

更改	描述	日期
AWSSupportServiceRolePolicy：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。 • Amazon DataSync — 解决与相关的问题 DataSync。 • Amazon Elastic Disaster Recovery — 解决复制和启动问题。 • Amazon GameSparks — 用于解决与之相关的问题 GameSparks。 • Amazon IoT TwinMaker — 调试与相关的问题 Amazon IoT TwinMaker。 • Amazon Lambda — 查看用于故障排除问题的函数 URL 的配置。 • Amazon Lookout for Equipment - 解决与 Lookout for Equipment 相关的问题。 • 亚马逊 Route 53 和亚马逊 Route 53 解析器 — 获取解析器配置，以便 Amazon Web Services 支持 可以检查 VPC 的 DNS 解析行为。	2022 年 8 月 17 日

更改	描述	日期
AWSSupportServiceRolePolicy：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： • Amazon CloudWatch 日志-帮助解决与 CloudWatch 日志相关的问题。 • 亚马逊互动视频服务 — 帮助 Amazon Web Services 支持 检查现有的亚马逊 IVS 资源，了解有关欺诈或账户被盗的支持案例。 • Amazon Inspector – 对 Amazon Inspector 相关问题进行问题排查。 移除了 Amazon 等服务的权限 WorkLink。亚马逊已 WorkLink 于 2022 年 4 月 19 日被弃用。	2022 年 6 月 23 日

更改	描述	日期
AWSSupportServiceRolePolicy：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： • Amazon Amplify 用户界面生成器-用于解决与组件和主题生成相关的问题。 • Amazon AppStream — 通过检索最近推出的功能的资源来解决问题。 • Amazon Backup — 解决与备份作业有关的问题。 • Amazon CloudFormation — 对与 IAM、扩展和版本控制相关的问题进行诊断。 • Amazon Kinesis – 排查与 Kinesis 相关的问题。 • Amazon Transfer Family — 解决与 Transfer Family 相关的问题。	2022 年 4 月 27 日

更改	描述	日期

AWSSupportServiceRolePolicy：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 Amazon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。
	• Amazon 网络管理器-用于解决与网络管理器相关的问题。
	• 节省计划 – 获取有关未完成的节省计划承诺的元数据。
	• Amazon Serverless Application Repository — 作为研究和解决支持案例的一部分，改进和支持响应行动。
	• Amazon WorkSpaces Web — 调试和解决 WorkSpaces 网络服务问题。
		2022 年 3 月 14 日

更改	描述	日期
AWSSupportServiceRolePolicy：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： • Amazon Application Migration Service — 支持应用程序迁移服务中的无代理复制。 • Amazon CloudFormation — 对 IAM、扩展和版本控制相关问题进行诊断。 • Amazon 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。 • Amazon Elastic Disaster Recovery — 解决客户账户中的复制和启动问题。 • 亚马逊 FSx — 查看亚马逊 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	2022 年 2 月 17 日

更改	描述	日期
	S3) 存储桶的元数据和配置。 • Amazon Storage Gateway — 查看有关客户自动磁带创建策略的元数据。 • 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。	
已发布的更改日志	Amazon Web Services 支持 托管策略的更改日志。	2022 年 2 月 17 日

AWSSupportServiceRolePolicy 的权限更改

添加的大多数权限都是 Amazon Web Services 支持 为了AWSSupportServiceRolePolicy允许调用同名的 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:GetAnalyticsConfiguration
	s3.ListBucketAnalyticsConfiguration	
	s3.GetBucketNotificationConfiguration	s3:GetBucketNotification

日期	API 操作名称	所需的策略权限
	s3.GetBucketEncryption	s3:GetEncryptionConfiguration
	s3.GetBucketIntelligentTieringConfiguration s3.ListBucketIntelligentTieringConfiguration	s3:GetIntelligentTieringConfiguration
	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

日期	API 操作名称	所需的策略权限
	s3.ListObjectVersions	s3:ListBucketVersions
	s3.ListParts	s3:ListMultipartUploadParts
2025 年 7 月 15 日添加了权限	cloudcontrolapi:GetResource	cloudformation:GetResource
	cloudcontrolapi:ListResources	cloudformation:ListResources

Amazon Web Services 的托管策略 Amazon Trusted Advisor

Trusted Advisor 具有以下 Amazon Web Services 托管策略。

目录

Amazon 托管策略：AWSTrustedAdvisorPriorityFullAccess

该AWSTrustedAdvisorPriorityFullAccess政策授予对 “ Trusted Advisor 优先级” 的完全访问权限。此策略还允许用户添加为可信服务， Amazon Organizations 并允许用户 Trusted Advisor 为 P Trusted Advisor riority 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 优先级中已识别的风险。这些权限允许您下载和更新风险状态。

- 描述您的 Trusted Advisor 优先电子邮件通知配置。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。
- 进行设置， Trusted Advisor 以便您的账户可以启用 Amazon 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。
- 列出您允许使用 Organizations 的。 Amazon Web Services 服务

在第三条语句中，此策略包含 organizations 的以下权限：

- 列出 Trusted Advisor 优先级的委派管理员。
- 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 服务关联角色。

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。

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityFullAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:UpdateRiskStatus",
    "trustedadvisor:DescribeNotificationConfigurations",
```

```
    "trustedadvisor:UpdateNotificationConfigurations",
    "trustedadvisor:DeleteNotificationConfigurationForDelegatedAdmin",
    "trustedadvisor:SetOrganizationAccess"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:EnableAWSServiceAccess",
    "organizations:DisableAWSServiceAccess"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  },
  {
   "Sid": "AllowCreateServiceLinkedRole",
   "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"
    }
   }
```

```
  },
  {
   "Sid": "AllowRegisterDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:RegisterDelegatedAdministrator",
    "organizations:DeregisterDelegatedAdministrator"
   ],
   "Resource": "arn:aws:organizations::*:*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
 ]
}
```

Amazon 托管策略：AWSTrustedAdvisorPriorityReadOnlyAccess

该AWSTrustedAdvisorPriorityReadOnlyAccess策略向 P Trusted Advisor riority 授予只读权限，包括查看委派管理员账户的权限。

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。
- 描述从 P Trusted Advisor riority 中识别出的风险并允许您下载它们。
- 描述 Trusted Advisor 优先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。
- 列出您允许使用 Organizations 的。 Amazon Web Services 服务
- 列出 Trusted Advisor 优先级的委派管理员

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [
  {
   "Sid": "AWSTrustedAdvisorPriorityReadOnlyAccess",
   "Effect": "Allow",
   "Action": [
    "trustedadvisor:DescribeAccount*",
    "trustedadvisor:DescribeOrganization",
    "trustedadvisor:DescribeRisk*",
    "trustedadvisor:DownloadRisk",
    "trustedadvisor:DescribeNotificationConfigurations"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowAccessForOrganization",
   "Effect": "Allow",
   "Action": [
    "organizations:DescribeOrganization",
    "organizations:ListAWSServiceAccessForOrganization"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AllowListDelegatedAdministrators",
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "organizations:ServicePrincipal": [
      "reporting.trustedadvisor.amazonaws.com"
     ]
    }
   }
  }
 ]
```

```
}
```

Amazon 托管策略：AWSTrustedAdvisorServiceRolePolicy

此策略附加到 AWSServiceRoleForTrustedAdvisor 服务关联角色。此角色允许服务关联角色为您执行操作。您不能将 AWSTrustedAdvisorServiceRolePolicy 附加到您的 Amazon Identity and Access Management （ IAM ）实体。有关更多信息，请参阅 将服务关联角色用于 Trusted Advisor。

此策略授予管理权限，允许服务关联角色访问 Amazon Web Services 服务。这些权限允许通过检查 Trusted Advisor 来评估您的账户。

权限详细信息

该策略包含以下权限。

- accessanalyzer— 描述 Amazon Identity and Access Management Access Analyzer 资源
- Auto Scaling— 描述 Amazon A EC2 uto Scaling 账户配额和资源
- cloudformation— 描述 Amazon CloudFormation (CloudFormation) 账户配额和堆栈
- cloudfront— 描述亚马逊的 CloudFront 分布
- cloudtrail— 描述 Amazon CloudTrail (CloudTrail) 路径
- dynamodb – 描述 Amazon DynamoDB 账户配额和资源
- dynamodbaccelerator – 描述 DynamoDB Accelerator 资源
- ec2— 描述亚马逊弹性计算云 (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
- networkfirewall— 描述 Amazon Network Firewall 资源
- 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 Amazon CloudWatch 事件（CloudWatch 事件）指标统计数据
- ce – 获取 Cost Explorer 服务 (Cost Explorer) 建议
- route53resolver— 获取 Amazon Route 53 Resolver 解析器端点和资源
- kafka – 获取 Amazon Managed Streaming for Apache Kafka 资源
- ecs – 获取 Amazon ECS 资源
- outposts— 获取 Amazon Outposts 资源

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "TrustedAdvisorServiceRolePermissions",
            "Effect": "Allow",
            "Action": [
                "access-analyzer:ListAnalyzers",
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:GetTrail",
                "cloudtrail:ListTrails",
                "cloudtrail:GetEventSelectors",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "dax:DescribeClusters",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
```

```
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeNatGateways",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeRegions",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
                "ec2:GetManagedPrefixListEntries",
                "ecs:DescribeTaskDefinition",
                "ecs:ListTaskDefinitions",
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeRules",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "iam:ListSAMLProviders",
                "kinesis:DescribeLimits",
                "kafka:DescribeClusterV2",
                "kafka:ListClustersV2",
                "kafka:ListNodes",
                "network-firewall:ListFirewalls",
```

```
                "network-firewall:DescribeFirewall",
                "outposts:GetOutpost",
                "outposts:ListAssets",
                "outposts:ListOutposts",
                "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",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
```

```
                "ses:GetSendQuota",
                "sqs:GetQueueAttributes",
                "sqs:ListQueues"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon 托管策略：AWSTrustedAdvisorReportingServiceRolePolicy

此策略附加到AWSServiceRoleForTrustedAdvisorReporting服务相关角色，该角色 Trusted Advisor 允许对组织视图功能执行操作。您不能将 AWSTrustedAdvisorReportingServiceRolePolicy 附加到您的 IAM 实体。有关更多信息，请参阅 将服务关联角色用于 Trusted Advisor。

此策略授予管理权限，允许服务相关角色执行 Amazon Organizations 操作。

权限详细信息

该策略包含以下权限。

- 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

JSON

```
{
    "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 Amazon 托管式策略的Trusted Advisor 更新

查看有关这些服务开始跟踪这些更改之前 Amazon Web Services 支持 和之 Trusted Advisor 后的 Amazon 托管策略更新的详细信息。要获得有关此页面更改的自动提示，请订阅 文档历史记录 页面上的 RSS 源。

下表描述了自 2021 年 8 月 10 日以来 Trusted Advisor 托管策略的重要更新。

Trusted Advisor

更改	描述	日期
AWSTrustedAdvisorServiceRolePolicy 更新为现有策略。	Trusted Advisor 添加了新的操作来授予`elasticloadbalancing:DescribeListeners`，和`elasticloadbalancing:DescribeRules` 权限。	2024 年 10 月 30 日
AWSTrustedAdvisorServiceRolePolicy 更新为现有策略。	Trusted Advisor 添加了新的操作来授予`access-analyzer:ListAnalyzers cloudwatch:ListMetrics` 、`dax:DescribeCluste`	2024 年 6 月 11 日

更改	描述	日期
	rs 、ec2:Describe NatGateways 、ec2:DescribeRouteTables 、ec2:DescribeVpcEndpoints 、ec2:GetManagedPrefixListEntries 、elasticloadbalancing:DescribeTargetHealth 、iam:ListSAMLProviders 、kafka:DescribeClusterV2 network-firewall:ListFirewalls network-firewall:DescribeFirewall 和sqs:GetQueueAttributes 权限。	
AWSTrustedAdvisorServiceRolePolicy 更新为现有策略。	Trusted Advisor 添加了新的操作来授予cloudtrail:GetTrail cloudtrail:ListTrails cloudtrail:GetEventSelectors outposts:GetOutpost 、outposts:ListAssets 和outposts:ListOutposts 权限。	2024 年 1 月 18 日

更改	描述	日期
AWSTrustedAdvisorPriorityFullAccess 更新为现有策略。	Trusted Advisor 更新了AWSTrustedAdvisorPriorityFullAccess Amazon 托管策略以包含声明 IDs。	2023 年 12 月 6 日
AWSTrustedAdvisorPriorityReadOnlyAccess 更新为现有策略。	Trusted Advisor 更新了AWSTrustedAdvisorPriorityReadOnlyAccess Amazon 托管策略以包含声明 IDs。	2023 年 12 月 6 日
AWSTrustedAdvisorServiceRolePolicy：对现有策略的更新	Trusted Advisor 添加了新的操作来授予ec2:DescribeRegions s3:GetLifecycleConfiguration ecs:DescribeTaskDefinition 和ecs:ListTaskDefinitions 权限。	2023 年 11 月 9 日
AWSTrustedAdvisorServiceRolePolicy：对现有策略的更新	Trusted Advisor 在加入新的弹性检查中添加了新的 IAM 操作route53resolver:ListResolverEndpoints route53resolver:ListResolverEndpointIpAddresses ec2:DescribeSubnets 、、kafka:ListClustersV2 和kafka:ListNodes 。	2023 年 9 月 14 日

更改	描述	日期
AWSTrustedAdvisorReportingServiceRolePolicy 附加到 Trusted Advisor AWSServiceRoleForTrustedAdvisorReporting 服务相关角色的托管策略的 V2	将 Trusted Advisor AWSServiceRoleForTrustedAdvisorReporting 服务相关角色的 Amazon 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 和 AWSTrustedAdvisorPriorityReadOnlyAccess 的新 Amazon 托管策略 Trusted Advisor	Trusted Advisor 添加了两个新的托管策略，您可以使用它们来控制对 Priority 的 Trusted Advisor 访问权限。	2022 年 8 月 17 日
AWSTrustedAdvisorServiceRolePolicy：对现有策略的更新	Trusted Advisor 添加了新的操作来授予DescribeTargetGroups 和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 Amazon Web Services 账户的阻止公有访问设置。	2021 年 8 月 10 日

更改	描述	日期
已发布的更改日志	Trusted Advisor 开始跟踪其 Amazon 托管策略的更改。	2021 年 8 月 10 日

AmazonAmazon Web Services 支持 计划的托管策略

Amazon Web Services 支持 计划具有以下托管策略。

目录

Amazon 托管策略：AWSSupportPlansFullAccess

Amazon Web Services 支持 计划使用AWSSupportPlansFullAccess Amazon 托管策略。IAM 实体使用此策略为您完成以下 Support Plans 操作：

- 查看您的支持计划 Amazon Web Services 账户
- 查看有关更改支持计划请求状态的详细信息
- 更改您的支持计划 Amazon Web Services 账户
- 为您制定支持计划时间表 Amazon Web Services 账户
- 查看您的所有支持计划修改器列表 Amazon Web Services 账户

JSON

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

```
                "supportplans:StartSupportPlanUpdate",
                "supportplans:CreateSupportPlanSchedule",
                "supportplans:ListSupportPlanModifiers"
            ],
            "Resource": "*"
        }
    ]
}
```

有关策略更改的列表，请参阅 Amazon Web Services 支持 计划对 Amazon 托管策略进行更新。

Amazon 托管策略：AWSSupportPlansReadOnlyAccess

Amazon Web Services 支持 计划使用AWSSupportPlansReadOnlyAccess Amazon 托管策略。IAM 实体使用此策略为您完成以下只读 Support Plans 操作：

- 查看您的支持计划 Amazon Web Services 账户
- 查看有关更改支持计划请求状态的详细信息
- 查看您的所有支持计划修改器列表 Amazon Web Services 账户

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "supportplans:GetSupportPlan",
                "supportplans:GetSupportPlanUpdateStatus",
                "supportplans:ListSupportPlanModifiers"
            ],
            "Resource": "*"
        }
    ]
}
```

有关策略更改的列表，请参阅 Amazon Web Services 支持 计划对 Amazon 托管策略进行更新。

Amazon Web Services 支持 计划对 Amazon 托管策略进行更新

查看自这些服务开始跟踪这些更改以来，Support Plans Amazon 托管政策更新的详细信息。要获得有关此页面更改的自动提示，请订阅 文档历史记录 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。

Amazon Web Services 支持

更改	描述	日期
AWSSupportPlansReadOnlyAccess – 对现有策略的更新 AWSSupportPlansFullAccess – 对现有策略的更新	将 `ListSupportPlanModifiers` 操作添加到 `AWSSupportPlansFullAccess` 和 `AWSSupportPlansReadOnlyAccess` 托管策略。	2024 年 9 月 9 日
AWSSupportPlansFullAccess – 对现有策略的更新	将 `CreateSupportPlanSchedule` 操作添加到 `AWSSupportPlansFullAccess` 托管策略。	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

AmazonAmazon 合作伙伴主导的 Support 的托管策略

Amazon 托管策略是由创建和管理的独立策略 Amazon。 Amazon 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， Amazon 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 Amazon 客户使用。我们建议通过定义特定于使用案例的客户管理型策略来进一步减少权限。

您无法更改 Amazon 托管策略中定义的权限。如果 Amazon 更新 Amazon 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 Amazon 最有可能在启动新的 API 或现有服务可以使用新 Amazon Web Services 服务 的 API 操作时更新 Amazon 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

Amazon 托管策略： AWSPartnerLedSupportReadOnlyAccess

您可以将 AWSPartnerLedSupportReadOnlyAccess 附加到您的用户、组和角色。

此政策可用于授予只读访问权限 APIs ，该权限可以读取您 Amazon 账户中服务的服务元数据。您可以使用此政策为合作伙伴主导的 Support P Amazon rogram 中的合作伙伴提供访问以下权限详细信息部分中指定的服务的权限。

> **Important**
>
> 尽管 AWSPartnerLedSupportReadOnlyAccess 这是由提供的托管策略 Amazon，但您有责任查看策略中包含的服务和权限，以验证它们是否符合您的特定支持要求。不要假设此托管策略会自动包含所有现有策略或新策略 Amazon Web Services 服务。您可能需要创建并维护额外的自定义策略，以涵盖此托管策略范围之外的服务。

权限详细信息

该策略包含以下权限。

- acm – 允许主体对与 Amazon Certificate Manager相关的技术支持案例进行故障排除。
- acm-pca – 允许主体对与 Amazon 私有证书颁发机构相关的技术支持案例进行故障排除。
- apigateway – 允许主体对与 Amazon API Gateway 相关的技术支持案例进行故障排除。
- athena – 允许主体对与 Amazon Athena 相关的技术支持案例进行故障排除。
- backup – 允许主体对与 Amazon Backup相关的技术支持案例进行故障排除。
- backup-gateway— 允许委托人对与 B Amazon ackup Gateway 相关的技术支持案例进行故障排除。
- cloudformation – 允许主体对与 Amazon CloudFormation相关的技术支持案例进行故障排除。
- cloudfront— 允许委托人对与 Amazon CloudFront 相关的技术支持案例进行故障排除。
- cloudtrail – 允许主体对与 Amazon CloudTrail相关的技术支持案例进行故障排除。

- cloudwatch— 允许委托人对与 Amazon CloudWatch 相关的技术支持案例进行故障排除。
- codepipeline – 允许主体对与 Amazon CodePipeline相关的技术支持案例进行故障排除。
- cognito-identity – 允许主体对与 Amazon Cognito Identity 相关的技术支持案例进行故障排除。
- cognito-idp – 允许主体对与 Amazon Cognito 用户池相关的技术支持案例进行故障排除。
- cognito-sync – 允许主体对与 Amazon Cognito Sync 相关的技术支持案例进行故障排除。
- connect – 允许主体对与 Amazon Connect 相关的技术支持案例进行故障排除。
- directconnect – 允许主体对与 Amazon Direct Connect相关的技术支持案例进行故障排除。
- dms – 允许主体对与 Amazon Database Migration Service相关的技术支持案例进行故障排除。
- ds – 允许主体对与 Amazon Directory Service相关的技术支持案例进行故障排除。
- ec2 – 允许主体对与 Amazon Elastic Compute Cloud 相关的技术支持案例进行故障排除。这包括 EC2（Windows 和 Linux）、虚拟私有云 (VPC) 和 VPC 中的技术支持类别。
- ecs – 允许主体对与 Amazon Elastic Container Service 相关的技术支持案例进行故障排除。
- eks – 允许主体对与 Amazon Elastic Kubernetes Service 相关的技术支持案例进行故障排除。
- elasticache— 允许委托人对与 Amazon ElastiCache 相关的技术支持案例进行故障排除。
- elasticbeanstalk – 允许主体对与 Amazon Elastic Beanstalk相关的技术支持案例进行故障排除。
- elasticfilesystem – 允许主体对与 Amazon Elastic File System 相关的技术支持案例进行故障排除。
- elasticloadbalancing – 允许主体对与 Elastic Load Balancing 相关的技术支持案例进行故障排除。
- emr-containers – 允许主体对与 Amazon EMR on EKS 相关的技术支持案例进行故障排除。
- emr-serverless – 允许主体对与 Amazon EMR Serverless 相关的技术支持案例进行故障排除。
- es— 允许委托人对与 Amazon OpenSearch 服务相关的技术支持案例进行故障排除。这包括技术支持类别，例如 OpenSearch 服务托管群集。
- events— 允许委托人对与 Amazon EventBridge 相关的技术支持案例进行故障排除。
- fsx— 允许委托人对与 Amazon FSx 相关的技术支持案例进行故障排除。这包括技术支持类别，例如 FSX for Windows File Server。
- glue – 允许主体对与 Amazon Glue相关的技术支持案例进行故障排除。
- guardduty— 允许委托人对与 Amazon GuardDuty 相关的技术支持案例进行故障排除。
- iam – 允许主体对与 Amazon Identity and Access Management相关的技术支持案例进行故障排除。

- kafka – 允许主体对与 Amazon Managed Streaming for Apache Kafka 相关的技术支持案例进行故障排除。
- kafkaconnect – 允许主体对与 Amazon Managed Streaming for Apache Kafka Connect 相关的技术支持案例进行故障排除。
- lambda – 允许主体对与 Amazon Lambda相关的技术支持案例进行故障排除。
- logs— 允许委托人对与 Amazon L CloudWatch ogs 相关的技术支持案例进行故障排除。
- medialive – 允许主体对与 AWS Elemental MediaLive相关的技术支持案例进行故障排除。
- mobiletargeting – 允许主体对与 Amazon Pinpoint 相关的技术支持案例进行故障排除。
- pipes— 允许委托人对与 Amazon Pip EventBridge es 相关的技术支持案例进行故障排除。
- polly – 允许主体对与 Amazon Polly 相关的技术支持案例进行故障排除。
- quicksight – 允许主体对与 Amazon Quick Suite 相关的技术支持案例进行故障排除。
- rds – 允许主体对与 Amazon Relational Database Service 相关的技术支持案例进行故障排除。这包括技术支持类别，例如：关系数据库服务 (Aurora - MySQL-Compat)、关系数据库服务 (Aurora - PostgreSQL-c)、关系数据库服务 (PostgreSQL)、关系数据库服务 (SQL Server)、关系数据库服务 (MySQL) 和关系数据库服务 (Oracle)。
- redshift – 允许主体对与 Amazon Redshift 相关的技术支持案例进行故障排除。
- redshift-data – 允许主体对与 Amazon Redshift Data API 相关的技术支持案例进行故障排除。
- redshift-serverless – 允许主体对与 Amazon Redshift Serverless 相关的技术支持案例进行故障排除。
- route53 – 允许主体对与 Amazon Route 53 相关的技术支持案例进行故障排除。
- route53domains – 允许主体对与 Amazon Route 53 域相关的技术支持案例进行故障排除。
- route53-recovery-cluster – 允许主体对与 Amazon Route 53 恢复集群相关的技术支持案例进行故障排除。
- route53-recovery-control-config – 允许主体对与 Amazon Route 53 恢复控件相关的技术支持案例进行故障排除。
- route53-recovery-readiness – 允许主体对与 Amazon Route 53 恢复就绪相关的技术支持案例进行故障排除。
- route53resolver – 允许主体对与 Amazon Route 53 Resolver 相关的技术支持案例进行故障排除。
- s3 – 允许主体对与 Amazon Simple Storage Service 相关的技术支持案例进行故障排除。
- s3express – 允许主体对与 Amazon S3 Express 相关的技术支持案例进行故障排除。
- sagemaker— 允许委托人对与 Amazon A SageMaker I 相关的技术支持案例进行故障排除。

- scheduler— 允许委托人对与 Amazon S EventBridge cheduler 相关的技术支持案例进行故障排除。
- servicequotas – 允许主体对与服务配额相关的技术支持案例进行故障排除。
- ses – 允许主体对与 Amazon Simple Email Service 相关的技术支持案例进行故障排除。
- sns – 允许主体对与 Amazon Simple Notification Service 相关的技术支持案例进行故障排除。
- ssm – 允许主体对与 Amazon Systems Manager相关的技术支持案例进行故障排除。
- ssm-contacts— 允许委托人对与 Amazon Systems Manager Incident Manager 联系人相关的技术支持案例进行故障排除。
- ssm-incidents – 允许主体对与 Amazon Systems Manager Incident Manager相关的技术支持案例进行故障排除。
- ssm-sap— 允许委托人对与 SAP 相关的技术支持案例进行故障排除 Amazon Systems Manager 。
- swf – 允许主体对与 Amazon Simple Workflow Service 相关的技术支持案例进行故障排除。
- vpc-lattice – 允许主体对与 Amazon VPC Lattice 相关的技术支持案例进行故障排除。这包括技术支持类别，例如 VPC - 中转网关。
- waf – 允许主体对与 Amazon WAF相关的技术支持案例进行故障排除。
- waf-regional— 允许委托人对与 Amazon WAF 区域相关的技术支持案例进行故障排除。
- wafv2— 允许委托人对与 Amazon WAF V2 相关的技术支持案例进行故障排除。
- workspaces— 允许委托人对与 Amazon WorkSpaces 相关的技术支持案例进行故障排除。这包括技术支持类别，例如 Workspaces (Windows)。
- workspaces-web— 允许委托人对与 Amazon WorkSpaces 安全浏览器相关的技术支持案例进行故障排除。这包括技术支持类别，例如 Workspaces (Windows)。

要查看此策略的权限，请参阅《Amazon 托管式策略参考》中的 AWSPartnerLedSupportReadOnlyAccess。

Amazon Partner-Led Support 更新了托管 Amazon 政策

查看自 Amazon Partner-Led Support Amazon 托管政策开始跟踪变更以来该服务更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 P Amazon artner-Led Support 文档历史记录页面上的 RSS feed。

更改	描述	日期
AWSPartnerLedSupportReadOnlyAccess - 新策略	添加了一个新的 Amazon 托管策略，其中包含可以读取您 Amazon 账户中服务的服务元数据的权限。	2024 年 11 月 22 日
Amazon 合作伙伴主导的 Support 开始跟踪变更	Amazon Partner-Led Support 开始跟踪其 Amazon 托管政策的变更。	2024 年 11 月 22 日

管理对 Cent Amazon Web Services 支持 er 的访问权限

您必须具有访问支持中心和创建支持案例的权限。

您可以使用以下选项之一访问支持中心：

- 使用 Amazon Identity and Access Management (IAM)。
- 使用与您的 Amazon 帐户关联的电子邮件地址和密码。此身份称为 Amazon 账户 root 用户（不推荐）。

如果您有 B Amazon usiness Support+、En Amazon terprise Suppor Amazon t 或 Unified Operations 计划，也可以使用 Amazon Web Services 支持 API 以编程方式进行访问 Amazon Web Services 支持和 Trusted Advisor 操作。有关更多信息，请参阅 Amazon Web Services 支持 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。

Amazon 账户（不推荐）

您可以使用您的 Amazon 账户电子邮件地址 Amazon Web Services 管理控制台 和密码登录并访问 Support Center。此身份称为 Amazon 账户 r oot 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。

Amazon 支持行动

您可以在控制台中执行以下 Amazon Web Services 支持 操作。您也可以在 IAM 策略中指定这些 Amazon Web Services 支持 操作以允许或拒绝特定操作。

> **Note**
>
> 若在 IAM 策略中拒绝以下任何操作，则在创建支持案例或与支持案例交互时，可能会导致 Support Center 出现意外行为。

Action	说明
`AddAttachmentsToSet`	授予向附件集添加一个或多个附件的权限。附件集是用于存放您添加到案例或案例通信的附件的临时容器。该附件集在创建后 1 小时内可供使用。响应中返回的 expiryTime 即为该附件集的到期时间。
`AddCommunicationToCase`	授予在 Amazon Web Services 支持 案例中添加其他客户通信的权限，包括一组要在通信中复制的电子邮件地址。
`CreateCase`	授予创建案例的权限。
`DescribeAttachment`	授予检索案例附件的权限。
`DescribeCaseAttributes`	授予允许辅助服务读取 Amazon Web Services 支持 案例属性的权限。*Cent Amazon Web Services 支持 er 内部使用它来获取在你的问题上标记的属性。
`DescribeCases`	授予返回与案例 ID 或 Amazon Web Services 支持 案例匹配的案例列表的权限 IDs。

Action	说明
DescribeCommunication	授予获取单个 Amazon Amazon Web Services 支持 案例的单一通信和附件的权限。
DescribeCommunications	允许返回一个或多个 Amazon Web Services 支持 案例的通信和附件。
DescribeCreateCaseOptions	授予返回 CreateCaseOption 类型列表以及相应的支持时间和语言可用性的权限。
DescribeIssueTypes	授予返回 Amazon Web Services 支持 案例问题类型的权限。Cent Amazon Web Services 支持 er 内部使用它来获取您账户的可用问题类型。
DescribeServices	授予返回当前服务列表和每项 Amazon 服务的服务类别列表的权限。然后，您可以使用服务名称和类别来创建案例。每项 Amazon 服务都有自己的一组类别。
DescribeSeverityLevels	授予返回您可以分配给 Amazon Web Services 支持 案例的严重性级别列表的权限。
DescribeSupportedLanguages	授予返回指定 categoryCode、issueType 和 serviceCode 的支持语言列表的权限。
DescribeSupportLevel	授予返回 Amazon 账户标识符支持级别的权限。Cent Amazon Web Services 支持 er 内部使用它来确定您的支持级别。
DescribeTrustedAdvisorCheck RefreshStatuses	授予返回具有指定 Amazon Trusted Advisor 支票的支票刷新状态的权限 IDs。
DescribeTrustedAdvisorCheck Result	授予返回具有指定支票 ID 的 Amazon Trusted Advisor 检查结果的权限。
DescribeTrustedAdvisorChecks	授予返回有关所有可用 Amazon Trusted Advisor 支票的信息的权限，包括姓名、ID、类别、描述和元数据。

Action	说明
DescribeTrustedAdvisorCheckSummaries	授予返回您指定 Amazon Trusted Advisor 支票的检查摘要结果的权限。 IDs
GetInteraction	授予通过唯一标识符检索特定交互的详细信息的权限。Cent Amazon Web Services 支持 er 内部使用它来检索个性化推荐。
InitiateCallForCase	授予在 Cent Amazon Web Services 支持 er 上发起呼叫的权限。Cent Amazon Web Services 支持 er 内部使用它来代表您发起呼叫。
ListInteractionEntries	授予在特定互动中检索条目列表的权限，包括消息、状态更新或其他相关数据点。Cent Amazon Web Services 支持 er 内部使用它来跟踪交互的详细轨迹。
ListInteractions	授予检索互动列表的权限，可能使用过滤器或分页。Cent Amazon Web Services 支持 er 内部使用它来管理和概述多个交互。
InitiateChatForCase	授予在 Amazon Web Services 支持 Center 上发起聊天的权限。Cent Amazon Web Services 支持 er 内部使用它来代表你开始聊天。
PutCaseAttributes	授予允许次要服务将属性附加到 Amazon Web Services 支持 案例的权限。Cent Amazon Web Services 支持 er 内部使用它来为您的 Amazon Web Services 支持 案例添加操作标签。
RateCaseCommunication	授予对 Amazon Web Services 支持 案例沟通进行评分的权限。
RefreshTrustedAdvisorCheck	授予刷新您使用 Amazon Trusted Advisor 支票 ID 指定的支票的权限。
ResolveCase	授予解决 Amazon Web Services 支持 案例的权限。

Action	说明
`ResolveInteraction`	授予使用交互的唯一标识符将交互标记为已解决的权限，表示问题已完全解决，无需采取进一步行动。解决后，互动的状态将设置为 “已关闭”，同一账户中的所有用户都可以访问该交互状态。
`SearchForCases`	授予返回与给定输入相匹配的 Amazon Web Services 支持 案例列表的权限。Cent Amazon Web Services 支持 er 内部使用它来查找搜索到的案例。
`StartInteraction`	授予发起新互动以获取针对账户及技术问题的个性化故障排除帮助的权限。Cent Amazon Web Services 支持 er 内部使用它来启动故障排除流程。
`UpdateInteraction`	授予用另一条消息更新通过唯一标识符指定的特定互动的权限。Cent Amazon Web Services 支持 er 内部使用它来更新故障排除流程。

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，您可以将 IAM 策略附加到这些实体，以便他们有权执行操作和访问资源，例如提交 Support Center 案例和使用 Amazon Web Services 支持 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，他们可以登录您的账户 Amazon Web Services 账户 并在 Support Center 中工作。有权 Amazon Web Services 支持访问的 IAM 用户可以查看为该账户创建的所有案例。

有关更多信息，请参阅 IAM 用户指南中的以 IAM 用户身份登录。 Amazon Web Services 管理控制台

授予权限的最简单方法是将 Amazon 托管策略 A AWSSupportcces s 附加到用户、组或角色。 Amazon Web Services 支持 允许操作级权限来控制对特定 Amazon Web Services 支持 操作的访问权限。 Amazon Web Services 支持 不提供资源级访问权限，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: 允许访问所有 Amazon Web Services 支持 操作

Amazon 托管策略 A AWSSupportcces s 授予 IAM 用户访问权限 Amazon Web Services 支持。拥有此策略的 IAM 用户可以访问所有 Amazon Web Services 支持 操作和资源。

JSON

```
{
    "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。以下政策声明允许 IAM 用户执行 Amazon Web Services 支持 除解决案例之外的所有操作。

JSON

```
{
   "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，则可以在该策略中添加 Amazon Web Services 支持特定于该策略的策略声明。

> **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 的身份和访问管理 Amazon Web Services 支持。

访问权限 Amazon Trusted Advisor

在中 Amazon Web Services 管理控制台，单独的 `trustedadvisor` IAM 命名空间控制对的访问权限 Trusted Advisor。在 Amazon Web Services 支持 API 中，`support`IAM 命名空间控制对的访问权限 Trusted Advisor。有关更多信息，请参阅 管理对的访问权限 Amazon Trusted Advisor。

管理对 Amazon Web Services 支持 套餐的访问权限

主题

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 Amazon Web Services 账户中 Support Plans 资源的详细信息。

您可以使用`supportplans`命名空间创建 Amazon Identity and Access Management (IAM) 策略。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 Amazon 托管策略并将其附加到您的 IAM 实体。有关更多信息，请参阅 AmazonAmazon Web Services 支持 计划的托管策略。

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。

Action	说明
`GetSupportPlan`	授予查看有关此 Amazon Web Services 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 Amazon Web Services 账户支持计划的权限。
`CreateSupportPlanSchedule`	授予权限以为此 Amazon Web Services 账户创建支持计划时间表。
`ListSupportPlanModifiers`	授予权限以查看此 Amazon Web Services 账户的所有支持计划修饰符列表。

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。

JSON

```
{
    "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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "supportplans:Get*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "supportplans:List*",
            "Resource": "*"
        }
    ]
}
```

拒绝对 Support Plans 的访问

以下策略不允许用户访问 Support Plans。

JSON

```
{
    "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 Amazon 托管策略。有关更多信息，请参阅 AmazonAmazon Web Services 支持 计划的托管策略。

如果您无权更新 IAM policy，请联系 Amazon Web Services 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

如果您的账户 Amazon Web Services 账户 是其中的一员 Amazon Organizations，则可能需要更新服务控制政策 (SCP)。 SCPs 是一种在组织中管理权限的策略。

由于 Support 计划是一项全球服务，因此限制 Amazon Web Services 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。这意味着组织中的账户可以访问这些服务，即使 SCP 拒绝了指定的 Amazon Web Services 区域服务。

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 Amazon Web Services 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。

> 的注意事项 Amazon Control Tower
>
> - 如果您的组织将 SCP 与一起使用 Amazon Control Tower，则可以 Amazon 根据请求的 Amazon Web Services 区域控件（通常称为区域拒绝控制）将拒绝访问更新为。
> - 如果您将 SCP 更新 Amazon Control Tower 为允许`supportplans`，则修复偏差将移除您对 SCP 的更新。有关更多信息，请参阅中的检测和解决偏差 Amazon Control Tower。

相关信息

有关更多信息，请参阅以下主题：

- 《Amazon Organizations 用户指南》中的@@ 服务控制策略 (SCPs)。
- 《Amazon Control Tower 用户指南》中的配置区域拒绝控制
- Amazon 根据Amazon Control Tower 用户指南 Amazon Web Services 区域中的要求拒绝访问

管理对的访问权限 Amazon Trusted Advisor

您可以 Amazon Trusted Advisor 从中访问 Amazon Web Services 管理控制台。所有 Amazon Web Services 账户 人都可以访问精选的核心Trusted Advisor 支票。如果您有 B Amazon usiness Support

+、En Amazon terprise Support 或 Amazon Unified Operations 计划，则可以访问所有支票。有关更多信息，请参阅。Amazon Trusted Advisor 查看参考资料

您可以使用 Amazon Identity and Access Management (IAM) 来控制对的访问权限 Trusted Advisor。

主题

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权限。这些权限必须允许用户列出和查看有关您的 Trusted Advisor 资源的详细信息 Amazon Web Services 账户。

可以使用以下选项来控制对 Trusted Advisor的访问：

- 使用 Trusted Advisor 控制台的标签筛选功能。用户或角色必须具有与标签关联的权限。

  您可以使用 Amazon 托管策略或自定义策略按标签分配权限。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。的命名空间 Trusted Advisor 是`trustedadvisor`。但是，您不能使用`trustedadvisor`命名空间来允许或拒绝 Trusted Advisor API 中的 Amazon Web Services 支持 API 操作。相反，您必须使用 Amazon Web Services 支持 的 `support` 命名空间。

> **Note**
>
> 如果您拥有Amazon Web Services 支持该 API 的权限，则中的 Trusted Advisor 微件会 Amazon Web Services 管理控制台 显示 Trusted Advisor 结果的摘要视图。要在 Trusted Advisor 控制台中查看结果，您必须拥有`trustedadvisor`命名空间的权限。

Trusted Advisor 行动

您可以在控制台中执行以下 Trusted Advisor 操作。您也可以在 IAM 策略中指定这些 Trusted Advisor 操作以允许或拒绝特定操作。

Action	说明
DescribeAccount	授予查看 Amazon Web Services 支持 计划和各种 Trusted Advisor 首选项的权限。
DescribeAccountAccess	授予查看是 Amazon Web Services 账户 启用还是禁用的权限 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 Trusted Advisor 查看支票摘要的权限。
DescribeChecks	授予查看 Trusted Advisor 支票详细信息的权限。
DescribeNotificationPreferences	授予权限以查看 Amazon 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。
RefreshCheck	授予刷新 Trusted Advisor 支票的权限。
SetAccountAccess	授予账户启用或禁 Trusted Advisor 用的权限。
UpdateNotificationPreferences	授予权限以更新 Trusted Advisor的通知首选项。
DescribeCheckStatusHistoryChanges	授予查看过去 30 天内检查的结果和更改状态的权限。

Trusted Advisor 用于组织视图的操作

以下 Trusted Advisor 操作适用于组织视图功能。有关更多信息，请参阅 的组织视图 Amazon Trusted Advisor。

Action	说明
DescribeOrganization	授予查看是否 Amazon Web Services 账户 满足启用组织视图功能的要求的权限。
DescribeOrganizationAccounts	授予查看组织中关联 Amazon 账户的权限。
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	授予查看组织视图报告相关信息的权限，例如支票类别、支票名称和资源状态。 Amazon Web Services 区域
GenerateReport	授予在组织中创建 Trusted Advisor 支票报告的权限。
ListAccountsForParent	授予在 Trusted Advisor 控制台中查看组织中由根或 Amazon 组织单位 (OU) 包含的所有账户的权限。
ListOrganizationalUnitsForParent	授予在 Trusted Advisor 控制台中查看上级组织单位或根目录中所有组织单位 (OUs) 的权限。
ListRoots	授予在 Trusted Advisor 控制台中查看 Amazon 组织中定义的所有根目录的权限。
SetOrganizationAccess	授予为启用组织视图功能的权限 Trusted Advisor。

Trusted Advisor 优先行动

如果您为账户启用了 Trusted Advisor 优先级，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 Priority 的 IAM policy 示例。

> **Note**
>
> Trusted Advisor 优先级中显示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推荐，例如 Trusted Advisor 支票。来自 TAM 的建议是手动为您创建的。接下来，您的 TAM 会发送这些推荐，使其显示在您账户的 “ Trusted Advisor 优先级” 中。

有关更多信息，请参阅 开始使用 P Amazon Trusted Advisor riority。

Action	说明
`DescribeRisks`	授予按 Trusted Advisor 优先级查看风险的权限。
`DescribeRisk`	授予按 Trusted Advisor 优先级查看风险详细信息的权限。
`DescribeRiskResources`	授予权限以查看 Trusted Advisor Priority 中受影响的风险资源。
`DownloadRisk`	授予下载包含 Trusted Advisor 优先级风险详细信息的文件的权限。
`UpdateRiskStatus`	授予权限以更新 Trusted Advisor Priority 中的风险状态。
`DescribeNotificationConfigurations`	授予获取 Trusted Advisor 优先级电子邮件通知首选项的权限。
`UpdateNotificationConfigurations`	授予权限以创建或更新 Trusted Advisor Priority 的电子邮件通知首选项。

Action	说明
DeleteNotificationConfigurationForDelegatedAdmin	向组织管理账户授予权限，允许其从 Priority 的委托管理员账户中删除电子邮件通知首选项。Trusted Advisor

IAM 策略示例

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

- 完全访问权限 Trusted Advisor
- 对 Trusted Advisor的只读访问权限
- 拒绝访问 Trusted Advisor
- 允许和拒绝特定操作
- 控制对 Amazon Web Services 支持 API 操作的访问权限 Trusted Advisor
- Trusted Advisor Priority 的 IAM policy 示例

完全访问权限 Trusted Advisor

以下策略允许用户在 Trusted Advisor 控制台中查看所有 Trusted Advisor 检查并对其执行所有操作。

JSON

```
{
    "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。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "trustedadvisor:Describe*",
                "trustedadvisor:Get*",
                "trustedadvisor:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

拒绝访问 Trusted Advisor

以下政策不允许用户在 Trusted Advisor 控制台中查看 Trusted Advisor 支票或对其执行操作。

JSON

```
{
    "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 支票，但不允许他们刷新任何支票。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:RefreshCheck",
            "Resource": "*"
        }
    ]
}
```

控制对 Amazon Web Services 支持 API 操作的访问权限 Trusted Advisor

在中 Amazon Web Services 管理控制台，单独的 `trustedadvisor` IAM 命名空间控制对的访问权限 Trusted Advisor。您不能使用`trustedadvisor`命名空间来允许或拒绝 Trusted Advisor API 中的 Amazon Web Services 支持 API 操作。相反，可以使用 `support` 命名空间。您必须拥有 Amazon Web Services 支持 API 权限才能以 Trusted Advisor 编程方式调用。

例如，如果要调用该RefreshTrustedAdvisorCheck操作，则必须在策略中拥有执行此操作的权限。

Example: 仅允许 Trusted Advisor API 操作

以下策略允许用户访问其他 Amazon Web Services 支持 API 操作的 API 操作 Trusted Advisor，但不允许访问其他 Amazon Web Services 支持 API 操作。例如，用户可以使用 API 查看和刷新检查。他们无法创建、查看、更新或解决 Amazon Web Services 支持 案例。

您可以使用此策略以编程方式调用 Trusted Advisor API 操作，但不能使用此策略在 Trusted Advisor 控制台中查看或刷新检查。

JSON

```
{
    "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 如何与 Amazon Web Services 支持 和配合使用的更多信息 Trusted Advisor，请参阅操作。

Trusted Advisor Priority 的 IAM policy 示例

您可以使用以下 Amazon 托管策略来控制对 Priority 的 Trusted Advisor 访问权限。有关更多信息，请参阅Amazon Web Services 的托管策略 Amazon Trusted Advisor和开始使用 P Amazon Trusted Advisor riority。

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 Amazon Trusted Advisor定义的操作。
- 控制对 Trusted Advisor 控制台的访问

Amazon Trusted Advisor的示例服务控制策略

Amazon Trusted Advisor 支持服务控制策略 (SCPs)。 SCPs 是您附加到组织中元素的策略，用于管理该组织内的权限。SCP 适用于您附加 SCP 的元素下的所有 Amazon Web Services 账户。 SCPs 提供对组织中所有账户的最大可用权限的集中控制。它们可以帮助您确保您的 Amazon Web Services 帐户符合组织的访问控制准则。有关更多信息，请参阅《Amazon Organizations 用户指南》中的服务控制策略。

主题

- 先决条件
- 示例服务控制策略

先决条件

要使用 SCPs，必须先执行以下操作：

- 启用组织中的所有功能。有关更多信息，请参阅《Amazon Organizations 用户指南》中的启用企业中的所有功能。
- 启用 SCPs 以便在您的组织内使用。有关更多信息，请参阅《Amazon Organizations 用户指南》中的启用和禁用策略类型。
- 创建你 SCPs 需要的。有关创建的更多信息 SCPs，请参阅《Amazon Organizations 用户指南》中的创建、更新和删除服务控制策略。

示例服务控制策略

以下示例展示如何能控制组织中资源共享的各个方面。

Example: 阻止用户在 Engage 中 Trusted Advisor 创建或编辑互动

以下 SCP 阻止用户创建新参与或编辑现有参与。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:CreateEngagement",
        "trustedadvisor:UpdateEngagement*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Example: 拒绝 Trusted Advisor 参与和 Trusted Advisor 优先访问

以下 SCP 禁止用户在 Eng Trusted Advisor age 和 Trusted Advisor Priority 中访问或执行任何操作。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "trustedadvisor:ListEngagement*",
        "trustedadvisor:GetEngagement*",
```

```
        "trustedadvisor:CreateEngagement*",
        "trustedadvisor:UpdateEngagement*",
        "trustedadvisor:DescribeRisk*",
        "trustedadvisor:UpdateRisk*",
        "trustedadvisor:DownloadRisk"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

对 Amazon Web Services 支持 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 Amazon Web Services 支持 和 IAM 时可能遇到的常见问题。

主题

- 我无权执行 iam：PassRole
- 我想要查看我的访问密钥
- 我是一名管理员，想允许其他人访问 Amazon Web Services 支持
- 我想允许 Amazon 账户之外的人访问我的 Amazon Web Services 支持 资源

我无权执行 iam：PassRole

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给。 Amazon Web Services 支持

有些 Amazon Web Services 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Amazon Web Services 支持中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

如果您需要帮助，请联系您的 Amazon 管理员。您的管理员是提供登录凭证的人。

我想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。通过这样做，您可以授予他人永久访问您的权限 Amazon Web Services 账户。

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。

我是一名管理员，想允许其他人访问 Amazon Web Services 支持

要允许其他人访问 Amazon Web Services 支持，您必须向需要访问的人员或应用程序授予权限。如果使用 Amazon IAM Identity Center 管理人员和应用程序，则可以向用户或组分配权限集来定义其访问权限级别。权限集会自动创建 IAM 策略并将其分配给与人员或应用程序关联的 IAM 角色。有关更多信息，请参阅《Amazon IAM Identity Center 用户指南》中的权限集。

如果未使用 IAM Identity Center，则必须为需要访问的人员或应用程序创建 IAM 实体（用户或角色）。然后，您必须将策略附加到实体，以便在 Amazon Web Services 支持中向其授予正确的权限。授予权限后，向用户或应用程序开发人员提供凭证。他们将使用这些凭证访问 Amazon。要了解有关创建 IAM 用户、组、策略和权限的更多信息，请参阅《IAM 用户指南》中的 IAM 身份和 IAM 中的策略和权限。

我想允许 Amazon 账户之外的人访问我的 Amazon Web Services 支持 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解是否 Amazon Web Services 支持 支持这些功能，请参阅如何 Amazon Web Services 支持 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 Amazon Web Services 账户 ，请参阅 IAM 用户指南中的向您拥有 Amazon Web Services 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 Amazon Web Services 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 Amazon Web Services 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

事件响应

的事件响应 Amazon Web Services 支持 是一种 Amazon 责任。 Amazon 有正式的、记录在案的政策和计划来管理事件响应。有关更多信息，请参阅 Amazon 安全事件响应 技术指南。

使用以下选项可自行获知操作性问题：

- 在 S Amazon ervice Health Das hboard 上查看具有广泛影响的 Amazon 运营问题。例如，影响非账户特定的服务或区域的事件。
- 在 Amazon 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《Amazon Health 用户指南》中的 Amazon Health Dashboard入门。

登录 Amazon Web Services 支持 和监控 Amazon Trusted Advisor

监控是维护和和其他 Amazon 解决方案的可靠性、可用性和性能的重要组成部分。 Amazon Web Services 支持 Amazon Trusted Advisor Amazon 提供了以下监控工具，供 Amazon Web Services 支持 您监视 Amazon Trusted Advisor、报告问题并在适当时采取措施：

- Amazon 会实时 CloudWatch监控您的 Amazon 资源和您运行 Amazon 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 Amazon CloudWatch 用户指南。
- Amazon EventBridge 提供了描述 Amazon 资源变化的近乎实时的系统事件流。 EventBridge 启用事件驱动的自动计算，因为您可以编写规则来监视某些事件，并在这些事件发生时在其他 Amazon 服务中触发自动操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。
- Amazon CloudTrail捕获由您的账户或代表您的 Amazon 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的亚马逊简单存储服务 (Amazon S3) Service 存储桶。您可以识别哪些用户和帐户拨打了电话 Amazon、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 Amazon CloudTrail 《用户指南》。

有关更多信息，请参阅Amazon Web Services 支持 的监控和日志记录和Amazon Trusted Advisor 的监控和日志记录。

合规性验证 Amazon Web Services 支持

要了解是否属于特定合规计划的范围，请参阅Amazon Web Services 服务 “” Amazon Web Services 服务 中的 “按合规计划划分的范围”，然后选择您感兴趣的合规计划。 Amazon Web Services 服务 有关一般信息，请参阅合规计划。

您可以使用下载第三方审计报告 Amazon Artifact。有关更多信息，请参阅中的 “下载报告” Amazon Artifact。

您在使用 Amazon Web Services 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。有关您在使用时的合规责任的更多信息 Amazon Web Services 服务，请参阅Amazon 安全文档。

韧性在 Amazon Web Services 支持

Amazon 全球基础设施是围绕 Amazon 区域和可用区构建的。 Amazon 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 Amazon 区域和可用区的更多信息，请参阅Amazon 全球基础设施。

中的基础设施安全 Amazon Web Services 支持

作为一项托管服务， Amazon Web Services 支持 受到《Amazon Web Services：安全流程概述》白皮书中描述的 Amazon 全球网络安全程序的保护。

您可以使用 Amazon 已发布的 API 调用 Amazon Web Services 支持 通过网络进行访问。客户端必须支持传输层安全性协议（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 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 Amazon Security Token Service（Amazon STS）生成临时安全凭证来对请求进行签名。

中的配置和漏洞分析 Amazon Web Services 支持

对于 Amazon Trusted Advisor， Amazon 处理基本的安全任务，例如客户机操作系统 (OS) 和数据库修补、防火墙配置和灾难恢复。

配置和 IT 控制由您（我们的客户）共同 Amazon 负责。有关更多信息，请参阅责任 Amazon 共担模型。

使用的代码示 Amazon Web Services 支持 例 Amazon SDKs

以下代码示例说明如何 Amazon Web Services 支持 使用 Amazon 软件开发套件 (SDK)。

基本功能是向您展示如何在服务中执行基本操作的代码示例。

操作是大型程序的代码摘录，必须在上下文中运行。您可以通过操作了解如何调用单个服务函数，还可以通过函数相关场景的上下文查看操作。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

代码示例

- 使用的基本示 Amazon Web Services 支持 例 Amazon SDKs
  - 你好 Amazon Web Services 支持
  - 学习 Amazon Web Services 支持 使用 Amazon SDK 的基础知识
  - Amazon Web Services 支持 使用的操作 Amazon SDKs
    - AddAttachmentsToSet与 Amazon SDK 或 CLI 配合使用
    - AddCommunicationToCase与 Amazon SDK 或 CLI 配合使用
    - CreateCase与 Amazon SDK 或 CLI 配合使用
    - DescribeAttachment与 Amazon SDK 或 CLI 配合使用
    - DescribeCases与 Amazon SDK 或 CLI 配合使用
    - DescribeCommunications与 Amazon SDK 或 CLI 配合使用
    - DescribeServices与 Amazon SDK 或 CLI 配合使用
    - DescribeSeverityLevels与 Amazon SDK 或 CLI 配合使用
    - 将 DescribeTrustedAdvisorCheckRefreshStatuses 与 CLI 配合使用
    - 将 DescribeTrustedAdvisorCheckResult 与 CLI 配合使用
    - 将 DescribeTrustedAdvisorCheckSummaries 与 CLI 配合使用
    - 将 DescribeTrustedAdvisorChecks 与 CLI 配合使用
    - 将 RefreshTrustedAdvisorCheck 与 CLI 配合使用
    - ResolveCase与 Amazon SDK 或 CLI 配合使用

使用的基本示 Amazon Web Services 支持 例 Amazon SDKs

以下代码示例说明如何使用 with 的基础 Amazon Web Services 支持 知识 Amazon SDKs。

示例

- 你好 Amazon Web Services 支持
- 学习 Amazon Web Services 支持 使用 Amazon SDK 的基础知识
- Amazon Web Services 支持 使用的操作 Amazon SDKs
  - AddAttachmentsToSet与 Amazon SDK 或 CLI 配合使用
  - AddCommunicationToCase与 Amazon SDK 或 CLI 配合使用
  - CreateCase与 Amazon SDK 或 CLI 配合使用
  - DescribeAttachment与 Amazon SDK 或 CLI 配合使用
  - DescribeCases与 Amazon SDK 或 CLI 配合使用
  - DescribeCommunications与 Amazon SDK 或 CLI 配合使用
  - DescribeServices与 Amazon SDK 或 CLI 配合使用
  - DescribeSeverityLevels与 Amazon SDK 或 CLI 配合使用
  - 将 DescribeTrustedAdvisorCheckRefreshStatuses 与 CLI 配合使用
  - 将 DescribeTrustedAdvisorCheckResult 与 CLI 配合使用
  - 将 DescribeTrustedAdvisorCheckSummaries 与 CLI 配合使用
  - 将 DescribeTrustedAdvisorChecks 与 CLI 配合使用
  - 将 RefreshTrustedAdvisorCheck 与 CLI 配合使用
  - ResolveCase与 Amazon SDK 或 CLI 配合使用

你好 Amazon Web Services 支持

以下代码示例展示了如何开始使用 Amazon Web Services 支持。

.NET

适用于 .NET 的 Amazon SDK

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

```
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 适用于 .NET 的 Amazon SDK API 参考DescribeServices中的。

Java

适用于 Java 的 SDK 2.x

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

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SupportException;
import java.util.ArrayList;
import java.util.List;

/**
 * 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 Amazon SDK for Java 2.x API 参考DescribeServices中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

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.",
      );
    }
    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 适用于 JavaScript 的 Amazon SDK API 参考DescribeServices中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
/**
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.fromEnvironment { 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 的详细信息，请参阅适用DescribeServices于 K otlin 的Amazon SDK API 参考。

Python

适用于 Python 的 SDK（Boto3）

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

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

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

学习 Amazon Web Services 支持 使用 Amazon SDK 的基础知识

以下代码示例演示了如何：

- 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

适用于 .NET 的 Amazon SDK

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

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));
    }
}
```

场景中用于 Amazon Web Services 支持 操作的封装方法。

```
/// <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 Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) 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 Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) 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 Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) 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 Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) 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《适用于 .NET 的 Amazon SDK API Reference》中的以下主题。

- AddAttachmentsToSet
- AddCommunicationToCase
- CreateCase
- DescribeAttachment
- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityLevels
- ResolveCase

Java

适用于 Java 的 SDK 2.x

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

运行各种 Amazon Web Services 支持 操作。

```
import software.amazon.awssdk.core.SdkBytes;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.support.SupportClient;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetResponse;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseRequest;
import
 software.amazon.awssdk.services.support.model.AddCommunicationToCaseResponse;
import software.amazon.awssdk.services.support.model.Attachment;
import software.amazon.awssdk.services.support.model.AttachmentDetails;
import software.amazon.awssdk.services.support.model.CaseDetails;
import software.amazon.awssdk.services.support.model.Category;
import software.amazon.awssdk.services.support.model.Communication;
import software.amazon.awssdk.services.support.model.CreateCaseRequest;
import software.amazon.awssdk.services.support.model.CreateCaseResponse;
import software.amazon.awssdk.services.support.model.DescribeAttachmentRequest;
```

```
import software.amazon.awssdk.services.support.model.DescribeAttachmentResponse;
import software.amazon.awssdk.services.support.model.DescribeCasesRequest;
import software.amazon.awssdk.services.support.model.DescribeCasesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeCommunicationsResponse;
import software.amazon.awssdk.services.support.model.DescribeServicesRequest;
import software.amazon.awssdk.services.support.model.DescribeServicesResponse;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsRequest;
import
 software.amazon.awssdk.services.support.model.DescribeSeverityLevelsResponse;
import software.amazon.awssdk.services.support.model.ResolveCaseRequest;
import software.amazon.awssdk.services.support.model.ResolveCaseResponse;
import software.amazon.awssdk.services.support.model.Service;
import software.amazon.awssdk.services.support.model.SeverityLevel;
import software.amazon.awssdk.services.support.model.SupportException;
import software.amazon.awssdk.services.support.model.AddAttachmentsToSetRequest;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileNotFoundException;
import java.io.InputStream;
import java.time.Instant;
import java.time.temporal.ChronoUnit;
import java.util.ArrayList;
import java.util.List;

/**
 * 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 = """

                Usage:
                    <fileAttachment>Where:
                    fileAttachment - The file can be a simple saved .txt file to
 use as an email attachment.\s
                """;

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

        String fileAttachment = "C:\\AWS\\test.txt" ; //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《Amazon SDK for Java 2.x API Reference》中的以下主题。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase

- DescribeAttachment
- DescribeCases
- DescribeCommunications
- DescribeServices
- DescribeSeverityLevels
- ResolveCase

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

在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 * as inquirer from "@inquirer/prompts";
import { retry } from "@aws-doc-sdk-examples/lib/utils/util-timers.js";

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.",
      );
    }
    throw err;
  }
};

/**
 * Select a service from the list returned from DescribeServices.
 */
export const getService = async () => {
  const { services } = await client.send(new DescribeServicesCommand({}));
  const selectedService = await inquirer.select({
    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;
};

/**
 * @param {{ categories: import('@aws-sdk/client-support').Category[]}} service
 */
export const getCategory = async (service) => {
  const selectedCategory = await inquirer.select({
    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.select({
    message: "Select a severity level.",
    choices: severityLevels.map((s) => ({ name: s.name, value: s })),
  });
  return selectedSeverityLevel;
};

/**
 * Create a new support case
 * @param {{
 *  selectedService: import('@aws-sdk/client-support').Service
 *  selectedCategory: import('@aws-sdk/client-support').Category
 *  selectedSeverityLevel: import('@aws-sdk/client-support').SeverityLevel
 * }} selections
 * @returns
 */
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;
};

/**
 * @param {import('@aws-sdk/client-support').Communication[]} communications
```

```
 */
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.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.
 * @param {{
 *   caseId: string,
 *   cases: import('@aws-sdk/client-support').CaseDetails[]
 *   nextToken: string
 * }} options
 * @returns
```

```
 */
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《适用于 JavaScript 的 Amazon SDK API Reference》中的以下主题。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Kotlin

适用于 Kotlin 的 SDK

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

```
/**
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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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.fromEnvironment { 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《Amazon SDK for Kotlin API Reference》中的以下主题。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

Python

适用于 Python 的 SDK（Boto3）

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

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.")
```

定义一个包装支持客户端操作的类。

```
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《Amazon SDK for Python (Boto3) API Reference》中的以下主题。
  - AddAttachmentsToSet
  - AddCommunicationToCase
  - CreateCase
  - DescribeAttachment
  - DescribeCases
  - DescribeCommunications
  - DescribeServices
  - DescribeSeverityLevels
  - ResolveCase

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

Amazon Web Services 支持 使用的操作 Amazon SDKs

以下代码示例演示了如何使用执行单个 Amazon Web Services 支持 操作 Amazon SDKs。每个示例都包含一个指向的链接 GitHub，您可以在其中找到有关设置和运行代码的说明。

以下示例仅包括最常用的操作。有关完整列表，请参阅 Amazon Web Services 支持 API 参考。

示例

- AddAttachmentsToSet与 Amazon SDK 或 CLI 配合使用
- AddCommunicationToCase与 Amazon SDK 或 CLI 配合使用
- CreateCase与 Amazon SDK 或 CLI 配合使用
- DescribeAttachment与 Amazon SDK 或 CLI 配合使用
- DescribeCases与 Amazon SDK 或 CLI 配合使用
- DescribeCommunications与 Amazon SDK 或 CLI 配合使用
- DescribeServices与 Amazon SDK 或 CLI 配合使用
- DescribeSeverityLevels与 Amazon SDK 或 CLI 配合使用
- 将 DescribeTrustedAdvisorCheckRefreshStatuses 与 CLI 配合使用
- 将 DescribeTrustedAdvisorCheckResult 与 CLI 配合使用
- 将 DescribeTrustedAdvisorCheckSummaries 与 CLI 配合使用
- 将 DescribeTrustedAdvisorChecks 与 CLI 配合使用
- 将 RefreshTrustedAdvisorCheck 与 CLI 配合使用
- ResolveCase与 Amazon SDK 或 CLI 配合使用

`AddAttachmentsToSet`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `AddAttachmentsToSet`。

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：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

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

```
    /// <summary>
    /// 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 适用于 .NET 的 Amazon SDK API 参考[AddAttachmentsToSet](#)中的。

CLI

Amazon CLI

向集合添加附件

以下`add-attachments-to-set`示例向一组图片添加了一张图片，然后您可以为 Amazon 账户中的支持案例指定该图片。

```
aws support add-attachments-to-set \
```

```
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE" \
    --attachments fileName=troubleshoot-screenshot.png,data=base64-encoded-string
```

输出：

```
{
    "attachmentSetId": "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE",
    "expiryTime": "2020-05-14T17:04:40.790+0000"
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的案例管理。

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

Java

适用于 Java 的 SDK 2.x

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

```
   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 Amazon SDK for Java 2.x API 参考AddAttachmentsToSet中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

```
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 适用于 JavaScript 的 Amazon SDK API 参考AddAttachmentsToSet中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
suspend fun 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.fromEnvironment { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.addAttachmentsToSet(setRequest)
        return response.attachmentSetId
    }
}
```

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

Python

适用于 Python 的 SDK（Boto3）

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

```
class 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 的详细信息，请参阅适用AddAttachmentsToSet于 Python 的Amazon SDK (Boto3) API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`AddCommunicationToCase`与 Amazon SDK 或 CLI 配合使用

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

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：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

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

```
    /// <summary>
    /// 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 适用于 .NET 的 Amazon SDK API 参考AddCommunicationToCase中的。

CLI

Amazon CLI

向案例添加通信

以下add-communication-to-case示例将通信添加到您 Amazon 账户中的支持案例中。

```
aws support add-communication-to-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --communication-body "I'm attaching a set of images to this case." \
    --cc-email-addresses "myemail@example.com" \
    --attachment-set-id "as-2f5a6faa2a4a1e600-mu-nk5xQlBr70-
G1cUos5LZkd38KOAHZa9BMDVzNEXAMPLE"
```

输出：

```
{
    "result": true
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的案例管理。

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

Java

适用于 Java 的 SDK 2.x

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

```
   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 Amazon SDK for Java 2.x API 参考AddCommunicationToCase中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

```
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 适用于 JavaScript 的 Amazon SDK API 参考AddCommunicationToCase中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
suspend fun addAttachSupportCase(
    caseIdVal: String?,
    attachmentSetIdVal: String?,
) {
    val caseRequest =
        AddCommunicationToCaseRequest {
            caseId = caseIdVal
            attachmentSetId = attachmentSetIdVal
            communicationBody = "Please refer to attachment for details."
        }

    SupportClient.fromEnvironment { 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 的详细信息，请参阅适用AddCommunicationToCase于 K otlin 的Amazon SDK API 参考。

PowerShell

适用于 PowerShell V4 的工具

示例 1：将电子邮件通信的正文添加到指定案例中。

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

示例 2：将电子邮件通信的正文添加到指定案例中，另加上电子邮件抄送行中包含的一个或多个电子邮件地址。

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CcEmailAddress @("email1@address.com", "email2@address.com") -CommunicationBody
 "Some text about the case"
```

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

适用于 PowerShell V5 的工具

示例 1：将电子邮件通信的正文添加到指定案例中。

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CommunicationBody "Some text about the case"
```

示例 2：将电子邮件通信的正文添加到指定案例中，另加上电子邮件抄送行中包含的一个或多个电子邮件地址。

```
Add-ASACommunicationToCase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -
CcEmailAddress @("email1@address.com", "email2@address.com") -CommunicationBody
 "Some text about the case"
```

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

Python

适用于 Python 的 SDK（Boto3）

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

```
class 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 的详细信息，请参阅适用AddCommunicationToCase于 Python 的Amazon SDK (Boto3) API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`CreateCase`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `CreateCase`。

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：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

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

```
    /// <summary>
    /// Create a new 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 Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) 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 适用于 .NET 的 Amazon SDK API 参考CreateCase中的。

CLI

Amazon CLI

创建案例

以下create-case示例为您的 Amazon 账户创建了一个支持案例。

```
aws support create-case \
    --category-code "using-aws" \
    --cc-email-addresses "myemail@example.com" \
    --communication-body "I want to learn more about an AWS service." \
    --issue-type "technical" \
    --language "en" \
    --service-code "general-info" \
    --severity-code "low" \
    --subject "Question about my account"
```

输出：

```
{
    "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47"
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的案例管理。

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

Java

适用于 Java 的 SDK 2.x

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

```
   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 Amazon SDK for Java 2.x API 参考CreateCase中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

```
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 适用于 JavaScript 的 Amazon SDK API 参考CreateCase中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
suspend fun 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.fromEnvironment { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.createCase(caseRequest)
        return response.caseId
    }
}
```

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

PowerShell

适用于 PowerShell V4 的工具

示例 1：在 Su Amazon pport Center 中创建新案例。-ServiceCode 和-CategoryCode 参数的值可以使用 Get-ASAService cmdlet 获取。-SeverityCode 参数的值可以使用 Get-ASASeverityLevel cmdlet 获得。-IssueType 参数值可以是 “客户服务” 或 “技术”。如果成功，则 Amazon 输出 Support 案例编号。默认情况下，案例将用英语处理，要使用日语，请添加 -Language“ja”参数。-ServiceCode、-CategoryCode、-主题和-CommunicationBody 参数是必需的。

```
New-ASACase -ServiceCode "amazon-cloudfront" -CategoryCode "APIs" -SeverityCode
 "low" -Subject "subject text" -CommunicationBody "description of the case" -
CcEmailAddress @("email1@domain.com", "email2@domain.com") -IssueType "technical"
```

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

适用于 PowerShell V5 的工具

示例 1：在 Su Amazon pport Center 中创建新案例。-ServiceCode 和-CategoryCode 参数的值可以使用 Get-ASAService cmdlet 获取。-SeverityCode 参数的值可以使用 Get-ASASeverityLevel cmdlet 获得。-IssueType 参数值可以是 “客户服务” 或 “技术”。如果成功，则 Amazon 输出 Support 案例编号。默认情况下，案例将用英语处理，要使用日语，请添加 -Language“ja”参数。-ServiceCode、-CategoryCode、-主题和-CommunicationBody 参数是必需的。

```
New-ASACase -ServiceCode "amazon-cloudfront" -CategoryCode "APIs" -SeverityCode
 "low" -Subject "subject text" -CommunicationBody "description of the case" -
CcEmailAddress @("email1@domain.com", "email2@domain.com") -IssueType "technical"
```

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

Python

适用于 Python 的 SDK（Boto3）

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

```
class 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 的详细信息，请参阅适用CreateCase于 Python 的Amazon SDK (Boto3) API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeAttachment`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DescribeAttachment`。

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：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

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

```
    /// <summary>
    /// 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 适用于 .NET 的 Amazon SDK API 参考DescribeAttachment中的。

CLI

Amazon CLI

描述附件

以下 `describe-attachment` 示例返回有关带指定 ID 的附件的信息。

```
aws support describe-attachment \
```

```
    --attachment-id "attachment-KBnjRNrePd9D6Jx0-Mm00xZuDEaL2JAj_0-
gJv9qqDooTipsz3V1Nb19rCfkZneeQeDPgp8X1iVJyHH7UuhZDdNeqGoduZsPrAhyMakqlc60-
iJjL5HqyYGiT1FG8EXAMPLE"
```

输出：

```
{
    "attachment": {
        "fileName": "troubleshoot-screenshot.png",
        "data": "base64-blob"
    }
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的案例管理。

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

Java

适用于 Java 的 SDK 2.x

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

```
   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 Amazon SDK for Java 2.x API 参考DescribeAttachment中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

```
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 适用于 JavaScript 的 Amazon SDK API 参考DescribeAttachment中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
suspend fun describeAttachment(attachId: String?) {
    val attachmentRequest =
        DescribeAttachmentRequest {
            attachmentId = attachId
        }

    SupportClient.fromEnvironment { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.describeAttachment(attachmentRequest)
        println("The name of the file is ${response.attachment?.fileName}")
    }
}
```

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

Python

适用于 Python 的 SDK（Boto3）

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

```
class 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 的详细信息，请参阅适用DescribeAttachment于 Python 的Amazon SDK (Boto3) API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeCases`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DescribeCases`。

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：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

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

```
    /// <summary>
    /// 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 Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
 (“ko”) 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 适用于 .NET 的 Amazon SDK API 参考DescribeCases中的。

CLI

Amazon CLI

描述案例

以下describe-cases示例返回有关您 Amazon 账户中指定支持案例的信息。

```
aws support describe-cases \
    --display-id "1234567890" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --include-resolved-cases \
    --language "en" \
    --no-include-communications \
    --max-item 1
```

输出：

```
{
    "cases": [
        {
            "status": "resolved",
            "ccEmailAddresses": [],
            "timeCreated": "2020-03-23T21:31:47.774Z",
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "severityCode": "low",
            "language": "en",
            "categoryCode": "using-aws",
            "serviceCode": "general-info",
            "submittedBy": "myemail@example.com",
            "displayId": "1234567890",
            "subject": "Question about my account"
        }
    ]
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的案例管理。

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

Java

适用于 Java 的 SDK 2.x

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

```
   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 Amazon SDK for Java 2.x API 参考DescribeCases中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

```
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 适用于 JavaScript 的 Amazon SDK API 参考DescribeCases中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
suspend fun 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.fromEnvironment { 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 的详细信息，请参阅适用DescribeCases于 K otlin 的Amazon SDK API 参考。

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回所有支持案例的详细信息。

```
Get-ASACase
```

示例 2：返回自指定日期和时间以来所有支持案例的详细信息。

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

示例 3：返回前 10 个支持案例的详细信息，包括已解决的支持案例。

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

示例 4：返回单个指定支持案例的详细信息。

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

示例 5：返回指定支持案例的详细信息。

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

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

适用于 PowerShell V5 的工具

示例 1：返回所有支持案例的详细信息。

```
Get-ASACase
```

示例 2：返回自指定日期和时间以来所有支持案例的详细信息。

```
Get-ASACase -AfterTime "2013-09-10T03:06Z"
```

示例 3：返回前 10 个支持案例的详细信息，包括已解决的支持案例。

```
Get-ASACase -MaxResult 10 -IncludeResolvedCases $true
```

示例 4：返回单个指定支持案例的详细信息。

```
Get-ASACase -CaseIdList "case-12345678910-2013-c4c1d2bf33c5cf47"
```

示例 5：返回指定支持案例的详细信息。

```
Get-ASACase -CaseIdList @("case-12345678910-2013-c4c1d2bf33c5cf47",
 "case-18929034710-2011-c4fdeabf33c5cf47")
```

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

Python

适用于 Python 的 SDK（Boto3）

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

```
class 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 的详细信息，请参阅适用DescribeCases于 Python 的Amazon SDK (Boto3) API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeCommunications`与 Amazon SDK 或 CLI 配合使用

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

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：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

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

```
    /// <summary>
    /// 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 适用于 .NET 的 Amazon SDK API 参考[DescribeCommunications](#)中的。

CLI

Amazon CLI

描述案例的最新通信

以下`describe-communications`示例返回您 Amazon 账户中指定支持案例的最新通信。

```
aws support describe-communications \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47" \
    --after-time "2020-03-23T21:31:47.774Z" \
    --max-item 1
```

输出：

```
{
    "communications": [
        {
            "body": "I want to learn more about an AWS service.",
            "attachmentSet": [],
            "caseId": "case-12345678910-2013-c4c1d2bf33c5cf47",
            "timeCreated": "2020-05-12T23:12:35.000Z",
            "submittedBy": "Amazon Web Services"
        }
    ],
```

```
    "NextToken":
 "eyJuZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQEXAMPLE=="
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的案例管理。

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

Java

适用于 Java 的 SDK 2.x

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

```
   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 Amazon SDK for Java 2.x API 参考DescribeCommunications中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

```
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 适用于 JavaScript 的 Amazon SDK API 参考DescribeCommunications中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
suspend fun listCommunications(caseIdVal: String?): String? {
    val communicationsRequest =
        DescribeCommunicationsRequest {
            caseId = caseIdVal
            maxResults = 10
        }

    SupportClient.fromEnvironment { 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 的详细信息，请参阅适用DescribeCommunications于 K otlin 的Amazon SDK API 参考。

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回指定案例的所有通信。

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

示例 2：返回自协调世界时 2012 年 1 月 1 日午夜以来针对指定案例的所有通信。

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

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

适用于 PowerShell V5 的工具

示例 1：返回指定案例的所有通信。

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

示例 2：返回自协调世界时 2012 年 1 月 1 日午夜以来针对指定案例的所有通信。

```
Get-ASACommunication -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47" -AfterTime
 "2012-01-10T00:00Z"
```

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

Python

适用于 Python 的 SDK（Boto3）

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

```
class 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 的详细信息，请参阅适用DescribeCommunications于 Python 的Amazon SDK (Boto3) API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeServices`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `DescribeServices`。

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：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

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

```
    /// <summary>
    /// Get the descriptions of AWS services.
    /// </summary>
    /// <param name="name">Optional language for services.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) 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 适用于 .NET 的 Amazon SDK API 参考DescribeServices中的。

CLI

Amazon CLI

列出 Amazon 服务和服务类别

以下 `describe-services` 示例列出了用于请求一般信息的可用服务类别。

```
aws support describe-services \
    --service-code-list "general-info"
```

输出：

```
{
    "services": [
        {
            "code": "general-info",
            "name": "General Info and Getting Started",
            "categories": [
                {
                    "code": "charges",
                    "name": "How Will I Be Charged?"
                },
                {
                    "code": "gdpr-queries",
                    "name": "Data Privacy Query"
                },
                {
                    "code": "reserved-instances",
                    "name": "Reserved Instances"
                },
                {
                    "code": "resource",
                    "name": "Where is my Resource?"
                },
                {
                    "code": "using-aws",
                    "name": "Using AWS & Services"
                },
                {
                    "code": "free-tier",
                    "name": "Free Tier"
                },
                {
                    "code": "security-and-compliance",
                    "name": "Security & Compliance"
                },
                {
                    "code": "account-structure",
                    "name": "Account Structure"
                }
```

```
            ]
        }
    ]
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的案例管理。

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

Java

适用于 Java 的 SDK 2.x

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

```
   // 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 Amazon SDK for Java 2.x API 参考DescribeServices中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
// 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.fromEnvironment { 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 的详细信息，请参阅适用DescribeServices于 K otlin 的Amazon SDK API 参考。

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回所有可用的服务代码、名称和类别。

```
Get-ASAService
```

示例 2：返回带有指定代码的服务的名称和类别。

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

示例 3：返回指定服务代码的名称和类别。

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

示例 4：返回指定服务代码的名称和类别（日语）。目前支持英语（“en”）和日语（“ja”）语言代码。

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

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

适用于 PowerShell V5 的工具

示例 1：返回所有可用的服务代码、名称和类别。

```
Get-ASAService
```

示例 2：返回带有指定代码的服务的名称和类别。

```
Get-ASAService -ServiceCodeList "amazon-cloudfront"
```

示例 3：返回指定服务代码的名称和类别。

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch")
```

示例 4：返回指定服务代码的名称和类别（日语）。目前支持英语（“en”）和日语（“ja”）语言代码。

```
Get-ASAService -ServiceCodeList @("amazon-cloudfront", "amazon-cloudwatch") -
Language "ja"
```

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

Python

适用于 Python 的 SDK（Boto3）

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

```
class 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 的详细信息，请参阅适用DescribeServices于 Python 的Amazon SDK (Boto3) API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`DescribeSeverityLevels`与 Amazon SDK 或 CLI 配合使用

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

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：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

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

```
    /// <summary>
    /// Get the descriptions of support severity levels.
    /// </summary>
    /// <param name="name">Optional language for severity levels.
    /// Currently Chinese (“zh”), English ("en"), Japanese ("ja") and Korean
(“ko”) 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 适用于 .NET 的 Amazon SDK API 参考DescribeSeverityLevels中的。

CLI

Amazon CLI

列出可用的严重性级别

以下 `describe-severity-levels` 示例列出了支持案例的可用严重性级别。

```
aws support describe-severity-levels
```

输出：

```
{
    "severityLevels": [
        {
            "code": "low",
            "name": "Low"
        },
        {
            "code": "normal",
            "name": "Normal"
        },
        {
            "code": "high",
            "name": "High"
        },
        {
            "code": "urgent",
            "name": "Urgent"
        },
        {
            "code": "critical",
            "name": "Critical"
        }
    ]
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的选择严重性。

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

Java

适用于 Java 的 SDK 2.x

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

```
   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 Amazon SDK for Java 2.x API 参考[DescribeSeverityLevels](#)中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

```
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 适用于 JavaScript 的 Amazon SDK API 参考DescribeSeverityLevels中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
suspend fun displaySevLevels(): String {
    var levelName = ""
    val severityLevelsRequest =
        DescribeSeverityLevelsRequest {
            language = "en"
        }

    SupportClient.fromEnvironment { 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 的详细信息，请参阅适用DescribeSeverityLevels于 K otlin 的Amazon SDK API 参考。

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回可分配给 Support 案例的 Amazon 严重性级别列表。

```
Get-ASASeverityLevel
```

示例 2：返回可以分配给 Support 案例的 Amazon 严重性级别列表。级别名称以日语返回。

```
Get-ASASeverityLevel -Language "ja"
```

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

适用于 PowerShell V5 的工具

示例 1：返回可分配给 Support 案例的 Amazon 严重性级别列表。

```
Get-ASASeverityLevel
```

示例 2：返回可以分配给 Support 案例的 Amazon 严重性级别列表。级别名称以日语返回。

```
Get-ASASeverityLevel -Language "ja"
```

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

Python

适用于 Python 的 SDK（Boto3）

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

```
class 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 的详细信息，请参阅适用DescribeSeverityLevels于 Python 的Amazon SDK (Boto3) API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 `DescribeTrustedAdvisorCheckRefreshStatuses` 与 CLI 配合使用

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

CLI

Amazon CLI

列出 Truste Amazon d Advisor 检查的刷新状态

以下 `describe-trusted-advisor-check-refresh-statuses` 示例列出两个 Trusted Advisor 检查的刷新状态：Amazon S3 存储桶权限和 IAM 使用。

```
aws support describe-trusted-advisor-check-refresh-statuses \
```

```
    --check-id "Pfx0RwqBli" "zXCkfM1nI3"
```

输出：

```
{
    "statuses": [
        {
            "checkId": "Pfx0RwqBli",
            "status": "none",
            "millisUntilNextRefreshable": 0
        },
        {
            "checkId": "zXCkfM1nI3",
            "status": "none",
            "millisUntilNextRefreshable": 0
        }
    ]
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的 Amazon Trusted Advisor。

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

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回指定检查的刷新请求的当前状态。Request-ASATrusted AdvisorCheckRefresh 可用于请求刷新支票的状态信息。

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

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

适用于 PowerShell V5 的工具

示例 1：返回指定检查的刷新请求的当前状态。Request-ASATrusted AdvisorCheckRefresh 可用于请求刷新支票的状态信息。

```
Get-ASATrustedAdvisorCheckRefreshStatus -CheckId @("checkid1", "checkid2")
```

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

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DescribeTrustedAdvisorCheckResult** 与 CLI 配合使用

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

CLI

Amazon CLI

列出 Tru Amazon sted Advisor 检查的结果

以下 describe-trusted-advisor-check-result 示例列出 IAM 使用检查的结果。

```
aws support describe-trusted-advisor-check-result \
    --check-id "zXCkfM1nI3"
```

输出：

```
{
    "result": {
        "checkId": "zXCkfM1nI3",
        "timestamp": "2020-05-13T21:38:05Z",
        "status": "ok",
        "resourcesSummary": {
            "resourcesProcessed": 1,
            "resourcesFlagged": 0,
            "resourcesIgnored": 0,
            "resourcesSuppressed": 0
        },
        "categorySpecificSummary": {
            "costOptimizing": {
                "estimatedMonthlySavings": 0.0,
                "estimatedPercentMonthlySavings": 0.0
            }
        },
        "flaggedResources": [
```

```
            {
                "status": "ok",
                "resourceId": "47DEQpj8HBSa-_TImW-5JCeuQeRkm5NMpJWZEXAMPLE",
                "isSuppressed": false
            }
        ]
    }
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的 Amazon Trusted Advisor。

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

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回 Trusted Advisor 检查的结果。可用 Trusted Advisor 支票列表可以使用 Get-获取 ASATrustedAdvisorChecks。输出是检查的总体状态、上次运行检查的时间戳以及特定检查的唯一 checkid。要以日语输出结果，请添加 -Language“ja”参数。

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

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

适用于 PowerShell V5 的工具

示例 1：返回 Trusted Advisor 检查的结果。可用 Trusted Advisor 支票列表可以使用 Get-获取 ASATrustedAdvisorChecks。输出是检查的总体状态、上次运行检查的时间戳以及特定检查的唯一 checkid。要以日语输出结果，请添加 -Language“ja”参数。

```
Get-ASATrustedAdvisorCheckResult -CheckId "checkid1"
```

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

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DescribeTrustedAdvisorCheckSummaries** 与 CLI 配合使用

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

CLI

Amazon CLI

列出 Tru Amazon sted Advisor 支票摘要

以下 describe-trusted-advisor-check-summaries 示例列出两个 Trusted Advisor 检查的结果：Amazon S3 存储桶权限和 IAM 使用。

```
aws support describe-trusted-advisor-check-summaries \
    --check-ids "Pfx0RwqBli" "zXCkfM1nI3"
```

输出：

```
{
    "summaries": [
        {
            "checkId": "Pfx0RwqBli",
            "timestamp": "2020-05-13T21:38:12Z",
            "status": "ok",
            "hasFlaggedResources": true,
            "resourcesSummary": {
                "resourcesProcessed": 44,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        },
        {
            "checkId": "zXCkfM1nI3",
            "timestamp": "2020-05-13T21:38:05Z",
            "status": "ok",
            "hasFlaggedResources": true,
```

```
            "resourcesSummary": {
                "resourcesProcessed": 1,
                "resourcesFlagged": 0,
                "resourcesIgnored": 0,
                "resourcesSuppressed": 0
            },
            "categorySpecificSummary": {
                "costOptimizing": {
                    "estimatedMonthlySavings": 0.0,
                    "estimatedPercentMonthlySavings": 0.0
                }
            }
        }
    ]
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的 Amazon Trusted Advisor。

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

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回指定 Trusted Advisor 检查的最新摘要。

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

示例 2：返回指定 Trusted Advisor 检查的最新摘要。

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

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

适用于 PowerShell V5 的工具

示例 1：返回指定 Trusted Advisor 检查的最新摘要。

```
Get-ASATrustedAdvisorCheckSummary -CheckId "checkid1"
```

示例 2：返回指定 Trusted Advisor 检查的最新摘要。

```
Get-ASATrustedAdvisorCheckSummary -CheckId @("checkid1", "checkid2")
```

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

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **DescribeTrustedAdvisorChecks** 与 CLI 配合使用

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

CLI

Amazon CLI

列出可用的 T Amazon rusted Advisor 支票

以下describe-trusted-advisor-checks示例列出了您 Amazon 账户中可用的 Trusted Advisor 支票。这些信息包括检查名称、ID、描述、类别和元数据。请注意，为便于阅读，输出已缩短。

```
aws support describe-trusted-advisor-checks \
    --language "en"
```

输出：

```
{
    "checks": [
        {
            "id": "zXCkfM1nI3",
            "name": "IAM Use",
            "description": "Checks for your use of AWS Identity and Access
 Management (IAM). You can use IAM to create users, groups, and roles in
 AWS, and you can use permissions to control access to AWS resources. \n<br>
\n<br>\n<b>Alert Criteria</b><br>\nYellow: No IAM users have been created
 for this account.\n<br>\n<br>\n<b>Recommended Action</b><br>\nCreate one or
 more IAM users and groups in your account. You can then create additional
 users whose permissions are limited to perform specific tasks in your AWS
 environment. For more information, see <a href=\"https://docs.aws.amazon.com/
```

```
IAM/latest/UserGuide/IAMGettingStarted.html\" target=\"_blank\">Getting
 Started</a>. \n<br><br>\n<b>Additional Resources</b><br>\n<a href=\"https://
docs.aws.amazon.com/IAM/latest/UserGuide/IAM_Introduction.html\" target=\"_blank
\">What Is IAM?</a>",
            "category": "security",
            "metadata": []
        }
    ]
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的 Amazon Trusted Advisor。

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

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回 Trusted Advisor 检查的集合。必须指定 Language 参数，该参数可以接受“en”（表示英语输出），也可以接受“ja”（表示日语输出）。

```
Get-ASATrustedAdvisorCheck -Language "en"
```

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

适用于 PowerShell V5 的工具

示例 1：返回 Trusted Advisor 检查的集合。必须指定 Language 参数，该参数可以接受“en”（表示英语输出），也可以接受“ja”（表示日语输出）。

```
Get-ASATrustedAdvisorCheck -Language "en"
```

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

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

将 **RefreshTrustedAdvisorCheck** 与 CLI 配合使用

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

CLI

Amazon CLI

刷新 Tru Amazon sted Advisor 支票

以下`refresh-trusted-advisor-check`示例刷新了您 Amazon 账户中的 Amazon S3 存储桶权限 Trusted Advisor 支票。

```
aws support refresh-trusted-advisor-check \
    --check-id "Pfx0RwqBli"
```

输出：

```
{
    "status": {
        "checkId": "Pfx0RwqBli",
        "status": "enqueued",
        "millisUntilNextRefreshable": 3599992
    }
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的 Amazon Trusted Advisor。

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

PowerShell

适用于 PowerShell V4 的工具

示例 1：请求刷新指定的 Trusted Advisor 检查。

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

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

适用于 PowerShell V5 的工具

示例 1：请求刷新指定的 Trusted Advisor 检查。

```
Request-ASATrustedAdvisorCheckRefresh -CheckId "checkid1"
```

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

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

`ResolveCase`与 Amazon SDK 或 CLI 配合使用

以下代码示例演示如何使用 `ResolveCase`。

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：

- 了解基本功能

.NET

适用于 .NET 的 Amazon SDK

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

```
/// <summary>
/// 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 适用于 .NET 的 Amazon SDK API 参考ResolveCase中的。

CLI

Amazon CLI

处理支持案例

以下resolve-case示例解决了您 Amazon 账户中的一个支持案例。

```
aws support resolve-case \
    --case-id "case-12345678910-2013-c4c1d2bf33c5cf47"
```

输出：

```
{
    "finalCaseStatus": "resolved",
    "initialCaseStatus": "work-in-progress"
}
```

有关更多信息，请参阅《Amazon Support 用户指南》中的案例管理。

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

Java

适用于 Java 的 SDK 2.x

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

```
   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 Amazon SDK for Java 2.x API 参考ResolveCase中的。

JavaScript

适用于 JavaScript (v3) 的软件开发工具包

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

```
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 适用于 JavaScript 的 Amazon SDK API 参考ResolveCase中的。

Kotlin

适用于 Kotlin 的 SDK

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

```
suspend fun resolveSupportCase(caseIdVal: String) {
    val caseRequest =
        ResolveCaseRequest {
            caseId = caseIdVal
        }
    SupportClient.fromEnvironment { region = "us-west-2" }.use { supportClient ->
        val response = supportClient.resolveCase(caseRequest)
        println("The status of case $caseIdVal is ${response.finalCaseStatus}")
    }
}
```

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

PowerShell

适用于 PowerShell V4 的工具

示例 1：返回指定案例的初始状态和完成用于解决该案例的调用后的当前状态。

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

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

适用于 PowerShell V5 的工具

示例 1：返回指定案例的初始状态和完成用于解决该案例的调用后的当前状态。

```
Resolve-ASACase -CaseId "case-12345678910-2013-c4c1d2bf33c5cf47"
```

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

Python

适用于 Python 的 SDK（Boto3）

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

```
class 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 的详细信息，请参阅适用ResolveCase于 Python 的Amazon SDK (Boto3) API 参考。

有关 S Amazon DK 开发者指南和代码示例的完整列表，请参阅Amazon Web Services 支持 与 Amazon SDK 一起使用。本主题还包括有关入门的信息以及有关先前的 SDK 版本的详细信息。

Amazon Web Services 支持 的监控和日志记录

监控是保持 Amazon Web Services 支持 和您的其他 Amazon 解决方案的可靠性、可用性和性能的重要方面。Amazon 提供了以下一些监控工具来监控 Amazon Web Services 支持、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，这些系统事件描述了 Amazon 资源中的更改。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，并在这些事件发生时在其他 Amazon 服务中触发自动操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。
- Amazon CloudTrail 捕获由您的 Amazon 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 Amazon S3 桶。您可以标识哪些用户和账户调用了 Amazon、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《Amazon CloudTrail 用户指南》。

主题

使用 Amazon EventBridge 将 Amazon Web Services 支持 集成到事件驱动型应用程序中

您可以将 Amazon Web Services 支持 集成到事件驱动型应用程序（EDA）中，这类应用程序使用 Amazon Web Services 支持 中发生的事件在应用程序组件之间进行通信并启动下游进程。

例如，当您的账户中发生以下 Amazon Web Services 支持 事件时，您会收到通知：

- 创建、解决或重新打开支持案例
- 将通信添加到现有支持案例

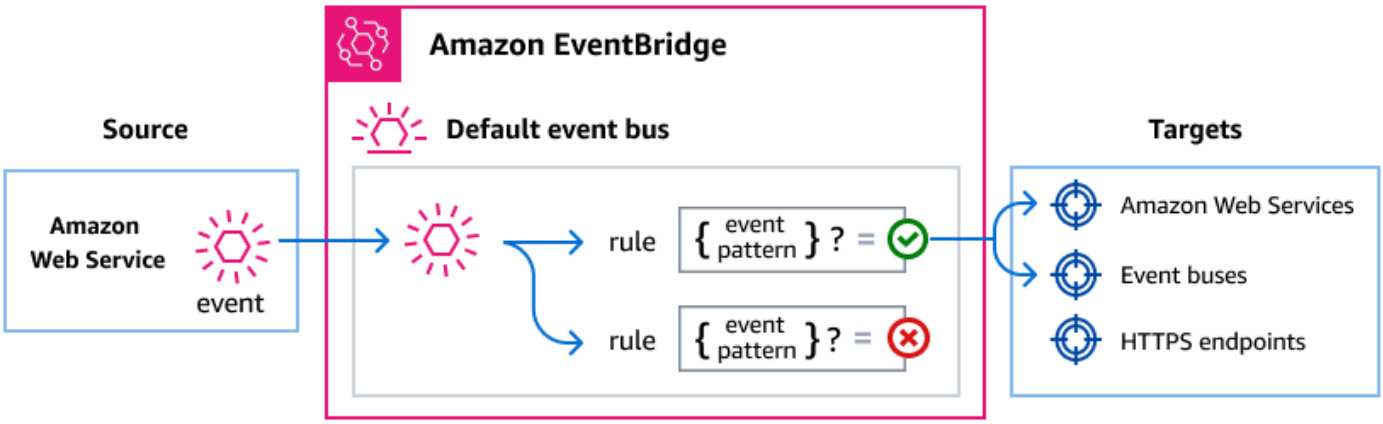
为此，您可以使用 Amazon EventBridge 将事件从 Amazon Web Services 支持 路由到其他软件组件。Amazon EventBridge 是一项无服务器服务，该服务使用事件将应用程序组件连接起来，让您无需额外代码和操作，就能更轻松地将 Amazon Web Services 支持 等 Amazon 服务集成到事件驱动型架构中。

EventBridge 如何路由 Amazon Web Services 支持 事件

以下介绍 EventBridge 如何与 Amazon Web Services 支持 事件协同工作：

与许多 Amazon 服务一样，Amazon Web Services 支持 会生成事件并将其发送到 EventBridge 的默认事件总线。事件总线是接收事件并将其路由到您所指定的目的地或目标的路由器。目标可以包括其他 Amazon 服务、自定义应用程序以及 SaaS 合作伙伴应用程序。

EventBridge 根据您在事件总线上创建的规则来路由事件。对于每条规则，您可以指定筛选条件或事件模式，以便仅选择所需的事件。每当向事件总线发送事件时，EventBridge 都会将其与每条规则进行比较。如果事件与规则匹配，EventBridge 就会将该事件路由到指定的目标。



Amazon Web Services 支持 事件

Amazon Web Services 支持 会自动将以下事件发送到默认的 EventBridge 事件总线。

事件详细信息类型	描述
支持案例更新	表示支持案例中的更改。

事件结构

来自 Amazon 服务的所有事件均包含两种类型的数据：

- 一组公共字段，其中包含有关事件的元数据，例如作为事件来源的 Amazon 服务、事件的生成时间、事件发生的账户和区域以及其他信息。有关这些常规字段的定义，请参阅《Amazon EventBridge 事件参考》中的事件结构。

- `detail` 字段包含该特定服务事件专有的数据。

通过 Amazon CloudTrail 传输 Amazon Web Services 支持 事件

Amazon 服务可直接将事件发送到 EventBridge 默认事件总线。此外，Amazon CloudTrail 还会将源自众多 Amazon 服务的事件发送至 EventBridge。这些事件可能包括 API 调用、控制台登录和操作、服务事件以及 CloudTrail Insights。有关更多信息，请参阅《EventBridge 用户指南》中的通过 Amazon CloudTrail 传输的 Amazon 服务事件。

有关发送到 EventBridge 的 Amazon Web Services 支持 事件列表，请参阅《EventBridge 事件参考》中的 Amazon Web Services 支持 主题。

创建与 Amazon Web Services 支持 事件匹配的事件模式

事件模式是一种筛选条件，用于指定您要选择的事件应包含的数据。

每个事件模式是一个 JSON 对象，其中包含：

- 标识发送事件的服务的 `source` 属性。对于 Amazon Web Services 支持 事件，来源是 `aws.support`。
- （可选）：包含要匹配的事件名称数组的 `detail-type` 属性。
- （可选）：包含要匹配的其他事件数据的 `detail` 属性。

例如，以下事件模式将从 Amazon Web Services 支持 中选择所有支持案例更新事件：

```
{
  "source": ["aws.support"],
  "detail-type": ["Support Case Update"]
}
```

通过在事件本身中包含值，让事件选择更具针对性。例如，以下事件模式与代表正重新打开的案例的支持案例更新事件相匹配：

```
{
  "source": ["aws.support"],
  "detail-type": ["Support Case Update"],
  "detail": {
      "event-name": "ReopenCase"
    }
```

```
}
```

有关写入事件模式的更多信息，请参阅《EventBridge 用户指南》中的 Event patterns。

另请参阅

有关如何将 EventBridge 与 Amazon Web Services 支持 配合使用的更多信息，请参阅以下资源：

- 如何使用 Amazon EventBridge 自动化 Amazon Web Services 支持 API
- GitHub 上的 Amazon Web Services 支持 案例活动通知程序

支持案例更新事件

以下是 `Support Case Update` 事件的详细信息字段。

`source` 和 `detail-type` 字段包含在下面，是因为其包含 Amazon Web Services 支持 事件的特定值。有关所有事件中包含的其它元数据字段的定义，请参阅《Amazon EventBridge 事件参考》中的事件结构。

```
{
  . . .,
  "detail-type": "Support Case Update",
  "source": "aws.support",
  . . .,
  "detail": {
    "case-id" : "string",
    "display-id" : "string",
    "communication-id" : "string",
    "event-name" : "string",
    "origin" : "string"
  }
}
```

`detail-type`

标识事件的类型。

对于这一事件，此值为 `Support Case Update`。

`source`

标识生成事件的服务。对于 Amazon Web Services 支持 事件，此值为 `aws.support`。

`detail`

包含关于事件信息的 JSON 对象。生成事件的服务决定该字段的内容。

对于此事件，此数据包括：

`case-id`

支持案例 ID。案例 ID 是一个字母数字字符串，格式如下：case-12345678910-2013-c4c1d2bf33c5cf47。

`display-id`

Amazon Web Services 支持 Center 页面上案例的标识符。

`communication-id`

通信 ID。

`event-name`

有效值：`CreateCase` |`AddCommunicationToCase` |`ResolveCase` |`ReopenCase`

指定支持案例事件的类型。

`origin`

有效值：`Amazon` |`CUSTOMER`

指定是您还是 Amazon Web Services 支持 坐席向支持案例添加了案例通信。

目前，仅 `event-name` 为 `AddCommunicationToCase` 的事件会包含此值。

Example支持案例更新事件示例：支持案例已创建

```
{
    "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支持案例更新事件示例：Amazon Web Services 支持 回复支持案例

```
{
    "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支持案例更新事件示例：支持案例已解决

```
{
    "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支持案例更新事件示例：支持案例已重新打开

```
{
    "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": ""
    }
}
```

使用 Amazon CloudTrail 记录 Amazon Web Services 支持 API 调用

Amazon Web Services 支持 与 Amazon CloudTrail 集成，后者是在 Amazon 中记录用户、角色或 Amazon Web Services 支持 服务所执行操作的服务。CloudTrail 将 Amazon Web Services 支持 的 API 调用作为事件捕获。捕获的调用包含来自 Amazon Web Services 支持 控制台和代码的 Amazon Web Services 支持 API 操作调用。

如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon Simple Storage Service (Amazon S3) 存储桶（包括 Amazon Web Services 支持 的事件）。如果您不配置跟踪记录，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。

使用 CloudTrail 收集的信息，您可以确定向 Amazon Web Services 支持 发出了什么请求、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。

要了解有关 CloudTrail 的更多信息（包括如何对其进行配置和启用），请参阅《Amazon CloudTrail 用户指南》。

Amazon Web Services 支持CloudTrail 中的 信息

在您创建 Amazon 账户时，将在该账户上启用 CloudTrail。当 Amazon Web Services 支持 中发生受支持的事件活动时，该活动将记录在 CloudTrail 事件中，并与其他 Amazon 服务事件一同保存在 Event history（事件历史记录）中。您可以在 Amazon 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 Amazon 账户中的事件（包括 Amazon Web Services 支持 的事件），请创建跟踪。通过跟踪记录，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 Amazon 区域。此跟踪记录在 Amazon 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 Amazon S3 存储桶。此外，您可以配置其他 Amazon 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：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个账户接收 CloudTrail 日志文件

CloudTrail 记录所有 Amazon Web Services 支持 API 操作，Amazon Web Services 支持 API 参考中介绍了这些操作。

例如，对 `CreateCase`、`DescribeCases` 和 `ResolveCase` 操作的调用将在 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 Amazon Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 Amazon 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

您也可以将多个 Amazon 区域和多个 Amazon 账户的 Amazon Web Services 支持 日志文件聚合到单个 Amazon S3 存储桶中。

Amazon Trusted AdvisorCloudTrail 日志记录中的 信息

Trusted Advisor 是一项 Amazon Web Services 支持 服务，您可以用它检查您的 Amazon 账户以了解如何节省成本、增强安全性和优化您的账户。

CloudTrail 记录所有 Trusted Advisor API 操作，Amazon Web Services 支持 API 参考中介绍了这些操作。

例如，对 `DescribeTrustedAdvisorCheckRefreshStatuses`、`DescribeTrustedAdvisorCheckResult` 和 `RefreshTrustedAdvisorCheck` 操作的调用将在 CloudTrail 日志文件中生成条目。

> **Note**
>
> CloudTrail 还会记录 Trusted Advisor 控制台操作。请参阅使用 Amazon CloudTrail 记录 Amazon Trusted Advisor 控制台操作。

了解 Amazon Web Services 支持 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：CreateCase 的日志条目

以下示例显示了 CreateCase 操作的一个 CloudTrail 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：RefreshTrustedAdvisorCheck 的日志条目

以下示例显示了 RefreshTrustedAdvisorCheck 操作的一个 CloudTrail 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 Amazon CloudTrail 记录 Slack API 调用中的 Amazon Web Services 支持 App

Slack 中的 Amazon Web Services 支持 App 已与 Amazon CloudTrail 集成。CloudTrail 提供了用户、角色或 Amazon Web Services 支持 App 中的 Amazon Web Services 服务 所执行操作的记录。为创建此记录，CloudTrail 会将 Amazon Web Services 支持 App 的所有公有 API 调用捕获为事件。这些捕获的调用包含来自 Amazon Web Services 支持 App 控制台的调用和代码对 Amazon Web Services 支持 App 公有 API 操作的调用。如果您创建了跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶。其中包括 Amazon Web Services 支持 App 事件。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的事件历史记录中查看最新事件。您可以使用 CloudTrail 所收集的信息来确定向 Amazon Web Services 支持 App 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。

要了解有关 CloudTrail 的更多信息，请参阅《Amazon CloudTrail 用户指南》https://docs.amazonaws.cn/awscloudtrail/latest/userguide/cloudtrail-user-guide.html。

CloudTrail 中的 Amazon Web Services 支持 App 信息

创建 Amazon Web Services 账户 后即可将在该账户上激活 CloudTrail。当 Amazon Web Services 支持 App 中发生公有 API 活动时，该活动将记录在 CloudTrail 事件中，并与其他 Amazon 服务事件一同保存在 Event history（事件历史记录）中。您可以在 Amazon Web Services 账户 中查看、搜索和下载最新事件。有关更多信息，请参阅 Viewing events with CloudTrail Event history。

要持续记录 Amazon Web Services 账户 中的事件（包括 Amazon Web Services 支持 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Amazon Web Services 区域。此跟踪记录在 Amazon 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）存储桶。此外，您可以配置其他 Amazon Web Services 服务，进一步分析在 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：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- Configuring Amazon SNS notifications for 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

CloudTrail 记录了所有公有 Amazon Web Services 支持 App 操作。这些操作也记录在 Amazon Web Services 支持 App in Slack API Reference 中。例如，对 `CreateSlackChannelConfiguration`、`GetAccountAlias` 和 `UpdateSlackChannelConfiguration` 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 Amazon Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 Amazon Web Services 服务 发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Amazon Web Services 支持 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记账条目。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 CreateSlackChannelConfiguration 操作的一个 CloudTrail 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 ListSlackChannelConfigurations 操作的一个 CloudTrail 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 GetAccountAlias 操作的一个 CloudTrail 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"
}
```

Amazon Web Services 支持 Plans 的监控和日志记录

监控是保持 Support Plans 和您的其他 Amazon 解决方案的可靠性、可用性和性能的重要方面。Amazon 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：

- Amazon CloudTrail 捕获由您的 Amazon 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 Amazon S3 桶。您可以标识哪些用户和账户调用了 Amazon、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《Amazon CloudTrail 用户指南》。

主题

使用 Amazon CloudTrail 记录 Amazon Web Services 支持 Plans API 调用

Amazon Web Services 支持 Plans与 Amazon CloudTrail 集成，后者是记录用户、角色或 Amazon Web Services 服务 所执行操作的服务。CloudTrail 将 Amazon Web Services 支持 Plans 的 API 调用作为事件捕获。捕获的调用包含来自 Amazon Web Services 支持 Plans 控制台和代码对 Amazon Web Services 支持 Plans API 操作的调用。

如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon Simple Storage Service（Amazon S3）存储桶（包括 Amazon Web Services 支持 Plans 事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的事件历史记录中查看最新事件。

使用 CloudTrail 收集的信息，您可以确定向 Amazon Web Services 支持 Plans 发出了什么请求、发出请求的 IP 地址、请求方、请求时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息（包括如何对其进行配置和启用），请参阅 Amazon CloudTrail 用户指南。

CloudTrail 中的 Amazon Web Services 支持 Plans 信息

在您创建 Amazon Web Services 账户时，将在该账户上启用 CloudTrail。当 Amazon Web Services 支持 Plans 中发生受支持的事件活动时，该活动将记录在 CloudTrail 事件中，并与其他 Amazon Web Services 服务 事件一同保存在 Event history（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 Amazon Web Services 支持 Plans 事件），请创建一个 trail（跟踪）。通过跟踪记录，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Amazon Web Services 区域。此跟踪记录在 Amazon 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）存储桶。此外，您可以配置其他 Amazon Web Services 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：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个账户接收 CloudTrail 日志文件

所有的 Amazon Web Services 支持 Plans API 操作均由 CloudTrail 记录。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 Amazon Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 Amazon Web Services 服务 发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

您也可以将多个 Amazon Web Services 区域 和多个账户的 Amazon Web Services 支持 Plans 日志文件聚合到单个 Amazon S3 存储桶中。

了解 Amazon Web Services 支持 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 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：GetSupportPlan 的日志条目

以下示例显示了 `GetSupportPlan` 操作的 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 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/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "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 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/7f03b7a233a0e87ebc79e56d4d2bcaf19e976c37
    },
    "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 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"
}
```

Example：ListSupportPlanModifiers 的日志条目

以下示例显示了 `ListSupportPlanModifiers` 操作的 CloudTrail 日志条目。

```
{
    "eventVersion": "1.09",
    "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:sts::111122223333:user/janedoe",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2024-08-15T15:44:43Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-08-15T16:29:59Z",
    "eventSource": "supportplans.amazonaws.com",
    "eventName": "ListSupportPlanModifiers",
    "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"
}
```


记录对您的 Amazon Web Services 支持 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 Amazon Web Services 支持 Plans 日志文件条目。

- `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

以下示例显示了用于 `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

以下示例显示了用于 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"
}
```

Amazon Trusted Advisor 的监控和日志记录

监控是保持 Trusted Advisor 和您的其他 Amazon 解决方案的可靠性、可用性和性能的重要方面。Amazon 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 提供近乎实时的系统事件流，这些系统事件描述了 Amazon 资源中的更改。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，并在这些事件发生时在其他 Amazon 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 Amazon 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，请参阅 Amazon EventBridge 用户指南。
- Amazon Trusted Advisor 检查可确定供您降低成本、改善性能和提高 Amazon 账户安全性的方法。您可以使用 EventBridge 来监控 Trusted Advisor 检查的状态。然后，您可以使用 Amazon CloudWatch 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。
- Amazon CloudTrail 捕获由您的 Amazon 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 Amazon S3 桶。您可以标识哪些用户和账户调用了 Amazon、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《Amazon CloudTrail 用户指南》。

主题

使用 Amazon 监控 Amazon Trusted Advisor 检查结果 EventBridge

您可以使用 EventBridge 来检测何时检查 Trusted Advisor 变更状态。然后，根据您创建的规则，当状态更改为您在规则中指定的值时， EventBridge 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 Amazon Lambda 函数将通知传递给 Slack 频道。

- 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。
- 获取 Amazon CloudWatch 警报操作的通知。

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 尽最大努力举办活动。并不总是能保证将事件传送到 EventBridge。
> -
> - 您必须有商业、企业入口或企业 Amazon Web Services 支持 计划才能创建 Trusted Advisor 检查规则。有关更多信息，请参阅 更改 Amazon Web Services 支持 计划。
> - 与全球服务一样 Trusted Advisor ，所有事件都发送到 EventBridge 美国东部（弗吉尼亚北部）地区。

按照以下步骤为创建 EventBridge 规则 Trusted Advisor。在创建事件规则之前，请执行以下操作：

- 熟悉中的事件、规则和目标。 EventBridge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。
- 创建将在事件规则中使用的目标。

要为创建 EventBridge 规则 Trusted Advisor

1. 打开 Amazon EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
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，选择规则。
4. 选择 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 事件总线和 规则类型，保留默认值，然后选择下一步。
7. 在构建事件模式页面上，为事件源选择Amazon 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（ Amazon Web Services 服务）。

9. 对于 Amazon Web Services 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。
      - 错误- Trusted Advisor 建议对检查采取行动。
      - 信息- Trusted Advisor 无法确定支票的状态。
      - OK — Trusted Advisor 未检测到支票存在问题。
      - 警告- Trusted Advisor 检测检查中可能存在的问题并建议进行调查。
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 Amazon 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 ARN 旁边的特定资源 ID，然后输入所需的亚马逊资源名称 (ARNs)。
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 创建规则。现在，您的规则将监控 Trusted Advisor 检查结果，然后将事件发送到您指定的目标。

创建 Amazon CloudWatch 告警以监控 Amazon Trusted Advisor 指标

Amazon Trusted Advisor 刷新您的检查时，Trusted Advisor 将有关您的检查结果的指标发布到 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）。

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

在为 Trusted Advisor 指标创建 CloudWatch 告警之前，审查以下信息：

- 了解 CloudWatch 如何使用指标和告警。有关更多信息，请参阅 Amazon CloudWatch 用户指南中的 CloudWatch 工作原理。
- 使用 Trusted Advisor 控制台或 Amazon Web Services 支持 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。

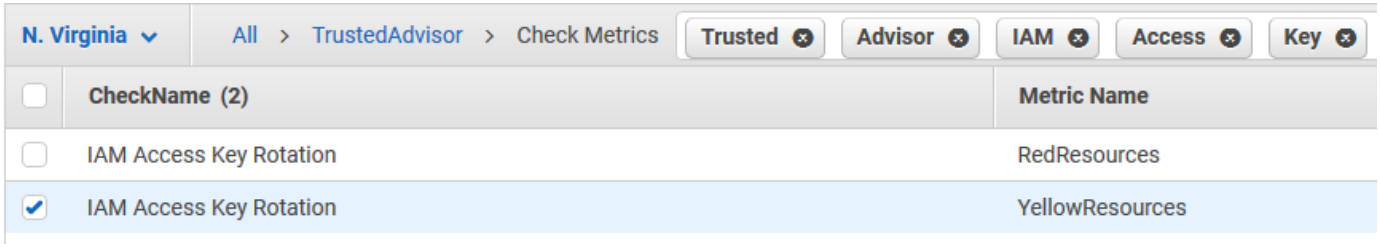
要为 Trusted Advisor 指标创建 CloudWatch 告警

1. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 使用区域选择器，然后选择美国东部（弗吉尼亚北部）Amazon 区域。
3. 在导航窗格中，选择告警。
4. 选择创建警报。
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。

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。

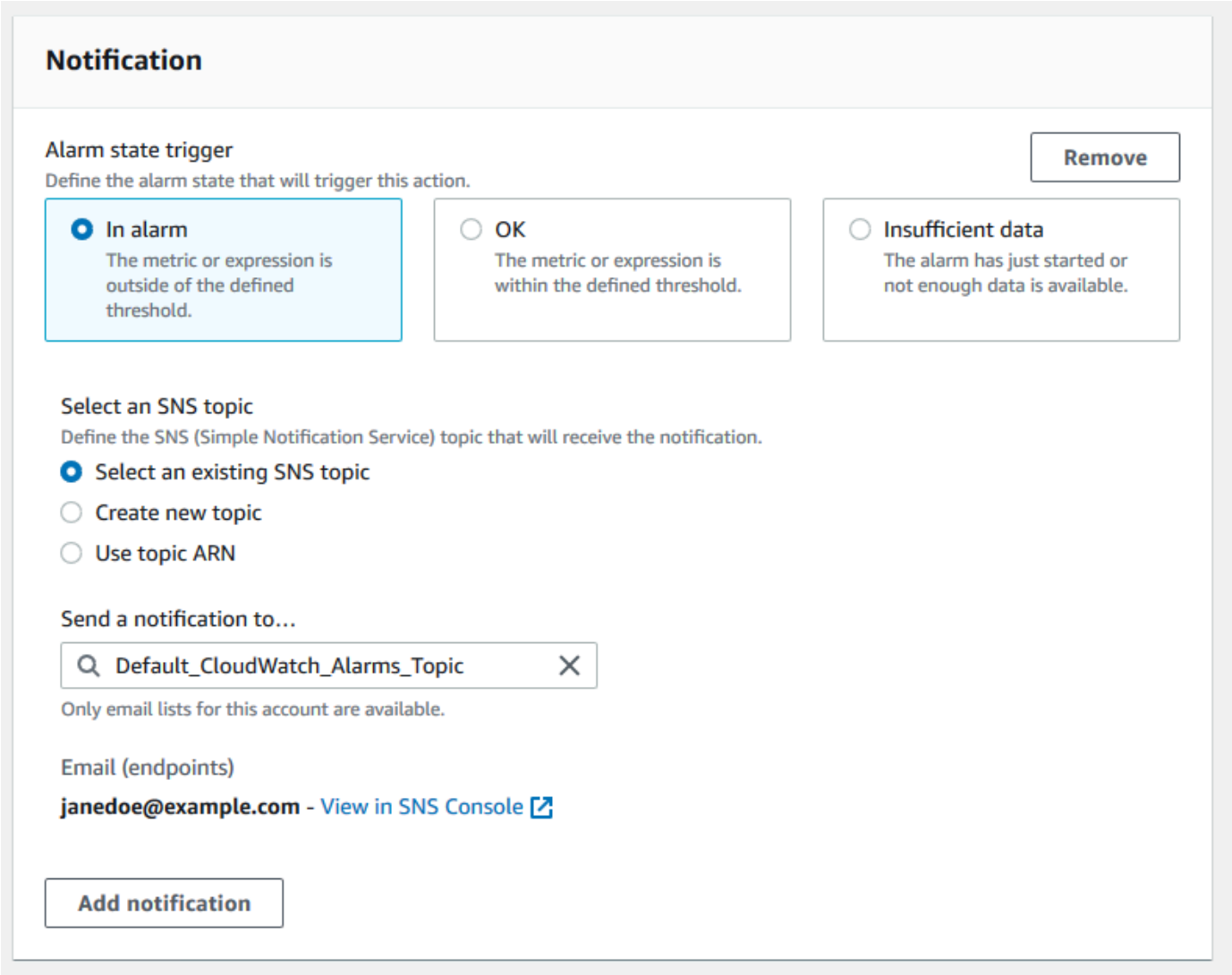


8. 选择选择指标。
9. 在 Specify metric and conditions（指定指标和条件）页面上，验证您选择的 Metric name（指标名称）和 CheckName（检查名称）显示在页面上。
10. 对于 Period（期限），您可以指定当检查状态变化时您希望告警开始的时间期限，如 5 分钟。
11. 在 Conditions（条件）下，选择 Static（静态），然后指定告警启动时的告警条件。

    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、YellowChecks、RedResources 和 YellowResources 指标，可以指定一个阈值，它可以是大于或等于零的任意整数。
> - Trusted Advisor 不会发送 GreenResources 的指标，它们为 Trusted Advisor 未检测到任何问题的资源。

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 CloudWatch 告警的电子邮件通知

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 Amazon Web Services #####:
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 Amazon access keys in
 my Amazon 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
- Amazon 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:
```

Trusted Advisor 的 CloudWatch 指标

您可以使用 CloudWatch 控制台或 Amazon Command Line Interface (Amazon CLI) 以查找可用于 Trusted Advisor 的指标。

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 Amazon 服务。

查看 Trusted Advisor 指标（控制台）

您可以登录 CloudWatch 控制台并查看 Trusted Advisor 的可用指标。

要查看可用的 Trusted Advisor 指标（控制台）

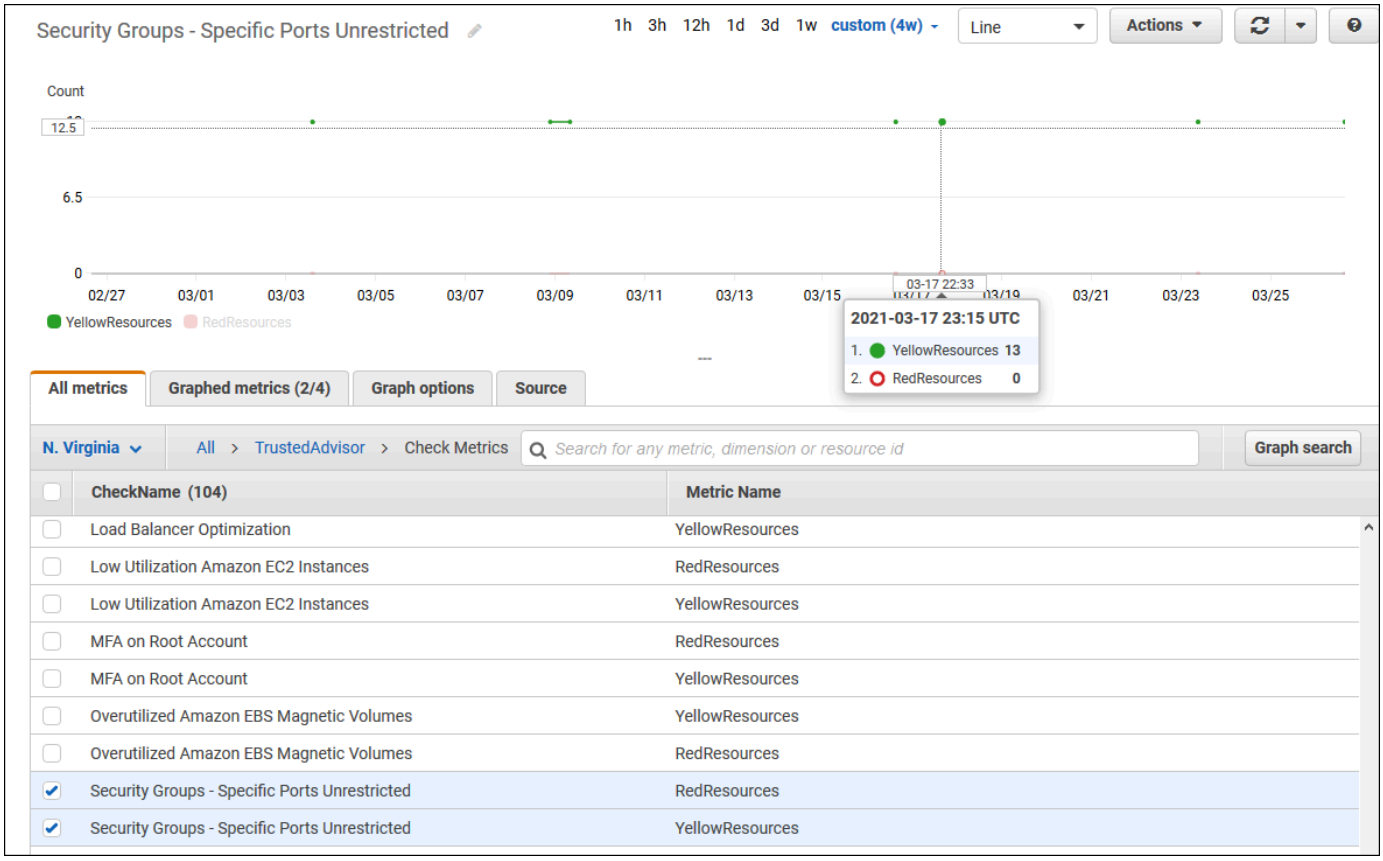
1. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 使用区域选择器，然后选择美国东部（弗吉尼亚北部） Amazon 区域。
3. 在导航窗格中，选择指标。
4. 输入指标命名空间，例如 **`TrustedAdvisor`**。
5. 选择指标维度，例如检查指标。
6. All metrics（所有指标）选项卡显示命名空间中该维度的指标。您可执行以下操作：

    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 Actions（操作），然后选择 Add to dashboard（添加到控制面板）。

   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 Amazon 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 Amazon 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 服务配额级指标

您可以使用以下有关 Amazon Web Services 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 Amazon Trusted Advisor 查看参考资料 中找到所有检查名称。

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	服务配额的 Amazon Web Services 区域。
ServiceName	Amazon Web Services 服务 的名称。
ServiceLimit	服务配额的名称。 有关服务配额的更多信息，请参阅 Amazon Web Services 一般参考 中 Amazon Web Services 服务 限额。

使用 Amazon CloudTrail 记录 Amazon Trusted Advisor 控制台操作

Trusted Advisor 与 Amazon CloudTrail 集成，后者是在 Amazon 中记录用户、角色或 Trusted Advisor 服务所执行操作的服务。CloudTrail 将 Trusted Advisor 的调用作为事件捕获。捕获的调用包括来自 Trusted Advisor 控制台的调用。如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon Simple Storage Service (Amazon S3) 存储桶（包括 Trusted Advisor 的事件）。如果您不配置跟踪记录，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。使用 CloudTrail 收集的信息，您可以确定向 Trusted Advisor 发出了什么请求、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。

要了解有关 CloudTrail 的更多信息（包括如何对其进行配置和启用），请参阅《Amazon CloudTrail 用户指南》。

Trusted AdvisorCloudTrail 中的 信息

在您创建 Amazon 账户时，将在该账户上启用 CloudTrail。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 CloudTrail 事件中，并与其他 Amazon 服务事件一同保存在 Event history（事件历史记录）中。您可以在 Amazon 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 Amazon 账户中的事件（包括 Trusted Advisor 的事件），请创建跟踪。通过跟踪记录，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 Amazon 区域。此跟踪记录在 Amazon 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 Amazon S3 存储桶。此外，您可以配置其他 Amazon 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：

- 创建跟踪概述
- 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：

- BatchUpdateRecommendationResourceExclusion
- CreateEngagement
- CreateEngagementAttachment
- CreateEngagementCommunication
- CreateExcelReport
- DescribeAccount
- DescribeAccountAccess
- DescribeCheckItems
- DescribeCheckRefreshStatuses
- DescribeCheckSummaries
- DescribeChecks
- DescribeNotificationPreferences
- DescribeOrganization

- DescribeOrganizationAccounts
- DescribeReports
- DescribeServiceMetadata
- ExcludeCheckItems
- GenerateReport
- GetEngagement
- GetEngagementAttachment
- GetEngagementType
- GetExcelReport
- GetOrganizationRecommendation
- GetRecommendation
- IncludeCheckItems
- ListAccountsForParent
- ListChecks
- ListEngagementCommunications
- ListEngagementTypes
- ListEngagements
- ListOrganizationRecommendationAccounts
- ListOrganizationRecommendationResources
- ListOrganizationRecommendations
- ListOrganizationalUnitsForParent
- ListRecommendationResources
- ListRecommendations
- ListRoots
- RefreshCheck
- SetAccountAccess
- SetOrganizationAccess
- UpdateEngagement
- UpdateEngagementStatus
- UpdateNotificationPreferences

- UpdateOrganizationRecommendationLifecycle
- UpdateRecommendationLifecycle

有关 Trusted Advisor 控制台操作的完整列表，请参阅 Trusted Advisor 行动。

> **Note**
>
> CloudTrail 还会记录 Amazon Web Services 支持 API 参考中的 Trusted Advisor API 操作。有关更多信息，请参阅。使用 Amazon CloudTrail 记录 Amazon Web Services 支持 API 调用

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 Amazon Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 Amazon 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

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记账条目。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：RefreshCheck 的日志条目

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 (ID R365s2Qddf) 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：UpdateNotificationPreferences 的日志条目

下面的示例显示了一个 CloudTrail 日志条目，该条目演示了 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：GenerateReport 的日志条目

下面的示例显示了一个 CloudTrail 日志条目，该条目演示了 GenerateReport 操作。此操作会为您的 Amazon 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

对于 Amazon EC2 Windows 实例，您可使用 EC2Rescue 检查实例，以帮助识别常见问题、收集日志文件，以及帮助 Amazon Web Services 支持 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 Amazon Web Services 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 Amazon Web Services 支持。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 Amazon 文档登录页面上的搜索文本框。

服务	链接
Amazon Web Services	排除 Amazon 签名版本 4 错误
Amazon API Gateway	HTTP API 故障排除
Amazon AppStream	Amazon AppStream 故障排除
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
Amazon Certificate Manager (ACM)	故障排查
Amazon CloudFormation	故障排除 Amazon CloudFormation

服务	链接
Amazon CloudFront	问题排查 | RTMP 分配问题排查
Amazon CloudHSM	故障排查
Amazon CloudSearch	Amazon CloudSearch 故障排除
Amazon CodeDeploy	故障排除 Amazon CodeDeploy
Amazon CloudWatch	故障排除 –
Amazon Database Migration Service	对 Amazon Database Migration Service 中的迁移任务进行故障排除
Amazon Data Pipeline	故障排查
Amazon Direct Connect	故障排除 Amazon Direct Connect
Amazon Directory Service	排查 Amazon Directory Service 管理问题
Amazon DynamoDB	故障排除 | 建立 SSL/TLS 连接故障排除
Amazon Elastic Beanstalk	故障排查
Amazon Elastic Compute Cloud（Amazon EC2）	实例故障排除 | Windows 实例故障排除 | VM Import/Export 故障排除 | API 请求错误排查
Amazon Elastic Container Service (Amazon ECS)	Amazon ECS 故障排除
Amazon Elastic Kubernetes Service(Amazon EKS)	Amazon EKS 故障排除
Elastic Load Balancing	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（Memcached）	对应用程序进行问题排查

服务	链接
Amazon ElastiCache（Redis OSS）	对应用程序进行问题排查
Amazon EMR	集群问题排查
Amazon Flow Framework	问题排查和调试提示
Amazon Glue	故障排除 Amazon Glue
Amazon Glue DataBrew	对 Amazon Glue DataBrew 中的身份和访问进行故障排除
Amazon GovCloud (US)	故障排查
Amazon Identity and Access Management（IAM）	IAM 故障排除
Amazon Keyspaces（Apache Cassandra 兼容）	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
适用于 Apache Flink 的亚马逊托管服务	性能故障排除 | 针对 SQL 应用程序的适用于 Apache Flink 的亚马逊托管服务进行故障排除
Amazon Data Firehose	Amazon Data Firehose 故障排除
Amazon Lambda	使用 CloudWatch 诊断和监控 Amazon Lambda 函数
Amazon OpenSearch Service	Amazon OpenSearch Service 故障排除
Amazon Personalize	故障排查
Amazon Quick Suite	Amazon Quick Suite 故障排除 | 跳过行错误故障排除
Amazon Resource Access Manager (Amazon RAM)	排查 Amazon RAM 的问题

服务	链接
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
Amazon SageMaker AI	排查错误 | Amazon SageMaker AI Studio 故障排除
Amazon Silk	故障排查
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 Amazon 流框架：问题排查和调试提示 | 适用于 Ruby 的 Amazon 流框架：问题排查和调试工作流程
Amazon Storage Gateway	排查网关问题
Amazon Systems Manager	SSM Agent 故障排除
Amazon Virtual Private Cloud（Amazon VPC）	故障排查
Amazon Virtual Private Network (Amazon VPN)	对客户网关设备进行故障排除
Amazon WAF	测试和调整您的 Amazon WAF 保护措施
Amazon WorkMail	Amazon WorkMail Web 应用程序故障排除
Amazon WorkSpaces	Amazon WorkSpaces 故障排除 | Amazon WorkSpaces 客户端故障排除

文档历史记录

下表描述了自该 Amazon Web Services 支持 服务上次发布以来对文档所做的重要更改。

- Amazon Web Services 支持 API 版本：2013-04-15
- Amazon Web Services 支持 应用程序 API 版本：2021-08-20

下表描述了从 2021 年 5 月 10 日起对 Amazon Web Services 支持 和 Amazon Trusted Advisor 文档进行的重要更新。您可以订阅 RSS 源来接收有关更新的通知。

变更	说明	日期
在通过支持互动创建支持案例中添加了 Enterprise Support 案例的最佳做法和目标响应时间	添加了一个新的下拉部分，详细介绍了 Enterprise Support 客户在创建案例时的最佳实践 Amazon Web Services 支持。有关更多信息，请参阅通过支持互动创建支持案例。	2026年1月12日
更新的变更 Amazon Web Services 支持 计划	添加了一份注释，详细说明了在注册了 B Amazon usiness Support+ 的组织中添加或删除账户后会发生什么。有关更多信息，请参阅变更 Amazon Web Services 支持 计划。	2026年1月8日
新章节设置权限以使用 AI 增强型故障排除	添加了一个新章节，概述了如何在 Service Catalog 中配置 AI 增强型故障排除所需的权限。有关更多信息，请参阅设置权限以使用 AI 增强型故障排除。	2025年12月22日
更新的 Trusted Advisor 支票参考	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 12 月 18 日

更新的 Trusted Advisor 支票参考	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025年12月17日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2025 年 12 月 8 日
添加了有关新 Amazon Web Services 支持 计划的信息	有关更多信息，请参阅Amazon Web Services 支持 计划。	2025 年 12 月 2 日
添加了有关 AI 增强型故障排除的信息	有关更多信息，请参阅 Support Center 控制台中的 AI 增强型疑难解答。	2025 年 12 月 2 日
添加了有关 Amazon 统一行动的新章节的信息	有关更多信息，请参阅什么是 Amazon 统一运营。	2025 年 12 月 2 日
添加了 Support Assistan APIs	在 “管理 Cent Amazon Web Services 支持 er” 访问权限 ResolveInteraction 中添加了 Su ListInteractions pport Assistant 的 Amazon Web Services 支持 API 操作：ListInteractionEntries、和。	2025 年 12 月 2 日
更新的 Trusted Advisor 支票参考	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 11 月 21 日
更新的 Trusted Advisor 支票参考	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 11 月 17 日

更新了编辑和删除的服务相关角色 Amazon Web Services 支持	已加入 Enterpris Amazon Organizations e Support 计划的客户可以删除AWSServiceRoleForSupport 服务相关角色。有关更多信息，请参阅为 Amazon Web Services 支持编辑和删除服务关联角色。	2025 年 10 月 31 日
更新的 Trusted Advisor 支票参考	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 10 月 15 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2025 年 9 月 30 日
新主题	新增了一个新主题，包含有关如何启用促销计划到期通知的信息。有关更多信息，请参阅配置促销计划到期通知。	2025 年 9 月 12 日
更新的 Trusted Advisor 支票	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 9 月 11 日
更新了测试支持中心控制台 API 调用	更新了步骤 3，指明正确的事件源为 support-console.amazonaws.com。有关更多信息，请参阅测试支持中心控制台 API 调用。	2025 年 9 月 2 日
更新了更改 Amazon Web Services 支持 计划	升级或降级 Amazon Web Services 支持 订阅的步骤已更新。有关更多信息，请参阅更改 Amazon Web Services 支持计划。	2025 年 8 月 27 日

更新的 Trusted Advisor 支票	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 8 月 19 日
移除了 “ Trusted Advisor 参与” 部分	移除了 “开始使用 Eng Amazon Trusted Advisor age（预览）” 部分。	2025 年 8 月 7 日
更新了如何将 Amazon Web Services 支持 应用程序添加到 Slack 频道	有关详细信息，请参阅配置 Slack 频道。	2025 年 8 月 6 日
更新了托管策略：AWSSupportAccess	有关详细信息，请参阅Amazon 托管策略的Amazon Web Services 支持 更新。	2025 年 7 月 18 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2025 年 7 月 15 日
更新了检查：Ubuntu LTS 终止标准支持的亚马逊 EC2 实例	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 7 月 3 日
更新的 Trusted Advisor 支票：Amazon S3 存储桶权限	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 7 月 3 日
更新了检查：根账户的 MFA	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 7 月 2 日
更新的检查：Amazon ECS Amazon日志驱动程序处于屏蔽模式。	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 7 月 2 日

更新了请求增加服务配额	添加了有关在 Service Quotas Amazon Web Services 服务 控制台 Amazon Web Services 区域 不支持的情况下如何创建服务配额增加请求的信息。有关更多信息，请参阅请求增加服务配额。	2025 年 7 月 2 日
不再支持在支持中心控制台中创建服务配额增加请求。	有关更多信息，请参阅创建服务配额增加请求。	2025 年 6 月 23 日
在 Amazon Web Services 支持 API UpdateInteraction 中添加了描述	在 “管理 Amazon Web Services 支持 中心访问权限” 中添加了 Amazon Amazon Web Services 支持 API UpdateInteraction 操作描述。	2025 年 6 月 23 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2025 年 6 月 17 日
新部分：关于支持中心控制台 API	支持中心控制台 API 可增强您使用支持中心控制台的体验。有关详细信息，请参阅关于支持中心控制台 API。	2025 年 6 月 16 日
更新了 Amazon Trusted Advisor 章节简介，以反映 Basic 和 Developer Support 计划不支持自动支票刷新。您必须手动刷新安全检查才能查看最新的检查状态。	有关更多信息，请参阅 Amazon Trusted Advisor。	2025 年 6 月 11 日

更新的检查：现在所有 Amazon Web Services 支持 套餐级别 Amazon Web Services 区域 均提供 Amazon STS 全球终端节点使用情况。	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 6 月 9 日
新检查：针对数据库集群存储的 Amazon Aurora 成本优化建议	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 6 月 9 日
新检查： Amazon STS 全球终端节点的使用情况 Amazon Web Services 区域	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 6 月 2 日
新增 15 Amazon 成本优化中心张支票 Trusted Advisor	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 5 月 30 日
更新了三张 Trusted Advisor 支票	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 5 月 21 日
新功能：更新支持案例的严重性	有关详细信息，请参阅创建支持案例和案例管理中的更改支持案例严重性级别部分。	2025 年 5 月 21 日
更新了您可以查看 Amazon Web Services 支持 案例详情的时间。	有关详细信息，请参阅您的 Amazon Web Services 支持 案例的安全性。	2025 年 4 月 29 日
更新了两张 Trusted Advisor 支票	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 4 月 2 日

添加了 Amazon Web Services 支持 API 的描述	在 “管理 Amazon Web Services 支持 中心访问权限” 中添加了 Amazon Amazon Web Services 支持 API 操作描述。	2025 年 3 月 7 日
已弃用 6 张支票 Amazon Security Hub CSPM	有关详细信息，请参阅Amazon Trusted Advisor 检查变更日志。	2025 年 3 月 5 日
删除了对类别级别指标的引用 Trusted Advisor	的类别级别指标已弃 Trusted Advisor 用。已从 “创建用于监控指标的 Amazon CloudWatch 警报” 中删除了对类别级别指标的引用。 Amazon Trusted Advisor	2025 年 1 月 27 日
更新了的文档 Trusted Advisor	增加了两项新检查： Amazon CloudTrail 管理事件记录和未启用 Amazon RDS 连续备份。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 12 月 23 日
更新了的文档 Trusted Advisor	更新了自动扩缩组资源。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 12 月 23 日
更新了的文档 Trusted Advisor	更新了 IAM Access Analyzer 外部访问权限检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 12 月 23 日

更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2024 年 11 月 25 日
更新了的文档 Trusted Advisor	添加了 1 张新 Trusted Advisor 支票。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 11 月 22 日
添加了 Amazon Partner-Led Support 的 Amazon 托管政策文档	添加了有关新 Amazon 托管策略的文档AWSPartnerLedSupportReadOnlyAccess 。有关更多信息，请参阅 Amazon Partner-Led Support 的Amazon 托管政策。	2024 年 11 月 22 日
更新了的文档 Trusted Advisor	更新了 3 张 Trusted Advisor 支票。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 11 月 7 日
更新了 Amazon Web Services 支持 计划文档	在 Logging Plans API 调用 Amazon CloudTrail页面中添加了该ListSupportPlanModifiers 操作的新日志 Amazon Web Services 支持示例。	2024 年 11 月 6 日

更新了 AWSTrustedAdvisorServiceRolePolicy 的文档	新增了 IAM 操作 elasticloadbalancing:DescribeListeners 和 elasticloadbalancing:DescribeRules ，以加入新的安全检查。有关更多信息，请参阅 Amazon 托管策略：AWSTrustedAdvisorServiceRolePolicy。	2024 年 10 月 30 日
更新了的文档 Trusted Advisor	添加了 4 张新 Trusted Advisor 支票。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 10 月 11 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2024 年 10 月 8 日
更新了的文档 Trusted Advisor	将 1 项成本优化检查移动至“容错能力”支柱下。更新了 1 项安全检查和 1 项容错能力检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 10 月 2 日
更新了 “ Amazon Trusted Advisor 参与” 部分	更新了 “ Amazon Trusted Advisor 参与” 部分以引用 “ Amazon 倒计时”。有关更多信息，请参阅 Eng Amazon Trusted Advisor age 入门（预览）。	2024 年 9 月 16 日

更新了 Amazon Web Services 支持 计划文档	添加了用于查看支持计划修改器列表的新权限和 CloudTrail 文档。有关更多信息，请参阅管理 Amazon Web Services 支持 计划的访问权限、计划的Amazon托管策略和日志 Amazon Web Services 支持 计划 API 调用 Amazon CloudTrail。 Amazon Web Services 支持	2024 年 9 月 9 日
更新了的文档 Trusted Advisor	Trusted Advisor 8 月 23 日新增了 9 张支票。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 8 月 23 日
更新了的文档 Trusted Advisor	更新了 1 Trusted Advisor 项卓越运营检查并添加了 1 项新的 Trusted Advisor 安全检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 8 月 22 日
更新了的文档 Trusted Advisor	更新了 6 Trusted Advisor 项安全检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 8 月 20 日
更新了的文档 Trusted Advisor	更新了 2 张 Trusted Advisor 支票。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 8 月 12 日

更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2024 年 8 月 5 日
更新了的文档 Trusted Advisor	更新了 9 张 Trusted Advisor 支票。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 7 月 21 日

更新了 AWSTrustedAdvisorServiceRolePolicy 的文档	新增了 IAM 操作 access-analyzer:ListAnalyzers 、cloudwatch:ListMetrics 、dax:DescribeClusters 、ec2:DescribeNatGateways 、ec2:DescribeRouteTables 、ec2:DescribeVpcEndpoints 、ec2:GetManagedPrefixListEntries 、elasticloadbalancing:DescribeTargetHealth 、iam:ListSAMLProviders 、kafka:DescribeClusterV2 network-firewall:ListFirewalls network-firewall:DescribeFirewall 和 sqs:GetQueueAttributes ，以加入新检查。有关更多信息，请参阅 Amazon 托管策略：AWSTrustedAdvisorServiceRolePolicy。	2024 年 6 月 11 日
从文档中删除了 5 个 Amazon Trusted Advisor 支票	移除了 5 个现已弃用的 Amazon Trusted Advisor 检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 5 月 15 日

在文档中添加了 1 项新的 Amazon Trusted Advisor 安全检查	在文档中添加了 1 项新的 Amazon Trusted Advisor 安全检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 5 月 15 日
从文档中移除了 3 项容错能力检查	移除了现已弃用的 3 项容错能力检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 4 月 25 日
更新了容错能力检查和安全检查文档	新增了 1 项容错能力检查。更新了 1 项容错能力检查和 1 项安全检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 3 月 29 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2024 年 3 月 22 日
更新了 Amazon Web Services 支持 计划文档	Amazon Web Services 支持 计划功能的更新。有关更多信息，请参阅 Amazon Web Services 支持 计划。	2024 年 3 月 11 日
更新了的文档 Trusted Advisor	新增了 1 项容错能力检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 2 月 29 日
更新了的文档 Trusted Advisor	新增了 1 项容错能力检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 1 月 31 日

更新了 AWSTrustedAdvisorServiceRolePolicy 的文档	新增了 IAM 操作 cloudtrail:GetTrail 、cloudtrail:ListTrails 、cloudtrail:GetEventSelectors 、outposts:GetOutpost 、outposts:ListAssets 和 outposts:ListOutposts ，以加入新检查。有关更多信息，请参阅 Amazon 托管策略：AWSTrustedAdvisorServiceRolePolicy。	2024 年 1 月 18 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2024 年 1 月 17 日
更新了的文档 Trusted Advisor	更新了 1 项容错能力检查以修改标题和描述。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2024 年 1 月 8 日
更新了的文档 Trusted Advisor	更新了 1 项安全检查，以反映弃用期限的变化。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2023 年 12 月 21 日
更新了的文档 Trusted Advisor	新增了 2 项安全检查和 2 项性能检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2023 年 12 月 20 日

更新了的文档 Trusted Advisor	新增了 1 项安全检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2023 年 12 月 15 日
更新了 Eng Trusted Advisor age 的文档	更新了 Eng Trusted Advisor age 文档，更改了电子邮件通知选项。	2023 年 12 月 14 日
更新了 Eng Trusted Advisor age 的文档	更新了 Trusted Advisor Engage 文档，对预定互动进行了更改。	2023 年 12 月 11 日
更新了的文档 Trusted Advisor	新增了 2 项容错能力检查和 1 项成本优化检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2023 年 12 月 7 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2023 年 12 月 6 日
更新了的 Amazon 托管策略 Trusted Advisor	更新了AWSTrustedAdvisorPriorityFullAccess 和AWSTrustedAdvisorPriorityReadOnlyAccess Amazon 托管策略以包含声明 IDs。有关更多信息，请参阅适用于Amazon Trusted Advisor的Amazon 托管策略。	2023 年 12 月 6 日
更新了的文档 Trusted Advisor	新增了 3 项容错能力检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2023 年 11 月 17 日

更新了的文档 Trusted Advisor	新增了 37 项适用于 Amazon RDS 的新检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2023 年 11 月 15 日
更新了 AWSTrustedAdvisorServiceRolePolicy 的文档	新增了 IAM 操作 ec2:DescribeRegions 、s3:GetLifecycleConfiguration 、ecs:DescribeTaskDefinition 和 ecs:ListTaskDefinitions ，以加入新检查。有关更多信息，请参阅 Amazon 托管策略：AWSTrustedAdvisorServiceRolePolicy。	2023 年 11 月 9 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2023 年 10 月 27 日
更新了的文档 Trusted Advisor	添加了从中集成的 64 张新支票 Amazon Config。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2023 年 10 月 26 日
更新了的文档 Trusted Advisor	添加了六个新的容错检查 Trusted Advisor。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2023 年 10 月 12 日

更新了 AWSTrustedAdvisorServiceRolePolicy 的文档	将新 IAM 操作 route53resolver:ListResolverEndpoints 、route53resolver:ListResolverEndpointIpAddresses 、ec2:DescribeSubnets 、kafka:ListClustersV2 和 kafka:ListNodes 添加到新加入的恢复能力检查。有关更多信息，请参阅 Amazon 托管策略：AWSTrustedAdvisorServiceRolePolicy。	2023 年 9 月 14 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2023 年 8 月 28 日
更新了的文档 Trusted Advisor	添加了 1 项新的服务限制检查 Amazon Lambda。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2023 年 8 月 17 日
更新了的文档 Trusted Advisor	新增了一项 Lambda 的容错能力检查。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2023 年 8 月 3 日
更新了 Eng Trusted Advisorage 的文档	更新了 Eng Trusted Advisorage 文档，更改了用于创建和编辑互动的表单。添加了包含示例服务控制策略的页面 Amazon Trusted Advisor。	2023 年 7 月 27 日

更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2023 年 6 月 26 日
更新了的文档 Trusted Advisor	新增了两项 Amazon MQ 的容错能力检查。为 Amazon Elastic File System 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Amazon Trusted Advisor 检查变更日志。	2023 年 6 月 1 日
更新了的文档 Trusted Advisor	新增了两项 NAT 网关的容错能力检查。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2023 年 5 月 16 日
更新了 Amazon Web Services 支持 计划文档	添加了用于创建支持计划时间表的新权限和 CloudTrail 文档。有关更多信息，请参阅管理 Amazon Web Services 支持 计划的访问权限、计划的Amazon托管策略和日志 Amazon Web Services 支持 计划 API 调用 Amazon CloudTrail。 Amazon Web Services 支持	2023 年 5 月 8 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2023 年 5 月 2 日

更新了 “ Trusted Advisor 参与度” 和 “ Trusted Advisor 优先级” 文档	阐明了 “ Trusted Advisor 参与” 和 “ Trusted Advisor 优先级” 的前提条件。增加了能够使用 Trusted Advisor Engage 和启用对 Trusted Advisor可信访问权限的示例 IAM policy。	2023 年 4 月 28 日
更新了的文档 Trusted Advisor	为 Amazon Resilience Hub 和事件管理器添加了两个新的容错检查。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2023 年 4 月 27 日
为 Eng Trusted Advisor age 添加了文档	您可以使用 Eng Amazon Trusted Advisor age，让您可以轻松查看、请求和跟踪所有主动互动，并与 Amazon Web Services 账户 团队就正在进行的互动进行沟通，从而充分利用您的 Amazon Web Services 支持 计划。有关更多信息，请参阅 Eng Amazon Trusted Advisor age 入门。	2023 年 4 月 6 日
更新了的文档 Trusted Advisor	新增了两项 Amazon ECS 的容错能力检查。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2023 年 3 月 30 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2023 年 3 月 16 日

为 Trusted Advisor 优先级添加了文档	更新了 P Trusted Advisor riority 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 优先级入门。	2023 年 2 月 16 日
更新了的代码示例 Amazon Web Services 支持	添加了.NET、Java 和 Kotlin 代码示例，这些示例展示了如何 Amazon Web Services 支持 使用 Amazon 软件开发套件 (SDK)。有关更多信息，请参阅Amazon Web Services 支持 使用代码示例 Amazon SDKs。	2023 年 1 月 16 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2023 年 1 月 10 日
更新了 Amazon Web Services 支持 App 的文档	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 Amazon Web Services 支持 App 的文档	你也可以使用 Terraform 为应用程序创建资源。 Amazon Web Services 支持 有关更多信息，请参阅使用 Terraform 创建 Amazon Web Services 支持 应用程序资源。	2022 年 12 月 22 日
更新了的文档 Trusted Advisor	为 M Amazon emoryDB ElastiCache、Amazon 和 添加了三项新的容错检查。 Amazon CloudHSM有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2022 年 12 月 15 日
更新了 Slack 中 Amazon Web Services 支持 应用程序的文档	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 频道中创建支持案例。	2022 年 12 月 14 日
更新了的文档 Amazon Web Services 支持	添加了有关 Amazon Web Services 支持 API 新端点的文档。有关更多信息，请参阅关于 Amazon Web Services 支持 API。	2022 年 12 月 14 日
添加了在 Slack 中用于 Amazon Web Services 支持 应用程序的 Amazon CloudFormation 模板的文档	您可以使用 CloudFormation 模板来创建 Slack 配置工作空间和频道。 Amazon Web Services 账户 Amazon Organizations有关更多信息，请参阅使用创建 Amazon Web Services 支持 应用程序资源 Amazon CloudFormation。	2022 年 12 月 5 日

更新了的文档 Trusted Advisor	为添加了两个新的容错检查 Amazon Resilience Hub。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2022 年 11 月 17 日
在中为你的 Amazon Security Hub CSPM 发现添加了文档 Trusted Advisor	你从 Security Hub CSPM 控件中发现的结果会被更快地删除 Trusted Advisor 。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2022 年 11 月 17 日
更新了的文档 Amazon Trusted Advisor	添加了 “ Trusted Advisor 推荐” 文档。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2022 年 11 月 16 日
更新了 Slack 中 Amazon Web Services 支持 应用程序的文档	新增了日语支持文档。有关更多信息，请参阅在 Slack 频道中创建支持案例。	2022 年 11 月 11 日
更新了 Amazon Web Services 支持 计划文档	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 Amazon Web Services 支持 应用程序的文档	添加了 `supportapp` 权限的文档。有关更多信息，请参阅Amazon Web Services 支持 应用程序连接到 Slack 所需的权限。	2022 年 11 月 1 日

更新了 Slack 中 Amazon Web Services 支持 应用程序的文档	您可以使用 `RegisterSlackWorkspaceForOrganization` API 操作为您的 Amazon Web Services 账户注册 Slack 工作区。要调用此 API，您的账户必须是 Amazon Organizations中的组织的一部分。有关更多信息，请参阅 Slack API 中的Amazon Web Services 支持 App 参考。	2022 年 10 月 19 日
更新了 `AWSSupportServiceRolePolicy` 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2022 年 10 月 4 日
更新了 Support Plans 文档	现在，您可以使用 Amazon Identity and Access Management (IAM) 来管理权限，以更改您的支持计划 Amazon Web Services 账户。有关更多信息，请参阅以下主题： • 管理 Amazon Web Services 支持 套餐的访问权限 • AmazonAmazon Web Services 支持 套餐的托管策略 • 更改 Amazon Web Services 支持 计划 • 日志 Amazon Web Services 支持 计划 API 调用时使用 Amazon CloudTrail	2022 年 9 月 29 日

更新了 Slack 中 Amazon Web Services 支持 应用程序的文档	添加了有关如何配置用于 Amazon Web Services 支持 应用程序的公共或私人频道的文档。有关更多信息，请参阅 Configuring a Slack channel（配置 Slack 频道）。	2022 年 9 月 22 日
更新了的文档 Amazon Web Services 支持	新增了有关您的支持案例安全性的新章节。有关更多信息，请参阅您的 Amazon Web Services 支持 案例的安全性。	2022 年 9 月 9 日
更新了的文档 Trusted Advisor	为 Amazon 添加了新的安全检查 EC2。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2022 年 9 月 1 日

更新了 Slack 中 Amazon Web Services 支持 应用程序的文档	请参阅以下主题： 您可以使用该 Amazon Web Services 支持 应用程序来管理您的支持案例，请求增加服务配额，并直接在您的 Slack 频道中与支持代理聊天。有关更多信息，请参阅 Slack 中的 Amazon Web Services 支持 App 文档。 您可以将 Amazon Web Services 托管策略附加到您的 IAM 角色以使用该 Amazon Web Services 支持 应用程序。有关更多信息，请参阅 Slack 中 Amazon Web Services 支持 应用程序的Amazon Web Services 托管策略。 该 Amazon Web Services 支持 应用程序的新 API 参考资料。请参阅 Amazon Web Services 支持 App API 参考。	2022 年 8 月 24 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2022 年 8 月 17 日

为 Trusted Advisor 优先级添加了文档	Trusted Advisor 优先级增加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 • Amazon Web Services 托管策略 有关更多信息，请参阅Trusted Advisor 优先级入门。	2022 年 8 月 17 日
更新了的文档 Trusted Advisor	Trusted Advisor 控制台中的“首选项” 页面已更新。有关更多信息，请参阅入门 Amazon Trusted Advisor。	2022 年 7 月 15 日
更新了的文档 Trusted Advisor	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 Amazon Trusted Advisor 检查参考。	2022 年 7 月 7 日
更新了的文档 Amazon Web Services 支持	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 • 故障排查	2022 年 6 月 28 日

更新了 AWSSupportServiceRolePolicy 的文档	更新了为服务关联角色提供账单、管理和支持服务的权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2022 年 6 月 23 日
更新了的文档 Trusted Advisor	Trusted Advisor 支持来自 Amazon Security Hub CSPM 的其他 Amazon 基础安全最佳实践安全标准控件。有关更多信息，请参阅Amazon Trusted Advisor 检查变更日志。	2022 年 6 月 23 日
更新了的文档 Trusted Advisor	添加了有关如何请求增加服务配额的更多信息。有关更多信息，请参阅服务限制。	2022 年 6 月 21 日
更新了的文档 Amazon Web Services 支持	Support 中心控制台中的工单创建体验已经更新。有关更多信息，请参阅创建支持案例和工单管理。	2022 年 5 月 18 日
更新了的文档 Trusted Advisor	增加了适用于 Amazon EBS 和 Amazon Lambda的四项检查。有关更多信息，请参阅选择加入 Amazon Compute Optimizer 以添加 Trusted Advisor 支票。	2022 年 5 月 4 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 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	此检查现在将自动为您刷新。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2022 年 4 月 25 日
更新了的文档 Trusted Advisor	容错类别中的 Amazon Direct Connect 检查已更新。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2022 年 3 月 29 日
更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2022 年 3 月 14 日
为 Trusted Advisor 优先级添加了文档	您可以使用 Pri Trusted Advisor ority 查看技术客户经理 (TAM) 提供的按优先顺序排列的建议列表。有关更多信息，请参阅Trusted Advisor 优先级入门。	2022 年 2 月 28 日
更新了有关使用 Amazon EventBridge 的文档 Trusted Advisor	您可以创建 EventBridge 规则来监控 Trusted Advisor 支票的变化。有关更多信息，请参阅使用监控 Amazon Trusted Advisor 检查结果 EventBridge。	2022 年 2 月 21 日
有关使用 Amazon EventBridge 监控 Amazon Web Services 支持 案例的新文档	您可以创建 EventBridge 规则来监控和接收有关您的支持案例的通知。有关更多信息，请参阅使用监控 Amazon Web Services 支持 案例 EventBridge。	2022 年 2 月 21 日

更新了 AWSSupportServiceRolePolicy 的文档	增加了为服务关联角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。	2022 年 2 月 17 日
添加了与集成的文档 Amazon Security Hub CSPM	在 Trusted Advisor 控制台中，您现在可以查看作为 Amazon 基础安全最佳实践安全标准一部分的 Security Hub CSPM 控件的调查结果。有关更多信息，请参阅在 Amazon Security Hub CSPM 控制 Amazon Trusted Advisor 台中查看控件。	2022 年 1 月 18 日
已更新的文档	如果您有 E nterprise On-Ramp Support 计划，则可以访问所有 Trusted Advisor 支票和 Amazon Web Services 支持 API。	2021 年 11 月 24 日
更新了的文档 Trusted Advisor	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 Amazon Trusted Advisor 检查日志。	2021 年 9 月 8 日
更新了支 Trusted Advisor 票文档	为所有 Trusted Advisor 检查添加了参考主题。有关更多信息，请参阅 Amazon Trusted Advisor 检查参考。	2021 年 9 月 1 日

更新了 Trusted Advisor 托管策略的文档	更新了 Trusted Advisor 托管策略的文档。有关更多信息，请参阅Amazon Web Services 支持 和的Amazon 托管策略 Amazon Trusted Advisor。	2021 年 8 月 10 日
更新了的文档 Trusted Advisor	更新了 Trusted Advisor 控制台的文档。有关更多信息，请参阅入门 Amazon Trusted Advisor。	2021 年 7 月 16 日
更新了创建 Amazon Web Services 支持 案例的文档	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
更新了的文档 Trusted Advisor	Trusted Advisor 为亚马逊 Elastic Block Store (Amazon EBS) 卷存储添加了两张新支票。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查日志。	2021 年 6 月 8 日
已更新的文档	更新了以下主题： • 更新了程序，并在 “创建 Amazon CloudWatch 警报以监控 Amazon Trusted Advisor 指标” 主题中添加了内容 • 添加了 Amazon Web Services 支持 API 部分的服务配额	2021 年 5 月 12 日

早期更新

更改	描述	日期
更新了的文档 Trusted Advisor	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 • 刷新检查结果 • 下载检查结果	2021 年 3 月 16 日
更新了有关 Amazon 托管策略的文档	添加了有关`AWSSupportServiceRolePolicy` Amazon 托管策略的信息。有关更多信息，请参阅 将服务关联角色用于 Amazon Web Services 支持。	2021 年 3 月 16 日
添加了支票 Amazon Lambda	在中添加了四项 Amazon Trusted Advisor 对 Lambda 的检查。更改日志 Amazon Trusted Advisor	2021 年 3 月 8 日
更新了 Amazon Elastic Block Store 的服务限制检查	更新了中针对亚马逊 EBS 的五张 Amazon Trusted Advisor 支票。更改日志 Amazon Trusted Advisor	2021 年 3 月 5 日
更新了 CloudTrail 日志记录文档	CloudTrail 支持在更改 Amazon Web Services 支持 计划时记录控制台操作。有关更多信息，请参阅 记录对您的 Amazon Web Services 支持 计划的更改。	2021 年 2 月 9 日
更新了的文档 Trusted Advisor	更新了 开始使用 Trusted Advisor 建议 主题。	2021 年 1 月 29 日
更新了 Trusted Advisor 报告文档	添加了有关在其他 Amazon 服务中使用 Trusted Advisor 报告的问题排查部分。	2020 年 12 月 4 日
增加了对 Amazon CloudTrail 日志记录	CloudTrail 支持记录 Trusted Advisor 控制台操作的子集。有关更多信息，请参阅 使用	2020 年 11 月 23 日

更改	描述	日期
的 Amazon Trusted Advisor 支持	Amazon CloudTrail 记录 Amazon Trusted Advisor 控制台操作。	
增加了更改日志主题	在中查看 Amazon Trusted Advisor 支票和类别的更改更改日志 Amazon Trusted Advisor。	2020 年 11 月 18 日
增加了对组织单位的支持	现在，您可以为组织单位的 Trusted Advisor 支票创建报告（OUs）。有关更多信息，请参阅创建组织视图报告。	2020 年 11 月 17 日
使用 Amazon CloudTrail 主题更新了日志记录	为 Trusted Advisor API 操作添加了示例日志条目。请参阅Amazon Trusted AdvisorCloudTrail 日志记录中的 信息。	2020 年 10 月 22 日
增加了 Amazon Web Services 支持 配额	增加了有关 Amazon Web Services 支持的当前配额和限制的信息。请参阅 Amazon Web Services 一般参考 中的 Amazon Web Services 支持 端点和限额。	2020 年 8 月 4 日
的组织视图 Amazon Trusted Advisor	现在，您可以为属于其中的账户的 Trusted Advisor 支票创建报告 Amazon Organizations。请参阅的组织视图 Amazon Trusted Advisor。	2020 年 7 月 17 日
安全和 Amazon Web Services 支持	更新了有关使用 Amazon Web Services 支持 和 Trusted Advisor时的安全注意事项的信息。请参阅 安全性 Amazon Web Services 支持	2020 年 5 月 5 日
安全和 Amazon Web Services 支持	添加了有关使用 Amazon Web Services 支持时的安全注意事项的信息。	2020 年 1 月 10 日
用 Trusted Advisor 作 Web 服务	添加了更新的说明，以便在获取 Trusted Advisor 支票列表后刷新 Trusted Advisor 数据。	2018 年 11 月 1 日
使用服务关联角色	增加了新部分。	2018 年 7 月 11 日
入门：问题排查	增加了 Route 53 和 Amazon Certificate Manager的问题排查链接。	2017 年 9 月 1 日

更改	描述	日期
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
使用记录 Amazon Web Services 支持 通话 Amazon CloudTrail	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 Amazon Web Services 管理控制台中的服务目录。	2014 年 10 月 30 日
对 Amazon Web Services 支持 案件的生命周期进行编程	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
正在访问 Amazon Web Services 支持	删除了指定支持联系人的访问方式。	2014 年 5 月 28 日
开始使用	增加了“入门”章节。	2013 年 12 月 13 日
初次发布	新 Amazon Web Services 支持 服务已发布。	2013 年 4 月 30 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。