# Amazon Web Services Support

## 用户指南

API 版本 2013-04-15

# Amazon Web Services Support: 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。

# Table of Contents

# Amazon Web Services Support 入门

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

注意

- 有关不同 Amazon Web Services Support 计划的更多信息，请参阅比较 Amazon Web Services Support 计划。
- 要在 Amazon Web Services Management Console 中创建支持案例，请参阅 创建支持案例 (p. 3)。

主题



# Amazon Web Services Support 计划的功能

Amazon Web Services Support 提供五种 Support 计划：

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

基本支持计划提供对账户和账单问题以及提升服务配额的支持。其他计划均提供很多技术支持案例，其定价为按月支付形式，且无需长期合同。

所有 Amazon 客户自动获得对以下“基本”支持计划功能的全天候访问权限：

- 对账户和账单问题的一对一响应
- 支持论坛
- 服务运行状况检查

- 文档、技术论文和最佳实践指南

“开发人员”支持计划客户可以访问以下额外功能：

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

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

- 使用案例指导 – 使用哪些 Amazon 产品、功能和服务最符合您的具体需要。
- Amazon Trusted Advisor (p. 29) – 一种 Amazon Web Services Support 功能，它会检查客户环境，找出可节省开支、弥补安全漏洞并提高系统可靠性和性能的机会。您可以访问所有 Trusted Advisor 检查。
- 与支持中心和 Trusted Advisor 交互的 Amazon Web Services Support API。您可以使用 Amazon Web Services Support API 自动执行支持案例管理和 Trusted Advisor 操作。
- 第三方软件支持 – 针对 Amazon Elastic Compute Cloud (Amazon EC2) 实例操作系统和配置提供帮助。此外，还针对 Amazon 上常用的第三方软件组件的性能问题提供帮助。对于使用基本或开发人员支持计划的客户，不提供第三方软件支持。
- 支持无限数量的 Amazon Identity and Access Management (IAM) 用户，他们可以打开技术支持案例。

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

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

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

# 创建支持案例和案例管理

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

- 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 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。

  Note

  - 如果您拥有“基本”支持计划，则无法创建技术支持案例。
  - 要更改您的支持计划，请参阅 更改您的 Amazon Web Services Support 计划 (p. 16)。

- 要关闭账户，请参阅 Amazon Billing 用户指南中的关闭账户。

# 创建支持案例

您可以在 Amazon Web Services Management Console 的支持中心创建支持案例。

注意

- 您可以以 Amazon 账户的根用户身份或 Amazon Identity and Access Management (IAM) 用户身份登录支持中心。有关更多信息，请参阅Amazon Web Services Support 的访问权限 (p. 14)。
- 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 Amazon Web Services Management Console中，您还可以选择问号图标（  ），然后选择 Support Center（Support 中心）。
2. 选择 Create case（创建案例）。
3. 请选择以下任一选项：
   - Account and billing（账户和账单）
   - Technical（技术）
   - 要提高服务限额，请选择 Looking for service limit increases?（想提高服务限制？），然后按照创建增加服务限额 (p. 9)的说明操作。
4. 选择 Service（服务）、Category（类别）和 Severity（严重性）。

   Tip

   您可以使用针对常见问题提供的建议解决方案。
5. 选择 Next step: Additional information（下一步：其他信息）
6. 在 Additional information（其他信息）页面上，对于 Subject（主题），请为您的问题输入一个标题。
7. 对于 Description（描述），请按照提示操作以描述您的情况，例如：
   - 您收到的错误消息
   - 您遵循的故障排除步骤
   - 您如何访问服务：
     - Amazon Web Services Management Console
     - 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，选择您的首选语言以及希望使用的联系方式。您可以选择以下选项之一：

    a. Web – 通过 Support 中心接收回复。

b. Chat（聊天）– 开始与支持座席在线聊天。如果您无法连接到聊天，请参阅 问题排查 (p. 14)。
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）
- 电话号码
- (Optional) Extension [（可选）分机]

注意

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

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

Note

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

12. 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 和摘要。

# 描述您的问题

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

您提供尽可能多的详细信息意味着提升了快速解决案例的可能性。

# 选择严重性

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

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

| 严重性 | 严重性级别代码 | 第一响应时间 | 说明和支持计划 |
| --- | --- | --- | --- |
| 一般指南 | `low` | 24 小时 | 您遇到一般开发问题或想要申请一个功能。（开发人员*、商业、Enterprise On-Ramp 或企业 Support 计划） |

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

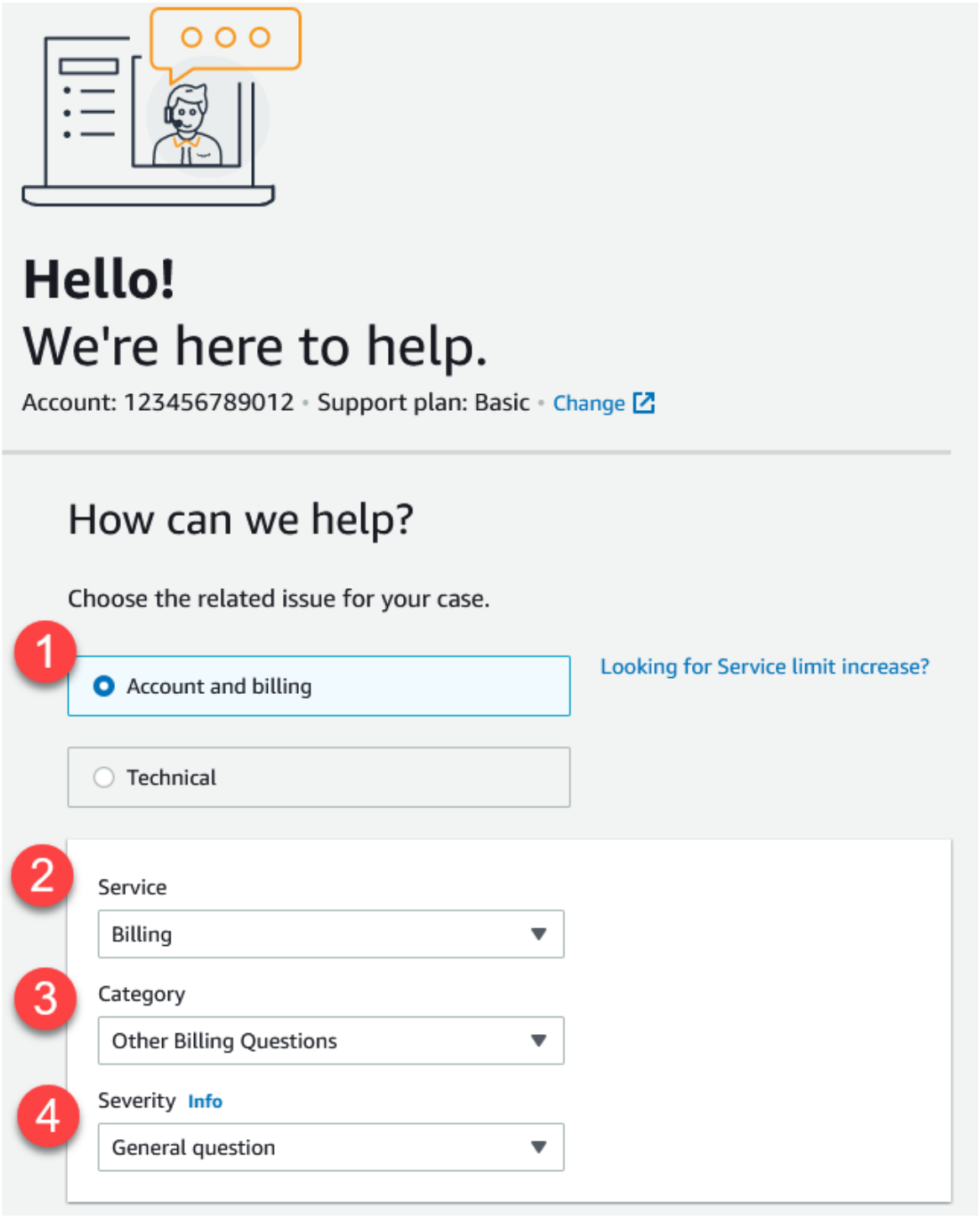
* 对于开发人员支持计划，响应目标按工作时间计算。工作时间是指客户所在国家/地区的上午 8:00 至下午 6:00，节假日和周末除外。此信息将显示在 Amazon Web Services Management Console 中的 My Account（我的账户）页面的 Contact Information（联系人信息）部分。对于跨多个时区的国家/地区，工作时间可能不尽相同。日语支持时间为上午 9:00 至下午 6:00。

Note

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

# 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。

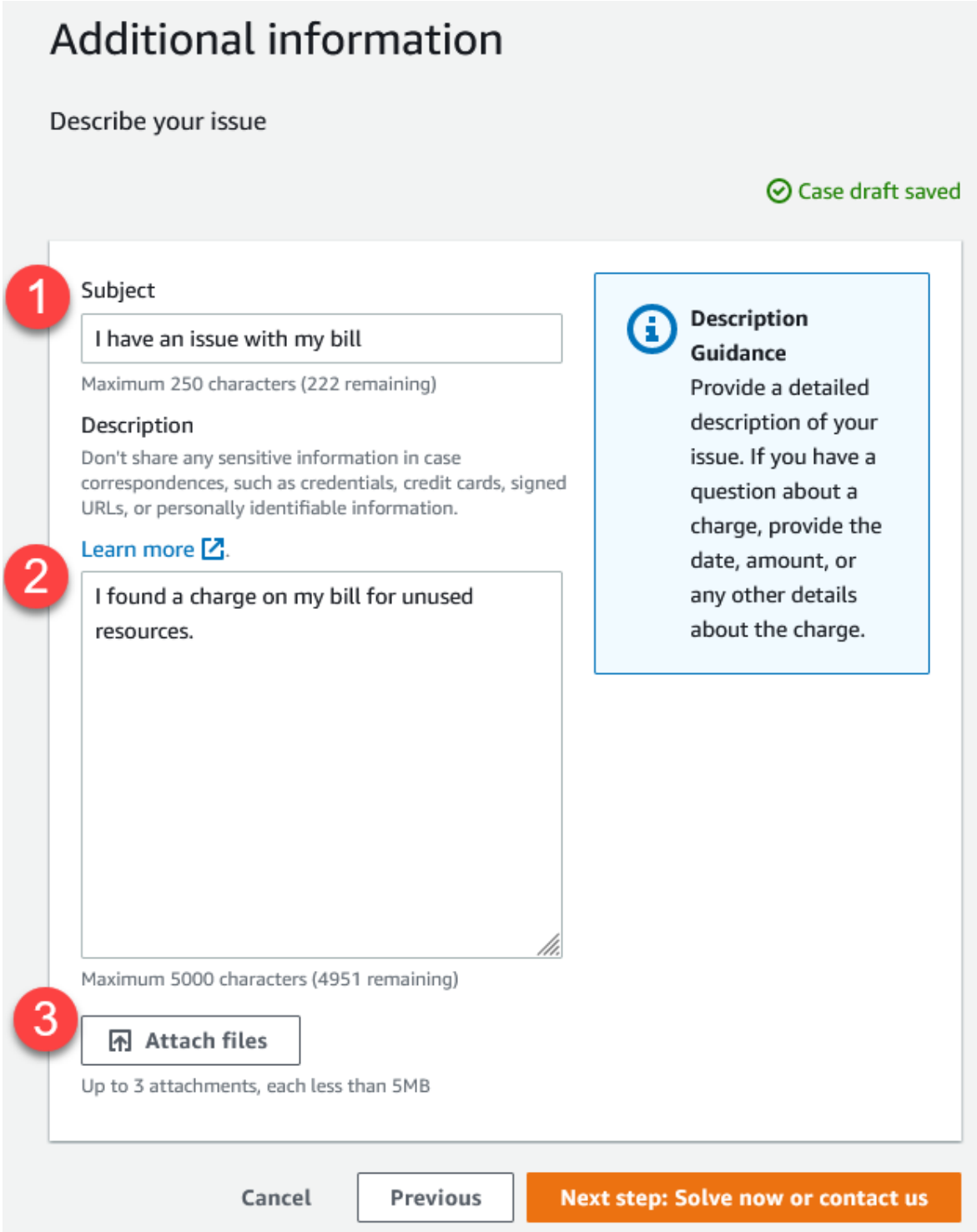
3. Category（类别）– 选择最符合您的使用案例的类别。当您选择某个类别时，将会在下方显示可解决问题的信息链接。
4. 严重性 – 已加入付费支持计划的客户可以选择 General guidance（一般指导）（响应时间为 1 天）或 System impaired（系统受影响）（响应时间为 12 小时）这两种严重性级别。已加入业务支持计划的客户还可以选择 Production system impaired（生产系统受损）（响应时间为 4 小时）或 Production system down（生产系统停机）（响应时间为 1 小时）。拥有商业、Enterprise On-Ramp 或企业 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 Amazon Web Services Support 首次响应的时间。这些响应时间不适用于后续响应。对于第三方问题，响应时间可能较长，具体取决于技术娴熟的人员是否有时间进行处理。有关更多信息，请参阅选择严重性 (p. 4)。

   Note

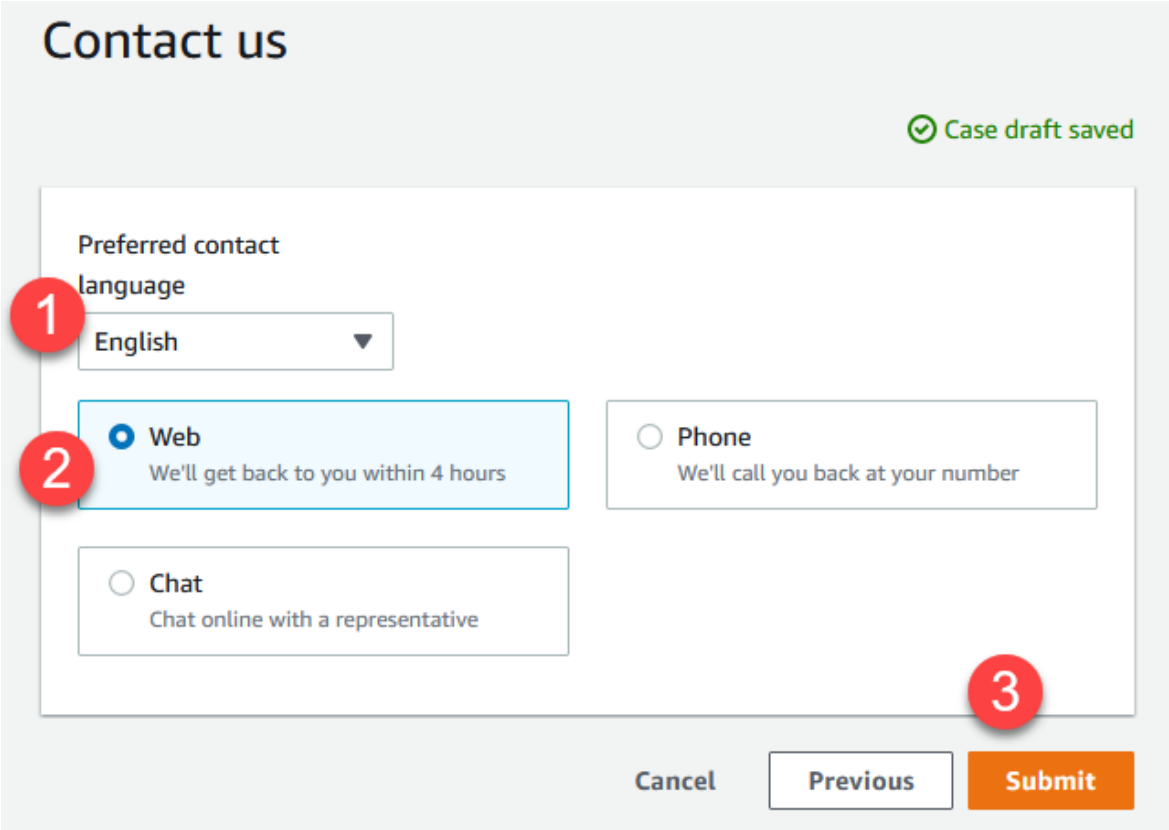
   根据您所选择的类别，系统可能会提示您提供更多信息。

在指定案例类型和分类后，可以指定描述以及希望与您联系的方式。




1. 主题 – 输入用于简要描述问题的标题。
2. Description（描述）– 描述您的支持案例。这是您向 Amazon Web Services Support 提供的最重要的信息。对于某些服务和类别组合，会有提示指出相关信息。请使用这些链接来帮助解决您的问题。有关更多信息，请参阅 描述您的问题 (p. 4)。
3. Attachments（附件）– 附上屏幕截图和其他文件，以帮助支持客服更快地解决您的问题。

在添加工单详细信息后，您可以选择您希望使用的联系方式。




1. 首选联系语言 – 目前，您可以选择英语或日语。
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)。

# 创建增加服务限额

请求增加服务限额（以前称为限制）以提高服务性能。

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

创建支持工单以请求增加服务限额

1. 登录到 Amazon Support Center Console。

   > Tip
   >
   > 在 Amazon Web Services Management Console中，您还可以选择问号图标（ ），然后选择 Support Center（Support 中心）。

2. 选择 Create case（创建案例）。
3. 选择 Looking for service limit increases?（想要提高服务限制？）
4. 要请求提高限额，请按照提示进行操作。可能的选项如下：

   - Limit type（限制类型）
   - 严重性

     Note

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

    - Web – 通过 Support 中心接收回复。
    - Chat（聊天）– 开始与支持客服实时聊天。如果您无法连接到聊天，请参阅 问题排查 (p. 14)。
    - 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）
      - 电话号码
      - (Optional) Extension [（可选）分机]
11. 选择 Submit（提交）。此时将显示您的案例 ID 和摘要。

# 更新、解决和重新打开您的案例

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

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

注意

- 您必须登录提交支持案例的 Amazon Web Services 账户。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Amazon Web Services Support 的访问权限 (p. 14)。
- 如果您在几天内未对案例作出回应，Amazon Web Services Support 会自动解决案例。
- 处于已解决状态超过 14 天的支持案例无法重新打开。如果您遇到与已解决案例相关的类似问题，您可以创建相关案例。有关更多信息，请参阅创建相关案例 (p. 12)。

主题

# 更新现有的支持案例

您可以更新案例，为支持代理提供更多信息。例如，您可以回复信件、开始另一个实时聊天、添加其他电子邮件收件人等。但是，在创建案例后，您无法更新案例的严重性。有关更多信息，请参阅选择严重性 (p. 4)。

### 更新现有的支持案例

1. 登录到 Amazon Support Center Console。

   Tip

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

   Tip

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

# 解决支持案例

当您对支持响应感到满意，或您的问题得到解决时，您可以在支持中心解决案例。

### 要解决支持案例

1. 登录到 Amazon Support Center Console。

   Tip

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

   Note

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

# 重新打开已解决的案例

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

注意

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

### 要重新打开已解决的案例

1. 登录到 Amazon Support Center Console。

   Tip

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

# 创建相关案例

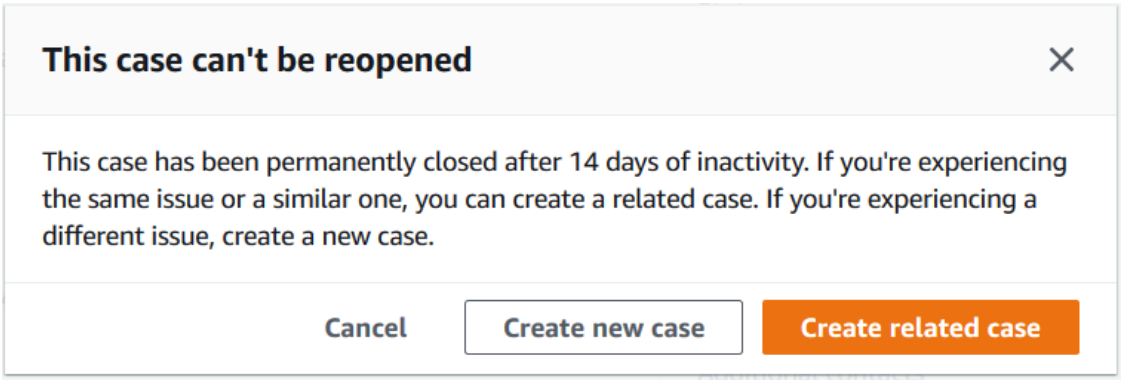
14 天处于不活动状态后，您将无法重新打开已解决的案例。如果您遇到与已解决案例相关的类似问题，您可以创建相关案例。此相关案例将包括指向先前解决的案例的链接，以便客服可以查看之前的案例详细信息和通信。如果您遇到的问题不同，我们建议您创建新案例。

### 要创建相关案例

1. 登录到 Amazon Support Center Console。

   Tip

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



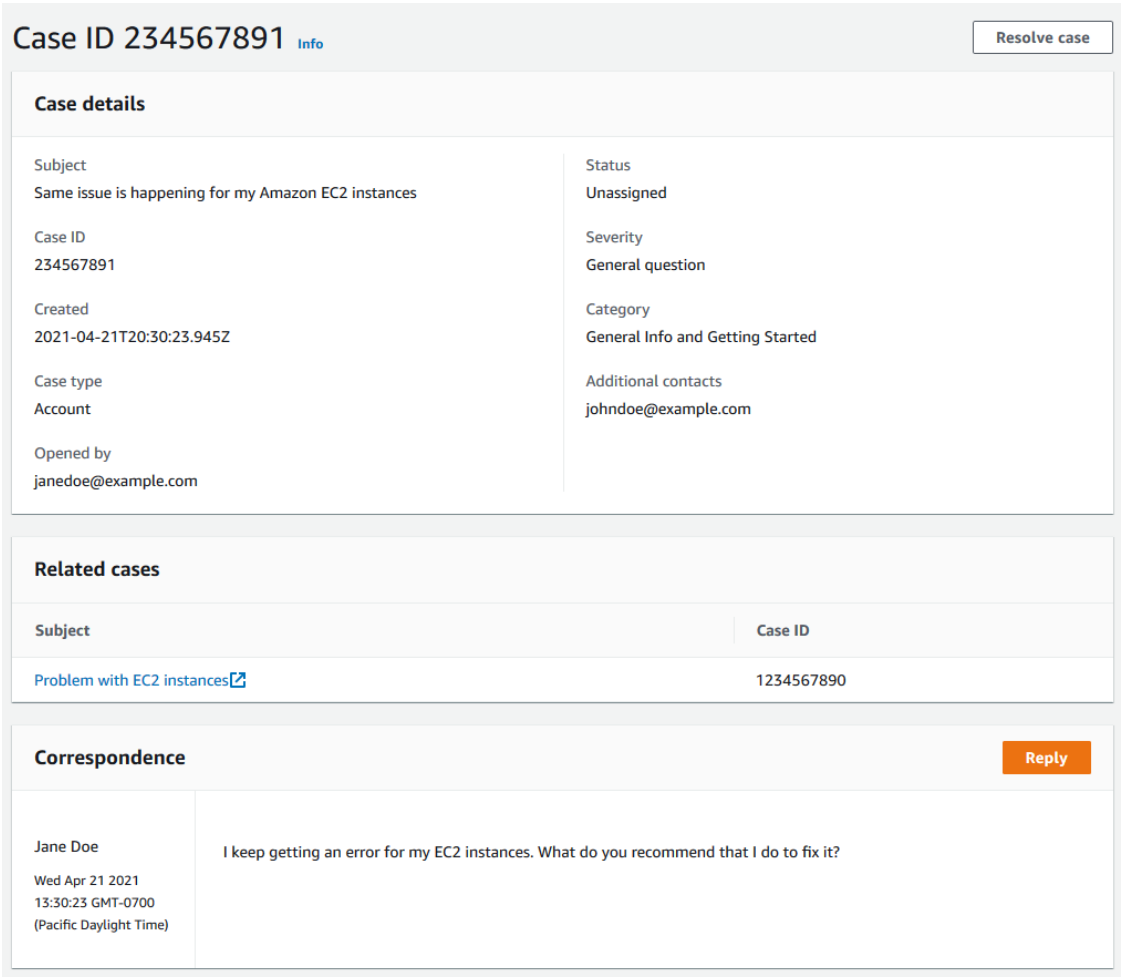

5. 按照同样的步骤创建您的案例。请参阅创建支持案例 (p. 3)。

   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 12 个月内查看案例历史记录信息。

# 问题排查

如果您在创建或管理支持案例时遇到问题，请参阅以下问题排查信息。

## 我想为我的案例重新打开实时聊天

您可以回复现有的支持案例以打开另一个聊天窗口。有关更多信息，请参阅更新现有的支持案例 (p. 11)。

## 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 Support：
  - 您的防火墙支持 Web 套接字连接。
  - 有关更多信息，请参阅《Amazon Connect 管理员指南》中的设置网络。

如果您仍然无法连接到聊天窗口，请联系您的 Amazon Web Services 账户 管理员。

# Amazon Web Services Support 的访问权限

您必须具有访问支持中心和创建支持案例 (p. 3)的权限。

您可以使用以下选项之一访问支持中心：

- 使用与您的 Amazon 账户关联的电子邮件地址和密码。此身份称作 Amazon 账户根用户。
- 使用 Amazon Identity and Access Management (IAM)。

如果您拥有商业、Enterprise On-Ramp 或企业 Support 计划，则还可以使用 Amazon Web Services Support API (p. 18) 以编程方式访问 Amazon Web Services Support 和 Trusted Advisor 操作。有关详细信息，请参阅 Amazon Web Services Support API 参考。

Note

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

## Amazon拥有账户

您可以使用您的 Amazon 账户电子邮件地址和密码登录 Amazon Web Services Management Console 并访问支持中心。此身份称作 Amazon 账户根用户。但是，我们强烈建议您不要使用根用户来执行日常任务，即使是管理任务。相反，我们建议您使用 IAM，它允许您控制哪些人可以在您的账户中执行某些任务。

# IAM

默认情况下，IAM 用户无法访问支持中心。您可以使用 IAM 创建各个用户或组。然后，您将 IAM 策略附加到这些实体，以便它们有权执行操作和访问资源，例如打开支持中心案例和使用 Amazon Web Services Support API。

创建 IAM 用户以后，您可以为这些用户提供单独的密码和账户特定的登录页面。然后，他们可以登录到 Amazon 账户并在支持中心工作。已获取 Amazon Web Services Support 访问权限的 IAM 用户可以看到为该账户创建的所有案例。

有关更多信息，请参阅 IAM 用户指南中的 IAM 用户如何登录您的 Amazon 账户。

授予权限的最简单方法是将 Amazon 托管策略 AWSSupportAccess 附加到用户、组或角色。Amazon Web Services Support 允许使用操作级权限来控制对特定 Amazon Web Services Support 操作的访问。Amazon Web Services Support 不提供资源级访问，因此 `Resource` 元素始终应设置为 `*`。您无法允许或拒绝对特定支持案例的访问。

### Example ：允许对所有 Amazon Web Services Support 操作的访问

Amazon 托管策略 AWSSupportAccess 向 IAM 用户授予对 Amazon Web Services Support 的访问权限。具有此策略的 IAM 用户可以访问所有 Amazon Web Services Support 操作和资源。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["support:*"],
            "Resource": "*"
        }
    ]
}
```

有关如何将 `AWSSupportAccess` 策略附加到您的实体的更多信息，请参阅 IAM 用户指南中的添加 IAM 身份权限（控制台）。

### Example ：允许访问除 ResolveCase 操作之外的所有操作

您也可以在 IAM 中创建客户托管策略来指定允许或拒绝哪些操作。以下策略语句允许 IAM 用户在 Amazon Web Services Support 中执行除解决案例之外的所有操作。

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "support:*",
      "Resource": "*"
   },
   {
       "Effect": "Deny",
       "Action": "support:ResolveCase",
       "Resource": "*"
    }]
}
```

有关如何创建客户托管式 IAM 策略的更多信息，请参阅 IAM 用户指南中的创建 IAM 策略（控制台）。

如果用户或组已有策略，则您可向该策略添加 Amazon Web Services Support 特定的策略语句。

Important

- 如果您无法在支持中心中查看案例，请确保您拥有所需的权限。您可能需要联系您的 IAM 管理员。有关更多信息，请参阅 适用于 Amazon Web Services Support 的 Identity and Access Management (p. 85)。

## 对 Amazon Trusted Advisor 的访问权限

在 Amazon Web Services Management Console中，单独的 `trustedadvisor` IAM 命名空间控制对 Trusted Advisor 的访问。在 Amazon Web Services Support API 中，`support` IAM 命名空间控制对 Trusted Advisor 的访问。有关更多信息，请参阅 管理对 Amazon Trusted Advisor 的访问 (p. 103)。

# 更改您的 Amazon Web Services Support 计划

您可以在 Amazon Web Services Management Console中更改您的支持计划。

更改您的支持计划

1. 使用您的根账户凭证在 https://console.aws.amazon.com/support/plans/home 登录到 Amazon Web Services Management Console。
2. 在 Support plans (支持计划) 页面上，选择 Change plan (更改计划)。
3. 在 Change support plan (更改支持计划) 页面上，选择 New plan (新建计划)，查看计划信息，然后选择 Change plan (更改计划)。

有关如何更改支持计划的示例视频，请参阅如何更改 Amazon Web Services Support 计划？

注意

如果您拥有商业、Enterprise On-Ramp 或企业 Support 计划，请使用 Change support plan（更改支持计划）页面上的链接联系 Amazon Web Services Support。

- 要关闭账户，请参阅 Amazon Billing 用户指南中的关闭账户。

# 将 Amazon Web Services Support 与 Amazon 开发工具包配合使用

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

| 软件开发工具包文档 |
| --- |
| Amazon SDK for Java |
| Amazon SDK for JavaScript |
| Amazon SDK for .NET |
| Amazon SDK for PHP |
| Amazon SDK for Python (Boto3) |

| 软件开发工具包文档 |
| --- |
| Amazon SDK for Ruby |

# 关于 Amazon Web Services Support API

Amazon Web Services Support API 提供对 Amazon 支持中心一些功能的访问。

API 提供两组不同的操作：

- 支持案例管理 (p. 18) 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 (p. 29) 检查的 Trusted Advisor (p. 18) 操作

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

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

主题

- 支持案例管理 (p. 18)
- Trusted Advisor (p. 18)
- Endpoint (p. 19)
- 在 Amazon 开发工具包中支持 (p. 19)

## 支持案例管理

可使用 API 执行以下任务：

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

Amazon Web Services Support API 能够对支持案例管理操作执行 CloudTrail 日志记录。有关更多信息，请参阅 使用 Amazon Web Services Support 记录 Amazon CloudTrail API 调用 (p. 117)。

有关演示如何管理支持案例的整个生命周期的 Java 代码示例，请参阅 为 Amazon Web Services Support 案例编程 (p. 20)。

## Trusted Advisor

您可以使用 Trusted Advisor 操作执行以下任务：

- 获取 Trusted Advisor 检查的名称和标识符

- 请求针对您的 Amazon 账户和资源运行 Trusted Advisor 检查
- 获取 Trusted Advisor 检查结果的摘要和详细信息
- 刷新您的 Trusted Advisor 检查
- 获取每个 Trusted Advisor 检查的状态

Amazon Web Services Support API 能够对 Trusted Advisor 操作执行 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 (p. 118)。

您可以使用 Amazon CloudWatch Events 监控对您的 Trusted Advisor 检查结果的更改。有关更多信息，请参阅 通过 Amazon EventBridge 监控 Amazon Trusted Advisor 的检查结果 (p. 123)。

例如，演示如何使用 Trusted Advisor 操作的 Java 代码，请参阅 使用 Trusted Advisor 即 Web 服务 (p. 34)。

# Endpoint

您可以使用以下终端节点访问 Amazon Web Services Support API：

- https://support.cn-north-1.amazonaws.com.cn

> **Important**
>
> Amazon Web Services Support 终端节点在生产数据库中创建案例。如果您正在创建测试支持案例，我们建议您在调用 CreateCase 操作时包含一个主题行，例如 TEST CASE-Please ignore。完成测试后，调用 ResolveCase 操作来解决案例。

有关使用 Amazon 终端节点的更多信息，请参阅 Amazon Web Services 一般参考中的区域和终端节点。

# 在 Amazon 开发工具包中支持

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

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

# 为 Amazon Web Services Support 案例编程

您可以使用 Amazon Web Services Support API 以编程方式创建支持案例，而不是在 Amazon Web Services Management Console 中使用 Amazon Web Services Support 中心。您可以添加通信信息并将文件附加到您的案例中，以便支持代理可以调查并帮助解决您的问题。本主题提供有关如何使用 Amazon Web Services Support API 操作的示例。

Notes

- 有关可用于 Amazon Web Services Support 的 API 操作、参数和数据类型的列表，请参阅 Amazon Web Services Support API 参考。
- 有关支持 Amazon Web Services Support API 的语言列表中，请选择一个操作名称，例如 CreateCase，并在 See Also（另请参阅）部分中，选择您的首选语言。

主题



## Overview

此主题使用 Java 代码示例演示 Amazon Web Services Support 的用法。有关开发工具包支持的更多信息，请参阅示例代码和库。

Note

如果您对 Amazon Web Services Support 的调用超出了服务配额，请参阅下列信息：

- Amazon Web Services Support API 的服务配额 (p. 28)
- Amazon 一般参考中 Amazon 中的错误重试和指数回退

### 结合使用 IAM 与 Amazon Web Services Support API

Amazon Identity and Access Management (IAM) 由 Amazon Web Services Support API 提供支持。有关更多信息，请参阅 Amazon Web Services Support 的访问权限 (p. 14)。

# 创建 Amazon Web Services Support 客户端

下方 Java 代码段显示了如何创建用于调用 AWSSupportClient 的 AWSSupportService：createClient 方法通过不带任何参数调用的 Amazon 构造函数来获取 AWSSupportClient() 凭证，该构造函数将从凭证提供程序链中检索凭证。有关此过程的更多信息，请参阅 Amazon SDK for Java 中的教程：使用 IAM 角色和 Amazon SDK for Java 授予访问权限。

有关 Amazon 凭证的更多信息，请参阅 Amazon 一般参考中的Amazon 安全凭证。

```
private static AWSSupportClient createClient()
{
    AWSSupportClient client = new AWSSupportClient();
    client.setEndpoint("https://support.cn-north-1.amazonaws.com.cn");
    return client;
}
```

# 发现 Amazon Web Services 和问题严重性级别

Amazon Web Services Support Java 客户端提供了 CreateCaseRequest 类型，用于以编程方式向 Amazon Web Services Support 提交案例。CreateCaseRequest 是一个结构，在填充请求参数后传递给 createClient 实例上的 AWSSupportClient 方法。这些参数包括指定 Amazon 服务和案例严重性的代码。

以下 Java 代码段展示了对 Amazon Web Services Support DescribeServices 和 DescribeSeverityLevel 操作的调用。

```
// DescribeServices example

public static void getServiceCodes(AWSSupportClient client)
{
    DescribeServicesResult result = client.describeServices();
    for (Service service : result.getServices())
    {
        System.out.println("Service code (name): " +
            service.getCode() + "(" + service.getName() + ")");
        for (Category category : service.getCategories())
        {
            System.out.println("    Category code (name): " +
                category.getCode() + "(" + category.getName() + ")");
        }
    }
}

// DescribeSeverityLevels example

public static void getSeverityLevels(AWSSupportClient client)
{
    DescribeSeverityLevelsResult result = client.describeSeverityLevels();
    for (SeverityLevel level : result.getSeverityLevelsList())
    {
        System.out.println("Severity level (name): " +
            level.getCode() + level.getName() + ")");
    }
}
```

每个调用均返回 JSON 格式的对象的列表。DescribeServices 返回服务代码及其相应的名称，DescribeSeverityLevels 返回严重性级别及其相应的名称。此外，DescribeServices 还返回适

用于每一种 Amazon Web Services Support 服务的 Amazon 类别的列表。另外，在使用 CreateCase 操作创建支持案例时，也会用到这些类别。虽然这些值也可以从 Amazon Web Services Support 站点获得，但 Amazon Web Services Support 服务始终会返回这些信息的最新版本。

# 创建附件集合

要为案例附加文件，必须在创建案例之前将附件添加到附件集合中。您最多可在一个附件集中添加 3 个附件，且附件集中任何附件的最大大小为 5 MB。有关更多信息，请参阅 AddAttachmentsToSet。

以下 Java 代码段创建一个文本文件附件，将它添加到一个附件集合，然后获取该附件集合的 ID 以便添加到案例中。

```
public static string createAttachmentSet() throws IOException
{
    BufferedReader reader =
        new BufferedReader(new InputStreamReader(System.in));

    // Get content and file name for an attachment.
    System.out.println("Enter text content for an attachment to the case: ");
    String attachmentcontent = null;
    try
    {
        attachmentcontent = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    System.out.println("Enter the file name for the attachment: ");
    String attachmentfilename = null;
    try
    {
        attachmentfilename = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    // Create the attachment.
    Attachment attachment1 = new Attachment();
    attachment1.setData(ByteBuffer.wrap(attachmentcontent.getBytes()));
    attachment1.setFileName("attachmentfilename");

    // Add the attachment to an array list.
    List<Attachment> attachments = new ArrayList<Attachment>();
    attachments.add(attachment1);

    // Create an attachment set and add the attachment array list to it.
    AddAttachmentsToSetRequest addAttachmentsToSetRequest =
        new AddAttachmentsToSetRequest();
    addAttachmentsToSetRequest.setAttachments(attachments);

    AddAttachmentsToSetResult addAttachmentsToSetResult =
        client.addAttachmentsToSet(addAttachmentsToSetRequest);

    // Get the ID of the attachment set.
    String attachmentsetid = addAttachmentsToSetResult.getAttachmentSetId();
    System.out.println("Attachment ID: " + attachmentsetid);
```

```
    return attachmentsetid;
}
```

# 创建支持案例

要使用 Amazon Web Services Support 服务创建 Amazon Web Services Support 案例，请使用以下信息填充 `CreateCaseRequest` 实例：

- `ServiceCode` – 通过调用 `DescribeServices` 操作获得的 Amazon Web Services Support 服务代码，如上一节中所述。
- `CategoryCode` – 描述支持案例所涉及的问题的类型的类别代码。
- `Language` – Amazon Web Services Support 提供支持时所用语言的代码。当前，Amazon 支持英语 (`en`) 和日语 (`ja`)。
- `CcEmailAddresses` – 将接收后续通信信息副本的电子邮件地址的列表。
- `CommunicationBody` – 最初所提交的案例的正文文本。
- `Subject` – 支持案例的标题。
- `SeverityCode` 调用 返回的值之一。`DescribeSeverityLevels`
- `AttachmentSetId` – ( 可选 ) 要纳入到案例中的一系列文件附件的 ID。`AddAttachmentsToSet` 操作可返回该 ID。

以下 Java 代码段从命令行收集每个案例创建参数的值。然后，它通过在 `CreateCaseRequest` 实例上调用 Amazon Web Services Support 方法填充 `createCase` 实例并将其传递给 `AWSSupportClient`。如果调用成功，该代码会返回以下格式的 Amazon Web Services Support `CaseId` 值：

```
case-123456789012-muen-2012-74a757cd8cf7558a
```

Note

Amazon Web Services Support 提供 `CaseId` 和 `DisplayId` 字段。`DisplayId` 字段对应于 Amazon Web Services Support 站点上显示的案例编号。`CaseId` 字段用于以编程方式与 Amazon Web Services Support 服务交互。这两个字段都通过 `CaseDetails` 数据类型公开。

```
public static void createCase(AWSSupportClient client) throws IOException
{
    BufferedReader reader =
        new BufferedReader(new InputStreamReader(System.in));

    System.out.println("Enter an Amazon service code: ");
    String servicecode = null;
    try
    {
        servicecode = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    System.out.println("Enter a category code: ");
    String categorycode = null;
    try
    {
```

```
    categorycode = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter a language code, 'en' for English: ");
String language = null;
try
{
    language = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter an email address to copy on correspondence: ");
String ccemailaddress = null;
try
{
    ccemailaddress = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter body text for the case: ");
String communicationbody = null;
try
{
    communicationbody = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter a subject for the case: ");
String casesubject = null;
try
{
    casesubject = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
}

System.out.println("Enter the severity code for the case: ");
String severitycode = null;
try
{
    severitycode = reader.readLine().trim();
}
catch (IOException e)
{
    e.printStackTrace();
    System.exit(1);
```

```
    }

    System.out.println("Enter the attachment set ID for the case: ");
    String attachmentsetid = null;
    try
    {
        attachmentsetid = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    CreateCaseRequest request = new CreateCaseRequest()
        .withServiceCode(servicecode)
        .withCategoryCode(categorycode)
        .withLanguage(language)
        .withCcEmailAddresses(ccemailaddress)
        .withCommunicationBody(communicationbody)
        .withSubject(casesubject)
        .withSeverityCode(severitycode)
        .withAttachmentSetId(attachmentsetid);

    CreateCaseResult result = client.createCase(request);
    System.out.println("CreateCase() Example: Case created with ID "
        + result.getCaseId());
}
```

# 检索和更新支持案例通信信息

Amazon Web Services Support 案例通常会导致客户和 Amazon Web Services Support 专业人员进行通信。Amazon Web Services Support 提供了 DescribeCommunications 和 DescribeAttachment 操作来检索此通信，以及 AddAttachmentsToSet 和 AddCommunicationToCase 操作来更新案例。这些操作使用 Communication 数据类型将更新传递给服务，并将它们返回到您的代码。

以下 Java 代码段将通信信息添加到 Amazon Web Services Support 案例。在示例中，为方便起见，提供了一个私有 `printCommunications` 方法。

```
public static void addCommunication(AWSSupportClient client)
{
    System.out.println("Enter the CaseID for the case you want to update.");
    BufferedReader reader =
        new BufferedReader(new InputStreamReader(System.in));
    String caseid = null;
    try
    {
        caseid = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    System.out.println("Enter text you want to add to this case.");
    String addcomm = null;
    try
    {
        addcomm = reader.readLine().trim();
    }
```

```
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    AddCommunicationToCaseRequest request =
        new AddCommunicationToCaseRequest().withCaseId(caseid)
                                           .withCommunicationBody(addcomm);
    client.addCommunicationToCase(request);

    System.out.println(
        "AddCommunication() Example: Call GetCommunications() " +
        "if you want to see if the communication was added.");
}

// DescribeCommunications example

public static void getCommunications(AWSSupportClient client)
    throws IOException
{
    BufferedReader reader =
        new BufferedReader(new InputStreamReader(System.in));
    String caseNumber = null;

    System.out.println("Enter a CaseID");
    caseNumber = reader.readLine().trim();

    {
        DescribeCommunicationsRequest request =
            new DescribeCommunicationsRequest()
            .withCaseId(caseNumber.toString());

        DescribeCommunicationsResult result =
            client.describeCommunications(request);
        printCommunications(result.getCommunications());

        // Get more pages.
        while (result.getNextToken() != null)
        {
            request.setNextToken(result.getNextToken());
            result = client.describeCommunications(request);
            printCommunications(result.getCommunications());
            System.out.println(
                "GetCommunications() Example: Case communications retrieved"
                + " for case number " + request.getCaseId().toString());
        }
    }
}

private static void printCommunications(List<Communication> communications)
{
    for (Communication communication : communications)
    {
        System.out.println("SubmittedBy: " + communication.getSubmittedBy());
        System.out.println("  Body: " + communication.getBody());
    }

}
```

Note

DescribeCommunications 返回一个支持案例的五条最近的通信信息。此外，DescribeCommunications 还接受 CaseId 值列表，以便您可以在单次调用中检索多个案例的通信信息。

# 检索所有支持案例信息

您可以通过调用 DescribeCases 操作检索与您的 Amazon Web Services Support 案例关联的所有信息。您用 DescribeCasesRequest 值列表填充 ClientId 数据类型，这些值在成功的 createCase 请求返回时由每个案例返回。

以下 Java 代码段从控制台接受 CaseId 值，并填充 DescribeCasesRequest 实例以供 DescribeCases 操作使用。为方便起见，提供了一个私有 printCases 方法。

```
public static void getCases(AWSSupportClient client)
{
    BufferedReader reader =
        new BufferedReader(new InputStreamReader(System.in));

    System.out.println("Enter an Amazon Web Services Support Case ID");
    String caseid = null;
    try
    {
        caseid = reader.readLine().trim();
    }
    catch (IOException e)
    {
        e.printStackTrace();
        System.exit(1);
    }

    DescribeCasesRequest request = new DescribeCasesRequest();
    request.withCaseIdList(caseid);

    DescribeCasesResult result = client.describeCases(request);
    printCases(result.getCases());

    // Get more pages.
    while (result.getNextToken() != null)
    {
        request.setNextToken(result.getNextToken());
        result = client.describeCases(request);
        printCases(result.getCases());
    }
}

private static void printCases(List<CaseDetails> caseDetailsList)
{
    for (CaseDetails caseDetails : caseDetailsList)
    {
        System.out.println(
            "Case ID: " + caseDetails.getCaseId()); // This ID is for API use.
        System.out.println(
            "  Display ID: " + caseDetails.getDisplayId());
            // This ID is displayed on the Amazon Web Services Support website.
        System.out.println("  Language: " + caseDetails.getLanguage());
        System.out.println("  Status: " + caseDetails.getStatus());
        System.out.println("  Subject: " + caseDetails.getSubject());
        System.out.println("Recent Communications: " +
            caseDetails.getRecentCommunications());
    }
}
```

Note

DescribeCases 操作所用的参数可用来控制要检索的案例数量、案例类型和详细信息数量。有关更多信息，请参阅 DescribeCases 操作。

# 解决支持案例

Amazon Web Services Support 提供了一个 ResolveCase 操作供您解决自己的支持案例。以下 Java 代码示例演示了该操作的用法。

```
public static void resolveSupportCase(AWSSupportClient client)
{
    System.out.println(
        "Enter the Amazon Web Services Support case ID for the case you want to resolve.");
    BufferedReader BR = new BufferedReader(new InputStreamReader(System.in));

    String caseid = null;
    try
    {
        caseid = BR.readLine().trim();
    }
    catch (IOException e)
    {
        // TODO Auto-generated catch block
        e.printStackTrace();
    }

    ResolveCaseResult rcr =
        client.resolveCase(new ResolveCaseRequest().withCaseId(caseid));
    System.out.println("Initial case status: " + rcr.getInitialCaseStatus());
    System.out.println("Final case status: " + rcr.getFinalCaseStatus());
}
```

# Amazon Web Services Support API 的服务配额

下表介绍了 Amazon Web Services Support API 的当前配额。

| 资源 | 默认值 |
| --- | --- |
| 您可以创建的 Amazon Web Services Support 案例的最大数量。 | 每小时 10 个<br><br>在中国（北京）区域，您每天最多可以创建 240 个 Amazon Web Services Support 案例。 |
| 每秒可执行的 Amazon Web Services Support API 操作的最大数量。 | 5 |
| 每秒可执行的 Amazon Trusted Advisor API 操作的最大数量。 | 100 |

# Amazon Trusted Advisor

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

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

如果您拥有商业、Enterprise On-Ramp 或企业 Support 计划，则可以使用 Trusted Advisor 控制台和 Amazon Web Services Support API (p. 18) 访问所有的 Trusted Advisor 检查。您也可以使用 Amazon CloudWatch Events 来监控 Trusted Advisor 检查的状态。有关更多信息，请参阅通过 Amazon EventBridge 监控 Amazon Trusted Advisor 的检查结果 (p. 123)。

您可以在 Amazon Web Services Management Console 中访问 Trusted Advisor。有关控制对 Trusted Advisor 控制台的访问权限的更多信息，请参阅 管理对 Amazon Trusted Advisor 的访问 (p. 103)。

有关更多信息，请参阅Trusted Advisor。

主题



# 开始使用 Amazon Trusted Advisor

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

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

主题

# 登录到 Trusted Advisor 控制台

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

Note

您必须具有 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 Amazon Trusted Advisor 的访问 (p. 103)。

### 登录到 Trusted Advisor 控制台

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Dashboard（控制面板）页面上，查看每种检查类别的摘要：
   - 建议操作（红色）– Trusted Advisor 建议对检查进行的操作。例如，检测到 IAM 资源安全问题的检查可能会建议紧急步骤。
   - 建议调查（黄泽）– Trusted Advisor检测到检查的可能问题。例如，达到资源配额的检查可能会建议删除未使用的资源的方法。
   - 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。例如，这可能是您不希望检查评估的 Amazon EC2 实例。
3. 您可以在 Dashboard（控制面板）上执行以下操作：
   - 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 – 可以使您的 Amazon 解决方案更加安全的安全设置的建议。
- Fault tolerance（容错能力）– 可帮助提高您的Amazon解决方案的弹性的建议。这些检查突出显示冗余不足、当前服务限制（也称为配额）和过度使用的资源。
- Service limits（服务限制）– 检查您账户的使用情况以及您的账户是否接近或超过Amazon服务和资源的限制（也称为配额）。

### 要查看检查类别

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
2. 在导航窗格中，选择检查类别。
3. 在类别页面上，查看每种检查类别的摘要：
   - 建议操作（红色）– Trusted Advisor 建议对检查进行的操作。
   - 建议调查（黄泽）– Trusted Advisor检测到检查的可能问题。

- 未检测到问题（绿色）– Trusted Advisor 未检测到检查的问题。
- 排除的项目（灰色）– 包含排除项目的检查数，例如您希望检查忽略的资源。

4. 对于每次检查，选择刷新图标 (  ) 以刷新此检查。
5. 选择下载图标 (  ) 以创建一个包含此检查结果的 .xls 文件。

# 查看特定检查

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

要查看特定检查

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
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。

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

要筛选您的检查

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
2. 在导航窗格或 Dashboard（控制面板）页面中，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：
   - 所有检查 – 列出此类别的所有检查
   - 建议的操作 – 列出建议您采取操作的检查。这些检查以红色突出显示。
   - 建议的调查 – 列出建议您采取可能的操作的检查。这些检查以黄色突出显示。

- 未检测到问题 – 列出没有任何问题的检查。这些检查以绿色突出显示。
- 包含排除项目的检查 – 列出您指定的用于从检查结果中排除项目的检查。

5. 如果您将标签添加到 Amazon 资源，例如 Amazon EC2 实例或 Amazon CloudTrail 跟踪，您可以筛选结果，以使检查仅显示具有指定标签的项目。

   对于按标签筛选，输入标签键和值，然后选择 Apply filter（应用筛选条件）。


6. 在检查的表中，检查结果仅显示具有指定键和值的项目。
7. 要按标签清除筛选条件，请选择 Reset（重置）。

## 相关信息

有关 Trusted Advisor 的标签的更多信息，请参阅以下主题：

- Amazon Web Services Support 启用 Trusted Advisor 的标记功能
- Amazon 一般参考中的标记 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。如果您使用的是开发人员或基本支持计划，则可以登录 Trusted Advisor 控制台刷新检查。如果您拥有商业、Enterprise On-Ramp 和企业 Support 计划，则 Trusted Advisor 会每周自动刷新您账户中的检查。

### 要刷新 Trusted Advisor 检查

1. 导航到位于 https://console.aws.amazon.com/trustedadvisor 的 Amazon Trusted Advisor 控制台。
2. 在 Dashboard（控制面板）或检查类别页面上，选择 Refresh all checks（刷新所有检查）。

您也可以通过以下方式刷新特定检查：

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

  注意

  - Trusted Advisor 会每天自动刷新几次某些检查，例如 Amazon Well-Architected high risk issues for reliability（可靠性高风险问题）检查。更改可能需要在几个小时后才会在您的账户中显示。对于这些自动刷新的检查，您无法选择刷新图标（ ）来手动刷新结果。
  - 如果您为账户启用了 Amazon Security Hub，您将无法使用 Trusted Advisor 控制台来刷新 Security Hub 控件。有关更多信息，请参阅刷新 Security Hub 检查结果 (p. 53)。

# 下载检查结果

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

要下载 Trusted Advisor 检查结果

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

# 组织视图

您可以设置组织视图功能，以为 Amazon 组织中的所有成员账户创建报告。有关更多信息，请参阅Amazon Trusted Advisor 的组织视图 (p. 37)。

# Preferences（首选项）

在 Trusted Advisor 控制台的 Preferences（首选项）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。

在 Organizations（组织）页面上，您可以启用或禁用组织视图功能。

## 设置通知首选项

指定谁可以接收检查结果和语言的 每周 Trusted Advisor 电子邮件消息。

要设置通知首选项

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
2. 在导航窗格中，在 Preferences（首选项）下，选择 Notifications（通知）。
3. 对于 Weekly email notification（每周电子邮件通知），选择将您检查结果通知给谁。您可以从 Amazon Billing and Cost Management 控制台的 Account Settings（账户设置）页面中添加和删除联系人。
4. 对于 Language（语言），选择电子邮件消息的语言。
5. 选择 Save email preferences（保存电子邮件首选项）。

## 设置组织视图

如果您使用 Amazon Organizations 设置账户，您可以为组织中的所有成员账户创建报告。有关更多信息，请参阅Amazon Trusted Advisor 的组织视图 (p. 37)。

## 禁用 Trusted Advisor

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

要禁用 Trusted Advisor

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
2. 在导航窗格中，选择 Preferences。
3. 在 Trusted Advisor 下，选择 Disable Trusted Advisor（禁用 Trusted Advisor）。此操作为您账户中的所有检查禁用 Trusted Advisor。
4. 然后，您可以从账户中手动删除 Trusted Advisor 服务角色。有关更多信息，请参阅删除 Trusted Advisor 的服务相关角色 (p. 94)。

## 相关信息

有关 Trusted Advisor 的更多信息，请参阅以下主题：

- 如何开始使用 Trusted Advisor？
- Amazon Trusted Advisor 检查引用 (p. 59)

# 使用 Trusted Advisor 即 Web 服务

借助 Amazon Web Services Support 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 (p. 34)
- 刷新可用 Trusted Advisor 检查的列表 (p. 34)
- 轮询 Trusted Advisor 检查以了解状态变化 (p. 35)
- 请求 Trusted Advisor 检查结果 (p. 36)
- 输出 Trusted Advisor 检查的详细信息 (p. 37)

## 获取可用 Trusted Advisor 检查的列表

以下 Java 代码段创建一个 Amazon Web Services Support 客户端实例，您可使用该客户端来调用所有 Trusted Advisor API 操作。接下来，这段代码通过调用 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 Support 客户端实例，您可使用该客户端来刷新 Trusted Advisor 数据。

```
// Refresh a Trusted Advisor Check
```

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

# 轮询 Trusted Advisor 检查以了解状态变化

在提交运行 Trusted Advisor 检查以生成最新状态数据的请求之后，请使用 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。

## 输出 Trusted Advisor 检查的详细信息

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

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

# Amazon Trusted Advisor 的组织视图

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

> 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：

- 该账户必须是 Amazon 组织的成员。
- 您的组织必须已启用 Organizations 的所有功能。有关更多信息，请参阅 Amazon Organizations 用户指南中的启用组织中的所有功能。
- 您组织中的管理账户必须拥有商业、Enterprise On-Ramp 和企业 Support 计划。您可以从 Amazon Web Services Support 中心或从 Support plans（支持计划）页面中查找您的支持计划。请参阅比较 Amazon Web Services Support 计划。
- 您必须以管理账户中的用户身份（或承担的等效角色）登录。无论您是以 IAM 用户还是 IAM 角色登录，您都必须拥有具有所需权限的策略。请参阅使用 IAM 策略允许访问组织视图 (p. 43)。

# 启用组织视图

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

- Trusted Advisor 被启用为组织中的可信服务。有关更多信息，请参阅 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 在您组织中的管理账户中为您创建。此角色包括 Trusted Advisor 代表您调用 Organizations 所需的权限。此服务关联角色已锁定，您无法手动删除它。有关更多信息，请参阅将服务相关角色用于 Trusted Advisor (p. 92)。

从 Trusted Advisor 控制台中启用组织视图。

要启用组织视图

1. 以管理员身份登录组织的管理账户，并打开位于 https://console.aws.amazon.com/trustedadvisor 的 Amazon Trusted Advisor 控制台。
2. 在导航窗格中的 Preferences（首选项）下，选择 Organization（组织）。
3. 在 Organization view（组织视图）下，选择 Enable organizational view（启用组织视图）。

> **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。Amazon Web Services Support 计划决定了为账户提供了哪些 Trusted Advisor 检查。

# 刷新 Trusted Advisor 检查

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

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

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

要刷新 Trusted Advisor 检查

1. 导航到位于 https://console.aws.amazon.com/trustedadvisor 的 Amazon Trusted Advisor 控制台。
2. 在控制面板页面上，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，并打开位于 https://console.aws.amazon.com/trustedadvisor 的 Amazon Trusted Advisor 控制台。
2. 在导航窗格中，选择 Organizational View（组织视图）。
3. 选择创建报告。
4. 默认情况下，报告包含所有 Amazon 区域、检查类别、检查和资源状态。在 Create report（创建报告）页面上，您可以使用筛选条件选项自定义报告。例如，您可以清除区域的 All（全部）选项，然后指定要包括在报告中的单个区域。
   a. 输入报告的 Name（名称）。
   b. 对于 Format，选择 JSON 或 CSV。
   c. 对于 Region（区域），指定 Amazon 区域或选择 All（全部）。
   d. 对于 Check category（检查类别），选择检查类别或选择 All（全部）。
   e. 对于 Checks（检查），选择该类别的特定检查，或选择 All（全部）。

      Note

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

   f. 对于 Resource status（资源状态），选择要筛选的状态，如 Warning（警告），或选择 All（全部）。
5. 对于 Amazon 组织，选择要包含在您的报告中的组织单位 (OU)。有关 OU 的更多信息，请参阅 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：

- 三个 Amazon 区域
- 所有的安全和性能检查

在以下示例中，报告包含 support-team OU 和属于组织一部分的一个 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 控制台中查看报告摘要。这样，您就可以快速查看整个组织的检查结果摘要。

### 要查看报告摘要

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

# 下载组织视图报告

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

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

### 要下载组织视图报告

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

   Organizational View（组织视图）页面显示可供下载的报告。
3. 选择一个报告，选择 Download report（下载报告），然后保存文件。一次只能下载一个报告。
4. 解压缩该文件。
5. 使用文本编辑器打开 `.json`文件或使用电子表格应用程序打开 `.csv` 文件。

   > **Note**
   >
   > 如果您的报告为 5MB 或以上，您可能会收到多个文件。

### Example ：summary.json 文件

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

Trusted Advisor 使用以下颜色代码表示检查结果：

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

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

```
{
    "numAccounts": 3,
    "filtersApplied": {
        "accountIds": ["123456789012","111122223333","111111111111"],
        "checkIds": "All",
        "categories": [
            "security",
            "performance"
```

```
        ],
        "statuses": "All",
        "regions": [
            "us-west-1",
            "us-west-2",
            "us-east-1"
        ],
        "organizationalUnitIds": [
            "ou-xa9c-EXAMPLE1",
            "ou-xa9c-EXAMPLE2"
        ]
    },
    "categoryStatusMap": {
        "security": {
            "statusMap": {
                "ERROR": {
                    "name": "Red",
                    "count": 2
                },
                "OK": {
                    "name": "Green",
                    "count": 1
                },
                "WARN": {
                    "name": "Yellow",
                    "count": 1
                }
            },
            "name": "Security"
        }
    },
    "accountStatusMap": {
        "123456789012": {
            "security": {
                "statusMap": {
                    "ERROR": {
                        "name": "Red",
                        "count": 2
                    },
                    "OK": {
                        "name": "Green",
                        "count": 1
                    },
                    "WARN": {
                        "name": "Yellow",
                        "count": 1
                    }
                },
                "name": "Security"
            }
        }
    }
}
```

Example ：schema.json 文件

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

```
{
    "Yw2K9puPzl": [
        "Password Policy",
        "Uppercase",
        "Lowercase",
```

```
        "Number",
        "Non-alphanumeric",
        "Status",
        "Reason"
    ],
    "DqdJqYeRm5": [
        "Status",
        "IAM User",
        "Access Key",
        "Key Last Rotated",
        "Reason"
    ],
    ...
}
```

Example

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

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

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

- 某些检查，例如根账户上的 MFA，没有资源，也不会显示在报告中。无资源的检查将改为显示在 `summary.json` 文件中。
- 有些检查仅在它们为 `Red` 或者 `Yellow` 时显示资源。如果所有资源都为 `Green`，则它们可能不会出现在您的报告中。
- 如果没有为需要检查的服务启用账户，则检查可能不会显示在报告中。例如，如果您的组织中没有使用 Amazon Elastic Compute Cloud 预留实例，则 Amazon EC2 Reserved Instance Lease Expiration 检查将不会显示在您的报告中。
- 账户尚未刷新检查结果。当具有基本支持计划或开发人员支持计划的用户首次登录 Trusted Advisor 控制台时可能会发生此情况。如果您拥有商业、Enterprise On-Ramp 和企业 Support 计划，则用户最长可能需要在账户注册后一周才能看到检查结果。有关更多信息，请参阅刷新 Trusted Advisor 检查 (p. 38)。
- 如果只有组织的管理账户启用了检查建议，则报告将不会包括组织中其他账户的资源。

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

.json 文件格式比 .csv 文件格式提供的灵活度更大，可用于高级使用案例，例如使用多个数据集的聚合和高级分析。例如，您可以将 SQL 界面与 Amazon 服务（例如 Amazon Athena）结合使用以对您的报告运行查询。您还可以使用 Amazon QuickSight 创建控制面板并可视化您的数据。有关更多信息，请参阅使用其他 Amazon 服务查看 Trusted Advisor 报告 (p. 45)。

# 禁用组织视图

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

禁用此功能后，将出现以下情况：

- Trusted Advisor 将作为 Organizations 中的可信服务删除。
- `AWSServiceRoleForTrustedAdvisorReporting` 服务关联角色在您组织的管理账户中解锁。这意味着如果需要，您可以手动删除它。
- 您无法为组织创建、查看或下载报告。要访问以前创建的报告，您必须从 Trusted Advisor 控制台中重新启用组织视图。请参阅启用组织视图 (p. 38)。

### 要禁用 Trusted Advisor 的组织视图

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

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

> **Note**
>
> 您可以使用其他 Amazon 服务查询和可视化组织视图报告的数据。有关更多信息，请参阅以下 资源：
>
> - 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 (p. 45)

# 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 Amazon Trusted Advisor 中的组织视图。

### Example ：对组织视图的完全访问权限

以下策略允许完全访问组织视图功能。具备这些权限的用户可以执行以下操作：

- 启用和禁用组织视图
- 创建、查看和下载报告

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
```

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

Example ：对组织视图的读取访问权限

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadStatement",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:DescribeOrganization",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "trustedadvisor:DescribeAccount",
                "trustedadvisor:DescribeChecks",
                "trustedadvisor:DescribeCheckSummaries",
                "trustedadvisor:DescribeAccountAccess",
                "trustedadvisor:DescribeOrganization",
                "trustedadvisor:DescribeReports",
```

```
                "trustedadvisor:ListAccountsForParent",
                "trustedadvisor:ListRoots",
                "trustedadvisor:ListOrganizationalUnitsForParent"
            ],
            "Resource": "*"
        }
    ]
}
```

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

Note

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

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

有关服务相关角色的更多信息，请参阅 将服务相关角色用于 Trusted Advisor (p. 92)。

# 使用其他 Amazon 服务查看 Trusted Advisor 报告

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

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

## Prerequisites

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 区域快速设置您的 Amazon 服务和资源。
- 创建 Amazon QuickSight 账户。有关更多信息，请参阅 Amazon QuickSight 用户指南中的 Amazon QuickSight 中的数据分析入门。

## 将报告上载到 Amazon S3

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

要将报告上载到 Amazon S3 存储桶

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

7. 在 folder1 中，选择 Upload（上载），然后选择 `resources.json` 文件。
8. 选择 Next（下一步），保留默认选项，然后选择 Upload（上载）。

   Note

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

## 使用 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。此模板将告知 Amazon CloudFormation 要为您的账户创建哪些资源，以便其他服务可以使用 S3 存储桶中的报告数据。该模板为 IAM 创建资源 Amazon Lambda 和 Amazon Glue。

要使用 Amazon CloudFormation 创建资源

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

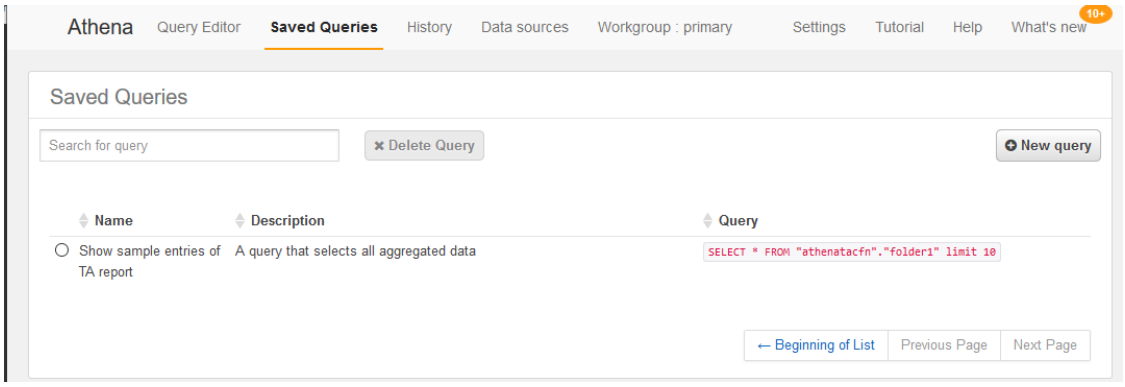
拥有资源后，您可以在 Athena 中查看数据。使用 Athena 创建查询并分析报告的结果，例如查找组织中的账户的特定检查结果。

Notes

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

### 要在 Athena 中查询数据

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



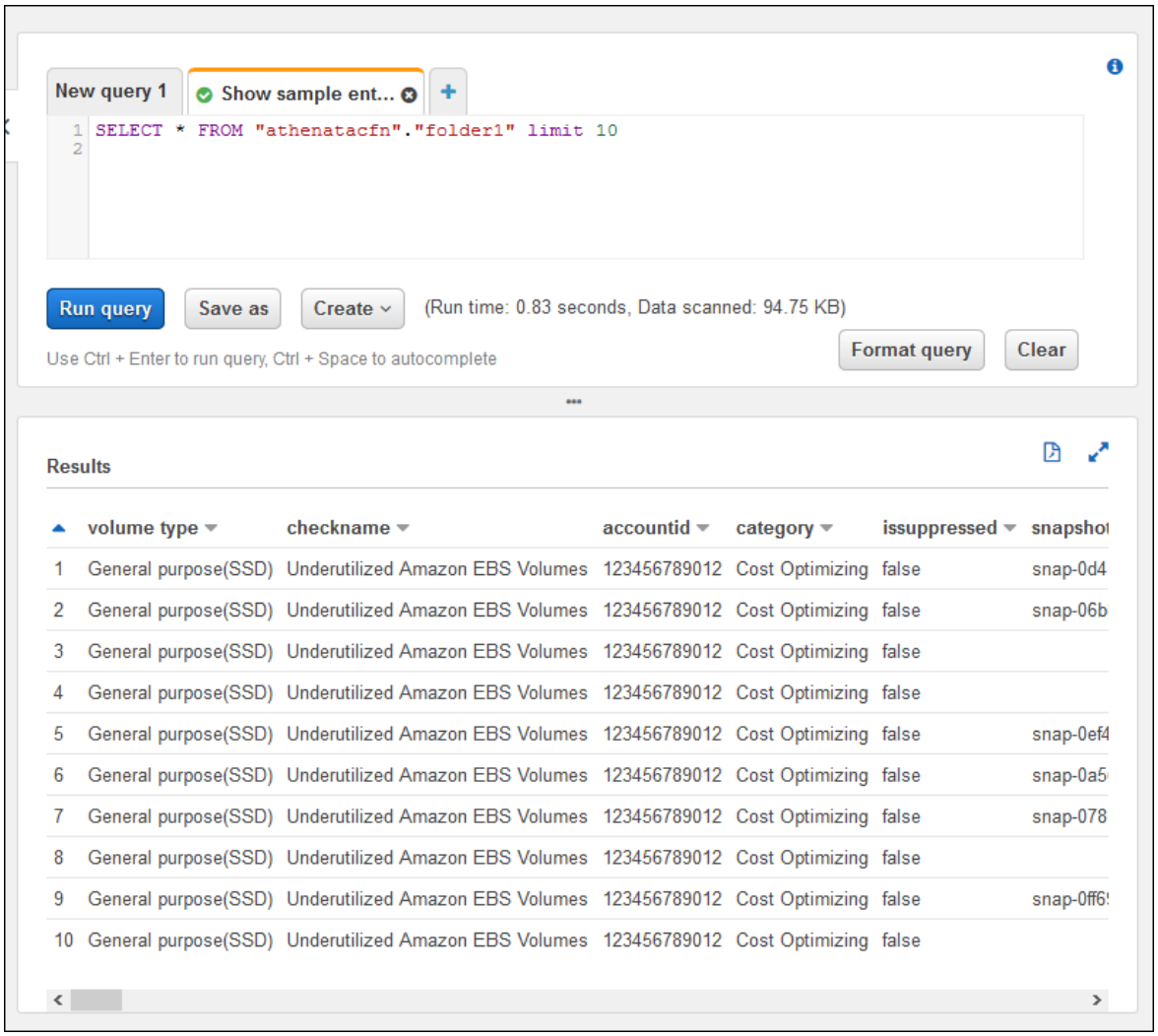

查询应与以下内容类似。

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

5. 选择 Run query (运行查询)。您的查询结果显示出来。

### Example ：Athena 查询

以下示例显示报告中的 10 个示例条目。




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

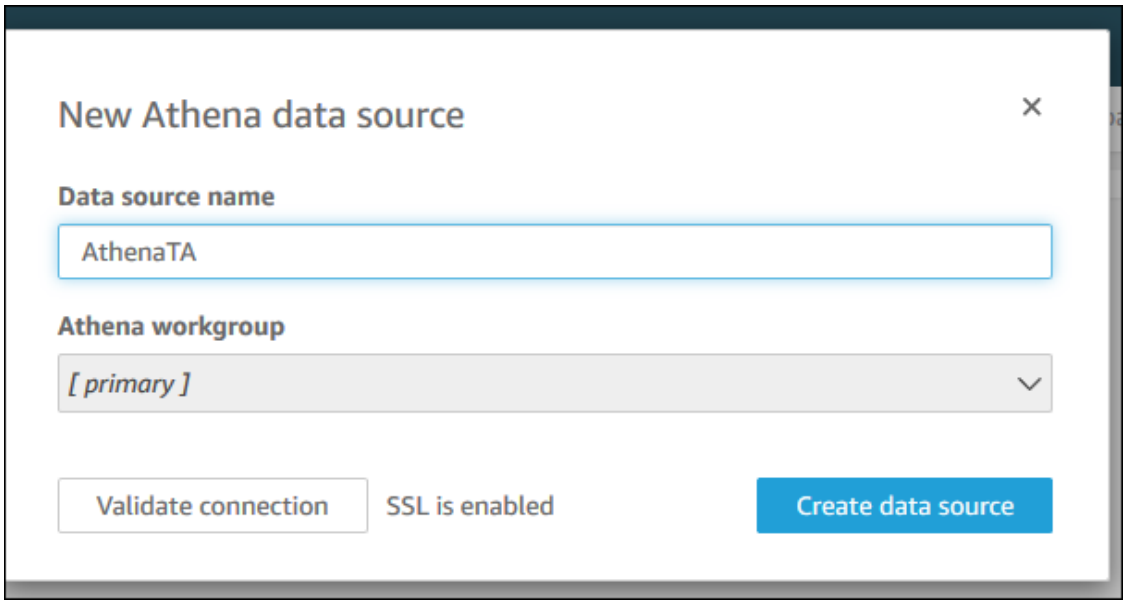
## 在 Amazon QuickSight 中创建控制面板

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

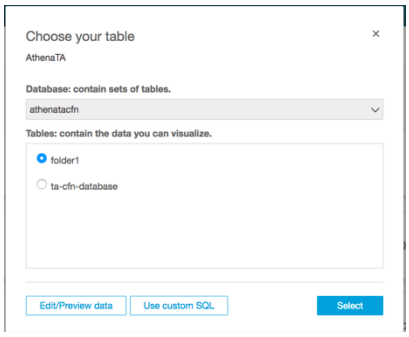
> Note
>
> 您必须使用美国东部（弗吉尼亚北部）区域。

### 要在 Amazon QuickSight 中创建控制面板

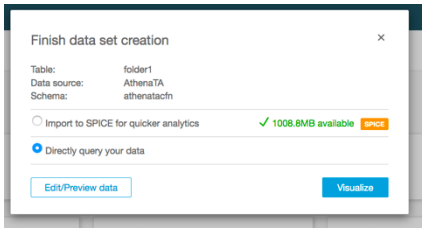
1. 导航到 Amazon QuickSight 控制台，然后登录您的账户。
2. 选择 New analysis（新的分析）、New dataset（新数据集），然后选择 Athena。
3. 在 New Athena data source（新 Athena 数据源）对话框中，输入数据源名称，例如 AthenaTA，然后选择 Create data source（创建数据源）。




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）。




现在，您可以在 Amazon QuickSight 中创建控制面板。有关更多信息，请参阅 Amazon QuickSight 用户指南中的使用控制面板。

### Example ：Amazon QuickSight 控制面板

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

- 受影响的账户 ID
- 按 Amazon 区域划分的摘要
- 检查类别
- 检查状态

- 每个账户的报告中的条目数


Note

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

# Troubleshooting

如果您在本教程中遇到问题，请参阅以下故障排除提示。

## 我没有在我的报告中看到最新数据

创建报告时，组织视图功能不会自动刷新您的组织中的 Trusted Advisor 检查。要获取最新的检查结果，请刷新组织中的管理账户和每个成员账户的检查。有关更多信息，请参阅 刷新 Trusted Advisor 检查 (p. 38)。

## 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 schema 并快速识别您的报告中是否有重复的列。

要查找重复列

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

   如果您有重复的列，则必须将新报告上载到您的 Amazon S3 存储桶。参阅以下 上载新报告 (p. 51) 部分。

### 上载新报告

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

要上载新报告

1. 如果您尚未设置，请为组织中的账户刷新您的 Trusted Advisor 检查。请参阅 刷新 Trusted Advisor 检查 (p. 38)。
2. 在 Trusted Advisor 控制台中创建并下载另一个 JSON 报告。请参阅 创建组织视图报告 (p. 38)。本教程中，您必须使用 JSON 文件。
3. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
4. 选择 Amazon S3 存储桶，然后选择 ***folder1*** 文件夹。
5. 选择上一个 ***resources***`.json` 报告并选择 Delete（删除）。
6. 在 Delete objects（删除对象）页面中的 Permanently delete objects?（永久删除对象？）下输入 **`permanently delete`**，然后选择 Delete objects（删除对象）。
7. 在 S3 存储桶中，选择 Upload（上载），然后指定新报告。此操作会自动更新您的 Athena 表格和包含最新报告数据的 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 (p. 46)。

   Note

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

# 在 Amazon Trusted Advisor 中查看 Amazon Security Hub 控件

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

注意

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

  有关 Security Hub 类别的更多信息，请参阅控件类别。

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

主题



# 先决条件

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

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

Note

如果您已经满足了这些先决条件，则可以跳到 查看 Security Hub 检查结果 (p. 52)。

## 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。会员账户无需单独联系 Amazon Web Services Support 以启用此功能。但组织中的成员账户必须启用 Security Hub 后才能在 Trusted Advisor 查看器检查结果。

如果要为特定的成员账户禁用此集成，请参阅为 Amazon Organizations 账户禁用此功能 (p. 53)。

# 查看 Security Hub 检查结果

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

在 Trusted Advisor 查看 Security Hub 检查结果

1. 导航到 Trusted Advisor 控制台，然后选择 Security（安全）类别。
2. 在 Search by keyword（按关键词搜索）字段中，输入控件的名称或描述。

   Tip

   对于 Source（源），您可以选择 Amazon Security Hub 以筛选 Security Hub 控件。
3. 选择 Security Hub 控件名称以查看以下信息：

   - Description（描述）– 描述此控件将如何检查您的账户是否存在安全漏洞。

- Source（源）– 检查是来自 Amazon Trusted Advisor 还是 Amazon Security Hub。对于 Security Hub 控件，您可以找到控件 ID。
- Alert Criteria（提示标准）– 控件的状态。例如，假设 Security Hub 检测到重要问题，则状态可能为 Red: Critical or High（红色：严重或高）。
- Recommended Action（建议的操作）– 使用 Security Hub 文档链接查找修复问题的建议步骤。
- Security Hub resources（Security Hub 资源）– 您可以查找 Security Hub 在您账户中检测到问题的资源。

注意

- 您必须使用 Security Hub 才能将资源从检查结果中排除。目前不支持使用 Trusted Advisor 控制台从 Security Hub 控件中排除项目。有关更多信息，请参阅 设置检查结果的工作流状态。
- 组织视图功能支持与 Security Hub 集成。您可以查看整个组织的 Security Hub 控件检查结果，然后创建和下载报告。有关更多信息，请参阅 Amazon Trusted Advisor 的组织视图 (p. 37)。

# 刷新 Security Hub 检查结果

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

Note

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

# 从 Trusted Advisor 禁用 Security Hub

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

禁用 Security Hub 集成

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

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

## 为 Amazon Organizations 账户禁用此功能

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

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

# 问题排查

如果您遇到与此集成有关的问题，请参阅以下问题排查信息。

目录



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

确认您是否已完成以下步骤：

- 您拥有商业、Enterprise On-Ramp 或企业 Support 计划。
- 您已在与 Security Hub 相同的区域的 Amazon Config 中启用了资源录制。
- 您已启用了 Security Hub 并选择了 Amazon Foundational Security Best Practices v1.0.0（ 基础安全最佳实践 v1.0.0）安全标准。
- 来自 Security Hub 的新控件将在两到四周内添加为 Trusted Advisor 中的检查。请参阅说明 (p. 52)。

有关更多信息，请参见 先决条件 (p. 52)。

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

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

注意

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

## 我想禁用特定的 Security Hub 控件

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

您可以登录到 Security Hub 控制台并确认控件已启用还是已禁用。

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

有关更多信息，请参阅以下主题：

- 禁用和启用各个控件
- 禁用或启用安全标准

## 我想查找已被排除的 Security Hub 资源

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

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

## 我想为属于某个 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 Support。

## 我看到针对 Security Hub 检查的相同受影响资源有多个 Amazon Web Services 区域

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

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

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

## 我关闭了 Security Hub 或 Amazon Config 在一个区域

如果您使用 Amazon Config 停止资源记录或者在 Amazon Web Services 区域 中禁用 Security Hub，Trusted Advisor 不再接收该区域中任何控件的数据。您的 Security Hub 数据将在 90 天后从 Trusted Advisor 中删除。此时间范围仅为近似值且仅尽力而为，并不能保证达到。有关更多信息，请参阅禁用 Security Hub。

要为您的账户禁用此功能，请参阅 从 Trusted Advisor 禁用 Security Hub (p. 53)。

## 我仍然无法查看我的 Security Hub 检查结果

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

# 启用 Amazon Compute Optimizer 以执行 Trusted Advisor 检查

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。借助 Compute Optimizer，您可以查看 Trusted Advisor 检查中的相同建议。

您可以仅为您的 Amazon Web Services 账户启用此服务，也可以为属于 Amazon Organizations 中组织一部分的所有成员账户启用。有关更多信息，请参阅《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。而要在 Trusted Advisor 中查看下列检查的结果，您最长可能需要再等待 48 小时：

成本优化 (p. 60)

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

性能 (p. 62)

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

注意

- 这些检查的结果会每天自动刷新几次。不允许刷新请求。更改可能需要几个小时才能显示。您目前无法从这些检查中排除资源。
- Trusted Advisor 已经有利用率不足 Amazon EBS 卷和利用率过高 Amazon EBS 磁性卷检查。

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

## 相关信息

有关更多信息，请参阅以下主题：

- 《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
- 《适用于 Linux 实例的 Amazon EC2 用户指南》中的请求对 Amazon EBS 卷进行修改

# Amazon Trusted Advisor Priority 入门

Amazon Trusted Advisor Priority 目前为预览版，可能会发生变化。

Amazon Trusted Advisor Priority 可帮助您保护和优化账户，以更好地遵循 Amazon Web Services 最佳实践。借助 Amazon Trusted Advisor Priority，您的技术客户经理 (TAM) 可以主动监控您的 Amazon Web Services 账户，并在发现风险时创建优先建议。例如，如果 TAM 发现您没有为根账户激活多重验证 (MFA)，他们可以创建建议，以便以立即对根账户的 MFA 检查采取措施。您可以在 Trusted Advisor 控制台的 Amazon Trusted Advisor Priority 页面上将此风险视为优先建议。

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

- Amazon Web Services – 服务(Trusted Advisor、Amazon Security Hub 和 Amazon Well-Architected ) 会自动创建建议。接下来，TAM 会发送这些建议，以便它们出现在您的 Amazon Trusted Advisor Priority 中。

- 您的 TAM – 您的 TAM 可以针对他们在您的账户中发现的风险创建手动建议。

Amazon Trusted Advisor Priority 可帮助您专注于最重要的建议。您和您的 TAM 可以跟踪建议生命周期，从建议的创建到接受、解决或拒绝的时间。您可以使用 Amazon Trusted Advisor Priority 为您的 Amazon Organizations 中的所有成员账户查找建议。

注意

- 您必须拥有企业支持计划，并且必须登录组织的管理账户才能使用 Amazon Trusted Advisor Priority。
- 有关控制对 Amazon Trusted Advisor Priority 的访问的信息，请参阅 Amazon Trusted Advisor Priority 的 IAM policy 示例 (p. 108)。

主题



# 启用 Amazon Trusted Advisor Priority

请联系您的 TAM 并让他们为您启用此功能。您必须拥有企业支持计划并成为组织的管理账户所有者。

# 查看优先建议

一旦您的账户启用了 Amazon Trusted Advisor，您就可以查看贵组织的最新建议。

查看优先建议

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Amazon Trusted Advisor Priority 页面上，您可以查看以下内容：
   - 对于 Actions needed（所需操作），您可以查看正等待您做出响应或正在进行的建议的数量。
   - 对于 Overview（概述），您可以查看以下建议的数量：
     - 过去 90 天内被拒绝的建议
     - 过去 90 天内已解决的建议
     - 超过 30 天没有状态更新的建议
     - 建议的平均解决时间
3. 在 Prioritized recommendations（优先建议）部分中，您可以查看 TAM 为您优先考虑的建议。

   您可以根据以下条件筛选结果：

   - Recommendation（建议）— 输入关键字以按建议名称进行搜索。这可以是检查名称，也可以是 TAM 创建的自定义名称。
   - Status（状态）– 建议正在等待响应、正在进行、被拒绝还是已解决。
   - Source（来源）– 优先建议的源。建议可以来自某服务、由您的 TAM 手动添加，也可以来自计划的服务事件。
   - Category（类别）– 建议类别，例如安全或成本优化。

- Age（期限）– 当您的 TAM 与您分享建议时。

4. 请选择建议名称以详细了解其风险详细信息、受影响的资源以及为解决建议应采取的建议操作。然后，您可以接受 (p. 58)或拒绝 (p. 58)建议。

# 接受建议

优先建议将出现在 Amazon Trusted Advisor Priority 页面上。在此页面上，您可以接受建议。接受建议意味着您承认风险并将着手解决问题。

接受建议

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Amazon Trusted Advisor Priority 页面上，选择一个建议名称。
3. 在建议详细信息页面上，查看有关此建议的信息以及组织内受影响的资源。
4. 选择 Accept (接受)。
5. 在 Accept recommendation（接受建议）对话框中，输入您的姓名和职务，然后选择 Accept（接受）。

   建议状态将变为 In progress（正在进行）。
6. 按照建议详细信息中的步骤修复问题。然后，您可以解决建议。有关更多信息，请参阅 解决建议 (p. 58)。

# 拒绝建议

您也可以拒绝建议，这意味着您承认风险，但此时选择不修复问题。如果您认为这不是风险，或者问题与您的账户无关，则可以拒绝建议。

拒绝建议

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Amazon Trusted Advisor Priority 页面上，选择一个建议名称。
3. 在建议详细信息页面上，查看有关此建议的信息以及组织内受影响的资源。
4. 如果此风险对您的账户来说不是问题，请选择 Reject（拒绝）。
5. 在 Reject（拒绝）对话框中，指定您是否承认该问题但不会修复它，或者该问题是否对您的账户或组织没有风险。
6. 对于 Reason for rejection（拒绝原因），请输入您选择不解决此问题的原因。
7. 输入您的姓名和职务。
8. 选择 Reject (拒绝)。

   建议状态将变为 Rejected（已拒绝）。您的 TAM 也会收到通知，获悉您拒绝了他们的建议。

# 解决建议

修复问题后，您可以解决建议。

> Note
>
> 如果不打算修复问题，您必须先接受该建议，然后才能解决问题。

解决建议

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。

2. 在 Amazon Trusted Advisor Priority 页面上，选择建议，然后选择 Resolve（解决）。
3. 在 Resolve recommendation（解决建议）对话框中，输入您的姓名和职务。

   选择 Resolve（解决）。

   建议状态将变为 Resolved（已解决）。您的 TAM 也会收到通知，获悉您已解决其建议。

## 下载建议详细信息

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

> Note
>
> 目前，Amazon Trusted Advisor Priority 一次只支持下载一个建议。

下载建议

1. 登录到 Trusted Advisor 控制台，网址为 https://console.aws.amazon.com/trustedadvisor/home。
2. 在 Amazon Trusted Advisor Priority 页面上，选择建议，然后选择 Download（下载）。

## 禁用 Amazon Trusted Advisor Priority

请联系您的 TAM 并让他们为您禁用此功能。删除后，优先建议将不会出现在您的控制台中。

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

# Amazon Trusted Advisor 检查引用

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

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

- 使用 Trusted Advisor 即 Web 服务 (p. 34)

> Note
>
> 如果您使用的是基本支持或开发人员支持计划，则可以使用 Trusted Advisor 控制台访问 Service Limits (p. 76) 类别中的所有检查和安全类别中的以下检查：
>
> - Amazon S3 存储桶权限 (p. 67)
> - 安全组 – 不受限制的特定端口 (p. 69)

> Note
>
> 您可以在中国区域中使用以下检查。

检查类别

- 成本优化 (p. 60)

# 成本优化

您可以使用以下成本优化类别检查。

检查名称



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

描述

检查过去 24 小时内运行 SQL Server 的 Amazon Elastic Compute Cloud（Amazon EC2）实例。SQL Server 数据库对每个实例都有计算容量限制。使用 SQL Server Standard 版的实例最多可以使用 48 个 vCPU。使用 SQL Server Web 版的实例最多可以使用 32 个 vCPU。如果实例超过此 vCPU 限制，则此检查会提示您。

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

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

Note

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

检查 ID

```
Qsdfp3A4L1
```

提醒条件

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

建议的操作

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

其他资源

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

报告列

- 状态
- Region
- 实例 ID

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

## 闲置的负载均衡器

描述

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

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

检查 ID

`hjLMh88uM8`

提醒条件

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

建议的操作

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

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

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

其他资源

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

报告列

- Region
- 负载均衡器名称
- Reason
- 预估每月节省

## 未关联的弹性 IP 地址

描述

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

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

检查 ID

`Z4AUBRNSmz`

提醒条件

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

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 EBS 预置 IOPS (SSD) 卷附件配置 (p. 62)
- 高使用率 Amazon EC2 实例 (p. 63)
- 应用于实例的大量 EC2 安全组规则 (p. 63)
- EC2 安全组中的大量规则 (p. 64)
- 过度使用的 Amazon EBS 磁性介质卷 (p. 65)

## Amazon EBS 预置 IOPS (SSD) 卷附件配置

描述

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

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

检查 ID

`PPkZrjsH2q`

提醒条件

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

建议的操作

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

其他资源

- Amazon EBS 卷类型

- Amazon EBS 卷性能

报告列

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

## 高使用率 Amazon EC2 实例

描述

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

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

检查 ID

`ZRxQlPsb6c`

提醒条件

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

建议的操作

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

其他资源

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

报告列

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

## 应用于实例的大量 EC2 安全组规则

描述

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

检查 ID

`j3DFqYTe29`

提醒条件

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

建议的操作

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

其他资源

Amazon EC2 安全组

报告列

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

## EC2 安全组中的大量规则

描述

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

如果安全组具有大量规则，则性能可能会降低。

检查 ID

`tfg86AVHAZ`

提醒条件

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

建议的操作

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

其他资源

Amazon EC2 安全组

报告列

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

## 过度使用的 Amazon EBS 磁性介质卷

描述

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

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

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

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

检查 ID

`k3J2hns32g`

提醒条件

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

建议的操作

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

其他资源

Amazon Elastic Block Store (Amazon EBS)

报告列

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

Note

如果您的账户启用了 Amazon Compute Optimizer，我们建议您改用 Amazon EBS 预调配不足卷检查。有关更多信息，请参阅启用 Amazon Compute Optimizer 以执行 Trusted Advisor 检查 (p. 55)。

# 安全性

您可以使用以下安全类别检查。

Note

如果为您的 Amazon Web Services 账户 启用 Security Hub，则可以在 Trusted Advisor 控制台中查看检查结果。有关信息，请参阅 在 Amazon Trusted Advisor 中查看 Amazon Security Hub 控件 (p. 51)。

您可以查看 Amazon 基础安全最佳实践安全标准中的所有控件，但具有 Category: Recover > Resilience（类别：恢复 > 弹性）的控件除外。有关受支持控件的列表，请参阅《Amazon Security Hub 用户指南》中的 Amazon基础安全最佳实践控件。

检查名称



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

描述

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

Note

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

检查 ID

```
Qsdfp3A4L3
```

提醒条件

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

建议的操作

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

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

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

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

其他资源

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

报告列

- 状态
- Region
- 实例 ID

- SQL Server 版本
- 支持周期
- 停止支持
- 上次更新时间

## Amazon S3 存储桶权限

描述

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

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

检查 ID

`Pfx0RwqBli`

提醒条件

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

建议的操作

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

其他资源

管理对 Amazon S3 资源的访问权限

报告列

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

## ELB 侦听器安全

描述

检查负载平衡器与未使用推荐的安全配置进行加密通信的侦听器。Amazon 建议使用安全协议（HTTPS 或 SSL）、最新的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，客户端和负载均衡器之间的请求将被加密，从而创建更安全的环境。Elastic Load Balancing 提供预定义的安全策略，其密码和协议符合 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

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

建议的操作

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

将负载均衡器的预定义 SSL 安全策略升级到最新版本。

只使用推荐的密码和协议。

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

其他资源

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

报告列

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

## ELB 安全组

描述

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

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

检查 ID

`xSqX82fQu`

提醒条件

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

建议的操作

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

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

其他资源

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

报告列

- 状态
- Region
- 负载均衡器名称
- 安全组 ID
- Reason

## IAM 密码策略

描述

检查账户的密码策略，并在未启用密码策略或未启用密码内容要求时发出警告。

密码内容要求通过强制创建强用户密码提高了 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

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

建议的操作

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

其他资源

管理密码

报告列

- 密码策略
- 大写
- 小写
- 数字
- 非字母数字

## 安全组 – 不受限制的特定端口

描述

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

不受限制的访问增加了恶意活动（黑客攻击、拒绝服务攻击、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 地址的入站规则。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，并且可能会安全地被忽略或被排除在外。有关更多信息，请参阅 Trusted Advisor 常见问题。

检查 ID

`HCP4007jGY`

提醒条件

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

建议的操作

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

其他资源

- Amazon EC2 安全组

  TCP 和 UDP 端口号列表
- 无类域间路由

报告列

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

## 安全组 – 不受限制的访问

描述

检查安全组是否存在允许不受限制地访问资源的规则。

不受限制的访问增加了恶意活动（黑客攻击、拒绝服务攻击、数据丢失）的机会。

Note

此检查仅评估您创建的安全组及其 IPv4 地址的入站规则。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，并且可能会安全地被忽略或被排除在外。有关更多信息，请参阅 Trusted Advisor 常见问题。

检查 ID

`1iG5NDGVre`

提醒条件

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

建议的操作

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

其他资源

- Amazon EC2 安全组
- 无类域间路由

报告列

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

# 容错能力

您可以使用以下容错类别检查。

检查名称

- Amazon EBS 快照 (p. 71)
- Amazon RDS 备份 (p. 72)
- Amazon S3 存储桶日志记录 (p. 72)
- Auto Scaling 组运行状况检查 (p. 73)
- Auto Scaling 组资源 (p. 74)
- ELB Connection Draining (p. 75)
- 负载均衡器优化 (p. 75)

## Amazon EBS 快照

描述

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

即使复制了 Amazon EBS 卷，也可能会发生故障。快照将保留到 Amazon Simple Storage Service (Amazon S3) 中以实现持久存储和时间点恢复。

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。

建议的操作

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

其他资源

Amazon Elastic Block Store (Amazon EBS)

报告列

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

## Amazon RDS 备份

描述

检查 Amazon RDS 数据库实例的自动备份。

默认情况下，启用备份，保留期为一天。备份可以降低意外数据丢失的风险，并允许进行时间点恢复。

检查 ID

`opQPADkZvH`

提醒条件

红色：数据库实例将备份保留期设置为 0 天。

建议的操作

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

其他资源

Amazon RDS 入门

报告列

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

## Amazon S3 存储桶日志记录

描述

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

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

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

检查 ID

`BueAdJ7NrP`

提醒条件

- 黄色：存储桶没有启用服务器访问日志记录。
- 黄色：目标存储桶权限不包括根账户，所以 Trusted Advisor 无法对其进行检查。
- 红色：目标存储桶不存在。
- 红色：目标存储桶和源存储桶的拥有者不同。
- 红色：日志提交者没有目标存储桶的写入权限。

建议的操作

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

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

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

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

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

其他资源

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

报告列

- 状态
- 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

描述

检查 Auto Scaling 组的运行状况检查配置。

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

检查 ID

`CLOG40CDO8`

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。

建议的操作

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

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

其他资源

Amazon EC2 Auto Scaling 用户指南

报告列

- 状态
- 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

描述

检查与启动配置和 Auto Scaling 组关联的资源的可用性。

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

检查 ID

`8CNsSllI5v`

提醒条件

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

建议的操作

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

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

其他资源

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

报告列

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

## ELB Connection Draining

描述

检查没有启用连接耗尽的负载均衡器

当未启用连接耗尽并且您从负载均衡器取消注册 Amazon EC2 实例时，负载均衡器将停止将流量路由到该实例并关闭连接。启用连接耗尽后，负载均衡器将停止向已取消注册的实例发送新请求，但会保持连接打开以提供活动请求。

检查 ID

`7qGXsKIUw`

提醒条件

黄色：负载均衡器未启用连接耗尽。

建议的操作

为负载均衡器启用连接耗尽。有关更多信息，请参阅连接耗尽和为负载均衡器启用或禁用连接耗尽。

其他资源

Elastic Load Balancing 概念

报告列

- 状态
- Region
- 负载均衡器名称
- Reason

## 负载均衡器优化

描述

检查您的负载均衡器配置。

为了帮助在使用 Elastic Load Balancing 时提高 Amazon Elastic Compute Cloud (Amazon EC2) 的容错能力级别，我们建议在一个区域的多个可用区中运行相同数量的实例。配置的负载均衡器会产生费用，因此这也是成本优化检查。

检查 ID

`iqdCTZKCUp`

提醒条件

- 黄色：已为单个可用区启用负载均衡器。
- 黄色：已为没有活跃实例的可用区启用负载均衡器。
- 黄色：在负载均衡器注册的 Amazon EC2 实例未在可用区之间平均分配。（使用的可用区的实例数最多与最少之间相差大于 1 且相差比最高数大 20%。）

建议的操作

确保负载均衡器指向至少两个可用区内活跃并运行正常的实例。有关更多信息，请参见添加可用区。

如果负载均衡器配置的对象是没有正常运行实例的可用区，或者可用区之间的实例分配不均衡，请确定所有可用区是否都是必要的。删除所有不必要的可用区，并确保实例在其余可用区之间均衡分配。有关更多信息，请参阅删除可用区。

其他资源

- 可用区和区域
- 管理负载均衡器
- 评估 Elastic Load Balancing 的最佳实践

报告列

- 状态
- 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

# Service Limits

请参阅以下有关服务限制（也称为配额）类别的检查。

此类别中的所有检查都有以下描述：

提醒条件

- 黄色：已达到限制的 80%。
- 红色：已达到限制的 100%。
- 蓝色：Trusted Advisor 无法检索一个或多个 Amazon Web Services 区域 中的使用率或限制。

建议的操作

如果您预计超出服务限制，请直接从服务限额控制台请求增加。如果服务限额还不支持您的服务，则可以在支持中心创建未结支持案例。

报告列

- 状态
- 服务
- 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

描述

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

描述

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

描述

检查使用量是否超过 EBS 活动快照配额的 80%。

检查 ID

`eI7KK0l7J9`

其他资源

Amazon EBS 限制

## EBS 通用型 SSD (gp2) 卷存储

描述

检查使用量是否超过 EBS 通用型 SSD (gp2) 卷存储配额的 80%。

检查 ID

`dH7RR0l6J9`

其他资源

Amazon EBS 限制

## EBS 通用型 SSD (gp3) 卷存储

描述

检查使用量是否超过 EBS 通用型 SSD (gp3) 卷存储配额的 80%。

检查 ID

`dH7RR0l6J3`

其他资源

Amazon EBS 限制

## EBS 磁介质（标准）卷存储

描述

检查使用量是否超过 EBS 磁性介质（标准）卷存储配额的 80%。

检查 ID

`cG7HH0l7J9`

其他资源

Amazon EBS 限制

## EBS 预置 IOPS (SSD) 卷聚合 IOPS

描述

检查使用量是否超过 EBS 预置 IOPS (SSD) 卷聚合 IOPS 配额的 80%。

检查 ID

`tV7YY0l7J9`

其他资源

Amazon EBS 限制

## EBS 预置 IOPS SSD (io1) 卷存储

描述

检查使用量是否超过 EBS 预置 IOPS SSD (io1) 卷存储配额的 80%。

检查 ID

`gI7MM0l7J9`

其他资源

Amazon EBS 限制

## EC2 预留实例租赁

描述

检查使用量是否超过 EC2 预留实例租赁配额的 80%。

检查 ID

`iH7PP0l7J9`

其他资源

Amazon EC2 配额

## EC2-VPC 弹性 IP 地址

描述

检查使用量是否超过 EC2-VPC 弹性 IP 地址配额的 80%。

检查 ID

`lN7RR0l7J9`

其他资源

VPC 弹性 IP 配额

## ELB Classic Load Balancer

描述

检查使用量是否超过 ELB Classic Load Balancer 配额的 80%。

检查 ID

`iK7OO0l7J9`

其他资源

Elastic Load Balancing 配额

## VPC

描述

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

描述

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 Amazon Trusted Advisor 检查的日志

请参阅以下主题以了解对 Trusted Advisor 检查的最近更改。

> **Note**
>
> 如果您使用 Trusted Advisor 控制台或 Amazon Web Services Support API，删除的检查不会出现在检查结果中。如果您使用任何已删除的检查，例如在 Amazon Web Services Support API 操作或您的代码中指定检查 ID，您必须删除这些检查以避免 API 调用错误。

有关可用检查的更多信息，请参阅 Amazon Trusted Advisor 检查引用 (p. 59)。

## 已将 Security Hub 检查添加到 Trusted Advisor

截至 2022 年 6 月 23 日，Trusted Advisor 仅支持 2022 年 4 月 7 日之前可用的 Security Hub 控件。此版本支持 Amazon 基础安全最佳实践安全标准中的所有控件，但 Category: Recover > Resilience（类别：恢复 > 弹性）中的控件除外。有关更多信息，请参阅在 Amazon Trusted Advisor 中查看 Amazon Security Hub 控件 (p. 51)。

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

## 增加了来自 Amazon Compute Optimizer 的检查

Trusted Advisor 于 2022 年 5 月 4 日增加了以下检查。

| 检查名称 | 检查类别 | 检查 ID |
| --- | --- | --- |
| Amazon EBS 过度预调配卷 | 成本优化 | `COr6dfpM03` |
| Amazon EBS 预调配不足的卷 | 性能 | `COr6dfpM04` |
| 相比内存大小过度预调配的 Amazon Lambda 函数 | 成本优化 | `COr6dfpM05` |
| 相比内存大小而言预调配不足的 Amazon Lambda 函数 | 性能 | `COr6dfpM06` |

您必须为您的 Amazon Web Services 账户 中启用 Compute Optimizer，才能让这些检查从您的 Lambda 和 Amazon EBS 资源接收数据。有关更多信息，请参阅启用 Amazon Compute Optimizer 以执行 Trusted Advisor 检查 (p. 55)。

# 更新了对 Amazon Direct Connect 的检查

Trusted Advisor 于 2022 年 3 月 29 日增加了以下检查。

| 检查名称 | 检查类别 | 检查 ID |
| --- | --- | --- |
| 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，只有您调查的 Trusted Advisor 建议的资源才会显示在此表中。这些资源旁边拥有一个警告图标 ( )。

# 更新了 Amazon OpenSearch Service 的检查名称

Trusted Advisor 于 2021 年 9 月 8 日将 Amazon Elasticsearch Reserved Instance Optimization 检查名称更新为 Amazon OpenSearch Service Reserved Instance Optimization。

Amazon OpenSearch Service 是 Amazon Elasticsearch Service 的后继者。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 Service 预留实例优化 | 成本优化 | `7ujm6yhn5t` |

Note

如果您将 Trusted Advisor 用于 Amazon CloudWatch 指标，此检查的指标名称也会更新。有关更多信息，请参阅创建 Amazon CloudWatch 告警以监控 Amazon Trusted Advisor 指标 (p. 125)。

# 增加了 Amazon Elastic Block Store 卷存储的检查

Trusted Advisor 于 2021 年 6 月 8 日增加了以下检查。

| 检查名称 | 检查类别 | 检查 ID |
| --- | --- | --- |
| EBS 通用型 SSD (gp3) 卷存储 | Service Limits | `dH7RR0l6J3` |

# 增加了 Amazon Lambda 的检查

Trusted Advisor 于 2021 年 3 月 8 日增加了以下检查。

| 检查名称 | 检查类别 | 检查 ID |
| --- | --- | --- |
| 过度超时的 Amazon Lambda 函数 | 成本优化 | `L4dfs2Q3C3` |
| 具有高误差率的 Amazon Lambda 函数 | 成本优化 | `L4dfs2Q3C2` |
| 使用弃用运行时的 Amazon Lambda 函数 | 安全性 | `L4dfs2Q4C5` |
| 无多可用区冗余的 Amazon Lambda VPC 支持的函数 | 容错能力 | `L4dfs2Q4C6` |

有关如何将这些检查用于 Lambda 的更多信息，请参阅 Amazon Lambda 开发人员指南中的查看建议的示例 Amazon Trusted Advisor 工作流。

# Trusted Advisor 检查删除

Trusted Advisor 于 2021 年 3 月 8 日删除了中国（北京）区域的以下检查。

| 检查名称 | 检查类别 | 检查 ID |
| --- | --- | --- |
| EC2 弹性 IP 地址 | Service Limits | `aW9HH0l8J6` |

# 更新了 Amazon Elastic Block Store 的检查

Trusted Advisor 于 2021 年 3 月 5 日在以下检查中将 Amazon EBS 卷的单位从 GiB 更新到 TiB。

> **Note**
>
> 如果您将 Trusted Advisor 用于 Amazon CloudWatch 指标，这五项检查的指标名称也会更新。有关更多信息，请参阅创建 Amazon CloudWatch 告警以监控 Amazon Trusted Advisor 指标 (p. 125)。

| 检查名称 | 检查类别 | 检查 ID | 更新了 ServiceLimit 的 CloudWatch 指标 |
| --- | --- | --- | --- |
| EBS 冷 HDD (sc1) 卷存储 | Service Limits | `gH5CC0e3J9` | 冷 HDD (sc1) 卷存储 (TiB) |
| EBS 通用型 SSD (gp2) 卷存储 | Service Limits | `dH7RR0l6J9` | 通用型 SSD (gp2) 卷存储 (TiB) |
| EBS 磁介质（标准）卷存储 | Service Limits | `cG7HH0l7J9` | 磁介质（标准）卷存储 (TiB) |
| EBS 预置 IOPS SSD (io1) 卷存储 | Service Limits | `gI7MM0l7J9` | 预置 IOPS (SSD) 存储 (TiB) |

| 检查名称 | 检查类别 | 检查 ID | 更新了 ServiceLimit 的 CloudWatch 指标 |
| --- | --- | --- | --- |
| EBS 吞吐量优化型 HDD (st1) 卷存储 | Service Limits | wH7DD0l3J9 | 吞吐量优化型 HDD (st1) 卷存储 (TiB) |

# Trusted Advisor 检查删除

Note

Trusted Advisor 于 2020 年 11 月 18 日删除了以下检查。

| 2020 年 11 月 18 日删除的检查 | 检查类别 | 检查 ID |
| --- | --- | --- |
| 适用于 EC2 Windows 实例的 EC2Config 服务 | 容错能力 | V77iOLlBqz |
| 适用于 EC2 Windows 实例的 ENA 驱动程序版本 | 容错能力 | TyfdMXG69d |
| 适用于 EC2 Windows 实例的 NVMe 驱动程序版本 | 容错能力 | yHAGQJV9K5 |
| 适用于 EC2 Windows 实例的 PV 驱动程序版本 | 容错能力 | Wnwm9Il5bG |
| EBS 活动卷 | Service Limits | fH7LL0l7J9 |

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

您可以通过使用 Amazon Systems Manager Distributor、其他第三方工具监控 Amazon EC2 实例并验证它们是否处于最新状态，或编写自己的脚本以返回 Windows Management Instrumentation (WMI) 的驱动程序信息。

# Trusted Advisor 检查删除

Trusted Advisor 于 2020 年 2 月 18 日删除了以下检查。

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

# Amazon Web Services Support 中的安全性

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是Amazon和您的共同责任。责任共担模型将其描述为云的安全性和云中的安全性：

- 云的安全性 – Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础设施。Amazon 还向您提供可安全使用的服务。作为 Amazon 合规性计划的一部分，第三方审计人员将定期测试和验证安全措施的有效性。要了解适用于 Amazon Web Services Support 的合规性计划，请参阅合规性计划范围内的 Amazon Web Services 服务。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Amazon Web Services Support 时应用责任共担模型 以下主题说明如何配置 Amazon Web Services Support 以实现您的安全性和合规性目标。您还会了解如何使用其他 Amazon Web Services 以帮助您监控和保护 Amazon Web Services Support 资源。

主题



## Amazon Web Services Support 中的数据保护

Amazon责任共担模式适用于 Amazon Web Services Support 中的数据保护。如该模式中所述，Amazon 负责保护运行所有 Amazon Web Services 云 的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 Amazon Web Services 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 Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 Amazon 资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 Amazon CloudTrail 设置 API 和用户活动日志记录。
- 使用 Amazon 加密解决方案以及 Amazon 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Simple Storage Service（Amazon S3）中的个人数据。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 终端节点。有关可用的 FIPS 终端节点的更多信息，请参阅《美国联邦信息处理标准 (FIPS) 第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（例如您客户的电子邮件地址）放入标签或自由格式字段（例如名称字段）。这包括使用控制台、API、Amazon CLI 或 Amazon SDK 处理 Amazon Web Services Support 或其他 Amazon 服务时。您在用于名称的标签或自由格式字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，我们强烈建议您不要在 URL 中包含凭证信息来验证您对该服务器的请求。

# 适用于 Amazon Web Services Support 的 Identity and Access Management

Amazon Identity and Access Management (IAM) 是一项 Amazon Web Service，可以帮助管理员安全地控制对 Amazon 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）来使用 Amazon Web Services Support 资源。IAM 是一项无需额外费用即可使用的 Amazon Web Service。

主题



## Audience

使用 Amazon Identity and Access Management (IAM) 的方式因您可以在 Amazon Web Services Support 中执行的操作而异。

服务用户 – 如果您使用 Amazon Web Services Support 服务来完成任务，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Amazon Web Services Support 功能来完成工作时，您可能需要额外权限。了解如何管理访问权限可帮助您向管理员请求适合的权限。如果您无法访问 Amazon Web Services Support 中的功能，请参阅 对 Amazon Web Services Support 身份和访问进行故障排除 (p. 109)。

服务管理员 – 如果您在公司负责管理 Amazon Web Services Support 资源，则您可能具有 Amazon Web Services Support 的完全访问权限。您有责任确定您的员工应访问哪些 Amazon Web Services Support 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与 Amazon Web Services Support 搭配使用的更多信息，请参阅Amazon Web Services Support 如何与 IAM 协同工作 (p. 88)。

IAM 管理员 – 如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 Amazon Web Services Support 的访问权限的详细信息。要查看您可在 IAM 中使用的 Amazon Web Services Support 基于身份的策略示例，请参阅 Amazon Web Services Support 基于身份的策略示例 (p. 89)。

## 使用身份进行身份验证

身份验证是您使用身份凭证登录 Amazon 的方法。有关使用Amazon Web Services Management Console 登录的更多信息，请参阅 IAM 用户指南中的以 IAM 用户或根用户身份登录Amazon Web Services Management Console。

您必须作为Amazon Web Services 账户根用户、IAM 用户或代入 IAM 角色以进行身份验证（登录到 Amazon）。您还可以使用公司的单一登录身份验证方法，甚至使用 Google 或 Facebook 登录。在这些情况

下，您的管理员以前使用 IAM 角色设置了联合身份验证。在您使用来自其它公司的凭证访问 Amazon 时，您间接地代入了角色。

要直接登录到Amazon Web Services Management Console，请将密码与根用户电子邮件地址或 IAM 用户名一起使用。您可以使用根用户或 IAM 用户访问密钥以编程方式访问 Amazon。Amazon 提供了 SDK 和命令行工具，可使用您的凭证对您的请求进行加密签名。如果您不使用 Amazon 工具，则必须自行对请求签名。使用 Signature Version 4（用于对入站 API 请求进行验证的协议）完成此操作。有关验证请求的更多信息，请参阅《Amazon 一般参考》中的 Signature Version 4 签名流程。

无论使用何种身份验证方法，您可能还需要提供其它安全信息。例如，Amazon 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《IAM 用户指南》中的在 Amazon 中使用多重身份验证 (MFA)。

## Amazon 账户根用户

当您首次创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services和资源有完全访问权限的单点登录身份。此身份称为Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不使用根用户执行日常任务，即使是管理任务。相反，请遵循仅使用根用户创建您的第一个 IAM 用户的最佳实践。然后请妥善保存根用户凭证，仅用它们执行少数账户和服务管理任务。

## IAM 用户和组

IAM 用户是Amazon Web Services 账户内对某个人员或应用程序具有特定权限的一个身份。IAM 用户可能具有长期凭证，例如用户名和密码或一组访问密钥。要了解如何生成访问密钥，请参阅 IAM 用户指南 中的管理 IAM 用户的访问密钥。为 IAM 用户生成访问密钥时，请确保查看并安全保存密钥对。您以后无法找回秘密访问密钥，而是必须生成新的访问密钥对。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。

## IAM 角色

IAM 角色是Amazon Web Services 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 Amazon Web Services Management Console 中暂时代入 IAM 角色。您可以调用 Amazon CLI 或 Amazon API 操作或使用自定义 URL 以代入角色。有关使用角色的方法的更多信息，请参阅 IAM 用户指南 中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 临时 IAM 用户权限 – IAM 用户可以代入 IAM 角色，以暂时获得不同的权限以执行特定的任务。
- 联合身份用户访问 – 您可以不创建 IAM 用户，而是使用来自 Amazon Directory Service、您的企业用户目录或 Web 身份提供商的现有身份。这些用户被称为联合用户。在通过身份提供商请求访问权限时，Amazon 将为联合身份用户分配角色。有关联合身份用户的更多信息，请参阅 IAM 用户指南 中的联合身份用户和角色。
- 跨账户访问 – 您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 Amazon Web Services，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 – 某些 Amazon Web Services使用其它 Amazon Web Services中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。

  - 主体权限 – 当您使用 IAM 用户或角色在 Amazon 中执行操作时，您将被视为主体。策略向主体授予权限。使用某些服务时，您可能会执行一个操作，此操作然后在不同服务中触发另一个操作。在这种情况下，您必须具有执行这两个操作的权限。要查看某个操作是否需要策略中的其它相关操作，请参阅服务授权参考中的 Amazon Web Services Support 的操作、资源和条件键。
  - 服务角色 – 服务角色是服务代表您在您的账户中执行操作而担任的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 Amazon Web Service 委派权限的角色。
  - 服务相关角色 – 服务相关角色是与 Amazon Web Service关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅 IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

# 使用策略管理访问

您将创建策略并将其附加到 IAM 身份或Amazon资源，以便控制Amazon中的访问。策略是Amazon中的对象；在与标识或资源相关联时，策略定义它们的权限。您可以通过 root 用户或 IAM 用户身份登录，也可以代入 IAM 角色。随后，当您提出请求时，Amazon会评估相关的基于身份或基于资源的策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 Amazon 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南 中的 JSON 策略概览。

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么条件 下执行。

每个 IAM 实体（用户或角色）最初没有任何权限。换言之，预设情况下，用户什么都不能做，甚至不能更改他们自己的密码。要为用户授予执行某些操作的权限，管理员必须将权限策略附加到用户。或者，管理员可以将用户添加到具有预期权限的组中。当管理员为某个组授予访问权限时，该组内的全部用户都会获得这些访问权限。

IAM policy 定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。具有该策略的用户可以从 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 获取角色信息。

## 基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM policy。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管式策略是可以附加到Amazon Web Services 账户中的多个用户、组和角色的独立策略。托管式策略包括 Amazon 托管式策略和客户托管式策略。要了解如何在托管式策略和内联策略之间进行选择，请参阅 IAM 用户指南 中的在托管式策略与内联策略之间进行选择。

## 其它策略类型

Amazon 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界 – 权限边界是一个高级功能，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体的基于身份的策略及其权限边界的交集。在

`Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。

- 服务控制策略 (SCP) – SCP 是 JSON 策略，指定了组织或组织单位 (OU) 在 Amazon Organizations 中的最大权限。Amazon Organizations 服务可以分组和集中管理您的企业拥有的多个 Amazon Web Services 账户 账户。如果在组织内启用了所有功能，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中实体的权限，包括每个 Amazon Web Services 账户 根用户。有关 Organizations 和 SCP 的更多信息，请参阅 Amazon Organizations 用户指南中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合身份用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

## 多个策略类型

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

# Amazon Web Services Support 如何与 IAM 协同工作

在使用 IAM 管理对 Amazon Web Services Support 的访问之前，您应了解哪些 IAM 功能可与 Amazon Web Services Support 结合使用。要大致了解 Amazon Web Services Support 和其他 Amazon 服务如何与 IAM 一起使用，请参阅 IAM 用户指南中的与 IAM 一起使用的 Amazon 服务。

主题



## Amazon Web Services Support 基于身份的策略

使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源，以及指定在什么条件下允许或拒绝操作。Amazon Web Services Support 支持特定的操作。要了解您在 JSON 策略中使用的元素，请参阅 IAM 用户指南 中的 IAM JSON 策略元素参考。

### 操作

管理员可以使用 Amazon JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体 可以对什么资源 执行操作，以及在什么 条件 下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 Amazon API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行相关操作的权限。

Amazon Web Services Support 中的策略操作在操作前使用以下前缀：`support:`。例如，要授予某人使用 Amazon EC2 `RunInstances` API 操作运行 Amazon EC2 实例的权限，您应将 `ec2:RunInstances` 操作纳入其策略。策略语句必须包括 `Action` 或 `NotAction` 元素。Amazon Web Services Support 定义了自己的一组操作，这些操作描述了可使用该服务执行的任务。

要在单个语句中指定多项操作，请使用逗号将它们隔开，如下所示：

```
"Action": [
      "ec2:action1",
      "ec2:action2"
```

您也可以使用通配符 (*) 指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，包括以下操作：

```
"Action": "ec2:Describe*"
```

要查看 Amazon Web Services Support 操作列表，请参阅 IAM 用户指南中的 Amazon Web Services Support 定义的操作。

### 示例

要查看 Amazon Web Services Support 基于身份的策略的示例，请参阅 Amazon Web Services Support 基于身份的策略示例 (p. 89)。

## Amazon Web Services Support IAM 角色

IAM 角色是 Amazon 账户中具有特定权限的实体。

### 将临时凭证用于 Amazon Web Services Support

您可以使用临时凭证进行联合身份登录，担任 IAM 角色或担任跨账户角色。您可以通过调用 Amazon STS API 操作（如 AssumeRole 或 GetFederationToken）获得临时安全凭证。

Amazon Web Services Support 支持使用临时凭证。

### 服务相关角色

服务相关角色允许 Amazon 服务访问其它服务中的资源以代表您完成操作。服务相关角色显示在您的 IAM 账户中，并归该服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

Amazon Web Services Support 支持服务相关角色。有关创建或管理 Amazon Web Services Support 服务相关角色的详细信息，请参阅 将服务相关角色用于 Amazon Web Services Support (p. 91)。

### 服务角色

此功能允许服务代表您担任服务角色。此角色允许服务访问其它服务中的资源以代表您完成操作。服务角色显示在您的 IAM 账户中，并归该账户所有。这意味着，IAM 管理员可以更改该角色的权限。但是，这样做可能会中断服务的功能。

Amazon Web Services Support 支持服务角色。

# Amazon Web Services Support 基于身份的策略示例

预设情况下，IAM 用户和角色没有创建或修改 Amazon Web Services Support 资源的权限。它们还无法使用 Amazon Web Services Management Console、Amazon CLI 或 Amazon API 执行任务。IAM 管理员必须创建 IAM policy，以便为用户和角色授予权限以对所需的指定资源执行特定的 API 操作。然后，管理员必须将这些策略附加到需要这些权限的 IAM 用户或组。

要了解如何使用这些示例 JSON 策略文档创建 IAM 基于身份的策略，请参阅 IAM 用户指南中的在 JSON 选项卡上创建策略。

主题



## 策略最佳实践

基于身份的策略非常强大。它们确定某个人是否可以创建、访问或删除您账户中的 Amazon Web Services Support 资源。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 Amazon 托管式策略 – 要快速开始使用 Amazon Web Services Support，请使用 Amazon 托管式策略，为您的员工提供他们所需的权限。这些策略已在您的账户中提供，并由 Amazon 维护和更新。有关更多信息，请参阅 IAM 用户指南中的开始使用 Amazon 托管式策略中的权限。
- 授予最低权限 – 创建自定义策略时，仅授予执行任务所需的许可。最开始只授予最低权限，然后根据需要授予其它权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说更为安全。有关更多信息，请参阅《IAM 用户指南》中的授予最低权限。
- 为敏感操作启用 MFA – 为增强安全性，要求 IAM 用户使用多重身份验证 (MFA) 来访问敏感资源或 API 操作。要了解更多信息，请参阅 IAM 用户指南中的在 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 Support 控制台

要访问 Amazon Web Services Support 控制台，您必须拥有一组最低的权限。这些权限必须允许您列出和查看有关您的 Amazon 账户中的 Amazon Web Services Support 资源的详细信息。如果您创建的基于身份的策略比所需的最低权限更严格，则无法为具有该策略的实体（IAM 用户或角色）正常运行控制台。

要确保这些实体仍可使用 Amazon Web Services Support 控制台，也可向实体附加以下 Amazon 托管策略。有关更多信息，请参阅 IAM 用户指南中的为用户添加权限：

对于只需要调用 Amazon CLI 或 Amazon API 的用户，无需为其提供最低控制台权限。相反，只允许访问与您尝试执行的 API 操作相匹配的操作。

## 允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上完成此操作或者以编程方式使用 Amazon CLI 或 Amazon API 所需的权限。

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

```
    ]
}
```

# 使用服务相关角色

Amazon Web Services Support 和 Amazon Trusted Advisor 使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 Amazon Web Services Support 和 Trusted Advisor 直接关联的独特 IAM 角色。在每个案例中，服务相关角色是预定义的角色。此角色包含 Amazon Web Services Support 或 Trusted Advisor 代表您调用其他 Amazon 服务所需的一切权限。以下主题说明了服务相关角色的功能以及如何在 Amazon Web Services Support 和 Trusted Advisor 中使用这些角色。

主题



## 将服务相关角色用于 Amazon Web Services Support

Amazon Web Services Support 工具通过 API 调用来收集有关 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核性，Amazon Web Services Support 现在使用 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 Support 的独特 IAM 角色。此服务相关角色是预定义的，并包含 Amazon Web Services Support 代表您调用其他 Amazon 服务所需的权限。

`AWSServiceRoleForSupport` 服务相关角色信任 `support.amazonaws.com` 服务来代入角色。

为提供这些服务，该角色的预定义权限会向 Amazon Web Services Support 授予对资源元数据而不是客户数据的访问权限。只有 Amazon Web Services Support 工具可以代入此角色，此角色存在于您的 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 调用的 GetExecutionHistory 的 `Input` 和 `Output` 字段对 Amazon Web Services Support 不可见。我们使用 Amazon KMS keys 加密敏感字段。这些字段在 API 响应中进行了编辑，对 Amazon Web Services Support 代理不可见。

> **Note**
>
> Amazon Trusted Advisor 使用单独的 IAM 服务相关角色来访问您账户的 Amazon 资源，以提供最佳实践建议和检查。有关更多信息，请参阅将服务相关角色用于 Trusted Advisor (p. 92)。

`AWSServiceRoleForSupport` 服务相关角色通过 Amazon CloudTrail 使所有 Amazon Web Services Support API 调用均对客户可见。这样便于监控和审核要求，因为您可以透明地了解 Amazon Web Services Support 代表您执行的操作。有关 CloudTrail 的更多信息，请参阅 Amazon CloudTrail 用户指南。

### Amazon Web Services Support 的服务相关角色权限

此角色使用 `AWSSupportServiceRolePolicy` Amazon 托管式策略。此托管策略已附加到角色，并授予角色代表您完成操作的权限。

这些操作可能包括以下内容：

- 账单、管理、支持和其他客户服务 – Amazon 客户服务使用托管策略授予的权限来执行很多服务以作为支持计划的一部分。其中包括调查和解答账户和账单问题、为账户提供管理支持、增加服务配额和提供额外的客户支持。
- 您的 Amazon 账户的服务属性和使用数据的处理 – Amazon Web Services Support 可能会使用托管策略授予的权限来访问您的 Amazon 账户的服务属性和使用数据。此策略允许 Amazon Web Services Support 为您的账户提供账单、管理和技术支持。服务属性包括账户的资源标识符、元数据标签、角色和权限。使用率数据包括使用策略、使用情况统计数据和分析。

- 维护账户及其资源的运行状况 – Amazon Web Services Support 使用自动化工具执行与操作和技术支持相关的操作。

有关允许的服务和操作的更多信息，请参阅 IAM 控制台中的 AWSSupportServiceRolePolicy 策略。

> **Note**
>
> Amazon Web Services Support 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 Web Services Support 和 Amazon Trusted Advisor 的 Amazon 托管策略 (p. 95)。

### 为 Amazon Web Services Support 创建服务相关角色

您无需手动创建 `AWSServiceRoleForSupport` 角色。当您创建 Amazon 账户时，将自动为您创建和配置此角色。

> **Important**
>
> 如果您在 Amazon Web Services Support 开始支持服务相关角色之前使用该服务，则 Amazon 会在您的账户中创建 `AWSServiceRoleForSupport` 角色。有关更多信息，请参阅我的 IAM 账户中出现新角色。

### 为 Amazon Web Services Support 编辑和删除服务相关角色

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

`AWSServiceRoleForSupport` 角色对于 Amazon Web Services Support 为您的账户提供管理、运营和技术支持是必需的。因此，无法通过 IAM 控制台、API 或 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。

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

## 将服务相关角色用于 Trusted Advisor

Amazon Trusted Advisor 使用 Amazon Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与 Amazon Trusted Advisor 直接关联的独特 IAM 角色。服务相关角色由 Trusted Advisor 预定义，并具有该服务代表您调用其他 Amazon 服务所需的一切权限。Trusted Advisor 使用此角色检查您在 Amazon 上的使用情况并提供用于改善 Amazon 环境的建议。例如，Trusted Advisor 通过分析您的 Amazon Elastic Compute Cloud (Amazon EC2) 实例使用来帮助您降低成本、提高性能、增强容错能力，并提高安全性。

> **Note**
>
> Amazon Web Services Support 使用单独的 IAM 服务相关角色来访问账户的资源，以提供账单、管理和支持服务。有关更多信息，请参阅将服务相关角色用于 Amazon Web Services Support (p. 91)。

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

主题

## Trusted Advisor 的服务相关角色权限

Trusted Advisor 使用两个服务相关角色：

- AWSServiceRoleForTrustedAdvisor – 此角色信任 Trusted Advisor 服务来代入代表您访问 Amazon 服务的角色。角色权限策略允许 Trusted Advisor 对所有的 Amazon 资源的只读访问权限。此角色可简化开始使用 Amazon 账户的过程，因为您不必为 Trusted Advisor 添加必要的权限。在开设一个 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 (p. 99)。
- AWSServiceRoleForTrustedAdvisorReporting – 此角色信任 Trusted Advisor 服务来担任组织视图功能的角色。此角色启用 Trusted Advisor 作为您的 Amazon Organizations 组织的可信服务。Trusted Advisor 将在您启用组织视图时为您创建此角色。

  有关附加策略的更多信息，请参阅 AWSTrustedAdvisorReportingServiceRolePolicy (p. 101)。

  您可以使用组织视图为组织中的所有账户的 Trusted Advisor 检查结果创建报告。有关此功能的更多信息，请参阅Amazon Trusted Advisor 的组织视图 (p. 37)。

## 管理服务相关角色的权限

必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。以下示例使用 `AWSServiceRoleForTrustedAdvisor` 服务相关角色。

### Example ：允许 IAM 实体创建 **`AWSServiceRoleForTrustedAdvisor`** 服务相关角色

仅当 Trusted Advisor 账户被禁用、服务相关角色被删除并且用户必须重新创建角色来重新启用 Trusted Advisor 时，才需执行此步骤。

将以下语句添加到 IAM 实体的权限策略可创建服务相关角色。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

### Example ：允许 IAM 实体编辑 **`AWSServiceRoleForTrustedAdvisor`** 服务相关角色的描述

您只能编辑 `AWSServiceRoleForTrustedAdvisor` 角色的描述。您可以将以下语句添加到 IAM 实体的权限策略来编辑服务相关角色的描述。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

Example ：允许 IAM 实体删除 **AWSServiceRoleForTrustedAdvisor** 服务相关角色

您可以将以下语句添加到 IAM 实体的权限策略来删除服务相关角色。

```
{
    "Effect": "Allow",
    "Action": [
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/trustedadvisor.amazonaws.com/
AWSServiceRoleForTrustedAdvisor*",
    "Condition": {"StringLike": {"iam:AWSServiceName": "trustedadvisor.amazonaws.com"}}
}
```

您也可以使用 Amazon 托管策略（如 AdministratorAccess）来提供对 Trusted Advisor 的完全访问权限。

## 为 Trusted Advisor 创建服务相关角色

无需手动创建 AWSServiceRoleForTrustedAdvisor 服务相关角色。开设 Amazon 账户时，Trusted Advisor 将为您创建服务相关角色。

> **Important**
>
> 如果您在 Trusted Advisor 服务开始支持服务相关角色之前使用该服务，则 Trusted Advisor 会在您的账户中创建 AWSServiceRoleForTrustedAdvisor 角色。要了解更多信息，请参阅 IAM 用户指南中的我的 IAM 账户中出现新角色。

如果您的账户没有 AWSServiceRoleForTrustedAdvisor 服务相关角色，Trusted Advisor 将无法按预期工作。如果您的账户中有人将 Trusted Advisor 禁用然后又删除服务相关角色，可能会出现上述情况。在这种情况下，您可以使用 IAM 创建 AWSServiceRoleForTrustedAdvisor 服务相关角色，然后重新启用 Trusted Advisor。

启用 Trusted Advisor（控制台）

1. 使用 IAM 控制台、Amazon CLI 或 IAM API 为 Trusted Advisor 创建服务相关角色。有关更多信息，请参阅创建服务相关角色。
2. 登录到 Amazon Web Services Management Console，然后导航到位于 https://console.amazonaws.cn/trustedadvisor 的 Trusted Advisor 控制台。

   禁用的 Trusted Advisor 状态横幅显示在控制台中。
3. 从状态横幅中选择 Enable Trusted Advisor Role（启用 Trusted Advisor 角色）。如果未检测到所需的 AWSServiceRoleForTrustedAdvisor，则已禁用状态横幅仍将显示。

## 为 Trusted Advisor 编辑服务相关角色

由于多个实体可能引用该角色，因此无法更改服务相关角色的名称。不过，您可以使用 IAM 控制台、Amazon CLI 或 IAM API 编辑角色描述。有关更多信息，请参阅 IAM 用户指南中的编辑服务相关角色。

## 删除 Trusted Advisor 的服务相关角色

如果您不需要使用 Trusted Advisor 的功能或服务，您可以删除 AWSServiceRoleForTrustedAdvisor 角色。您必须禁用 Trusted Advisor，然后才能删除此服务相关角色。这样可以防止您删除 Trusted Advisor 操作所需的权限。当您禁用 Trusted Advisor 时，将禁用所有服务功能，包括脱机处理和通知。此外，如果为成员账户禁用 Trusted Advisor，则单独的付款人账户也会受到影响，这意味着您将不会收到确定成本节省方法的 Trusted Advisor 检查。您无法访问 Trusted Advisor 控制台。对 Trusted Advisor 的 API 调用将返回访问被拒绝错误。

您必须在 AWSServiceRoleForTrustedAdvisor 账户中重新创建服务相关角色，然后才能重新启用 Trusted Advisor。

在删除 AWSServiceRoleForTrustedAdvisor 服务相关角色之前，您必须先在控制台中禁用 Trusted Advisor。

要禁用 Trusted Advisor

1. 登录到 Amazon Web Services Management Console 并导航到位于 https://console.amazonaws.cn/trustedadvisor 的 Trusted Advisor 控制台。
2. 在导航窗格中，选择 Preferences。
3. 在服务相关角色权限部分中，选择禁用 Trusted Advisor。
4. 在确认对话框中，通过选择 OK（确定）来确认您要禁用 Trusted Advisor。

禁用 Trusted Advisor 后，所有 Trusted Advisor 功能都将被禁用，Trusted Advisor 控制台将只显示已禁用状态横幅。

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

# Amazon Web Services Support 和 Amazon Trusted Advisor 的 Amazon 托管策略

要向用户、组和角色添加权限，与自己编写策略相比，使用 Amazon 托管策略更简单。创建仅为团队提供所需权限的 IAM 客户托管策略需要时间和专业知识。要快速入门，您可以使用我们的 Amazon 托管式策略。这些策略涵盖常见使用案例，可在您的 Amazon Web Services 账户 中使用。有关 Amazon 托管式策略的更多信息，请参阅 IAM 用户指南中的Amazon 托管式策略。

Amazon Web Services 负责维护和更新 Amazon 托管式策略。您无法更改 Amazon 托管式策略中的权限。服务偶尔会向 Amazon 托管式策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新功能或新操作可用时，服务最有可能会更新 Amazon 托管式策略。服务不会从 Amazon 托管式策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，Amazon 还支持跨多种服务的工作职能的托管式策略。例如，ViewOnlyAccess Amazon 托管式策略提供对许多 Amazon Web Services 服务和资源的只读访问权限。当服务启动新功能时，Amazon 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 Amazon 托管策略。

目录



## Amazon适用于 Amazon Web Services Support 的托管策略

Amazon Web Services Support 具有以下托管式策略。

目录

## Amazon 托管策略：AWSSupportServiceRolePolicy

Amazon Web Services Support 使用 AWSSupportServiceRolePolicy Amazon 托管策略。此托管策略附加到 `AWSServiceRoleForSupport` 服务相关角色。该策略允许服务相关角色代表您完成操作。您不能将此策略附加到您的 IAM 实体。有关更多信息，请参阅Amazon Web Services Support 的服务相关角色权限 (p. 91)。

有关对策略的更改列表，请参阅 对 Amazon 托管式策略的 Amazon Web Services Support 更新 (p. 96) 和 AWSSupportServiceRolePolicy 的权限更改 (p. 98)。

## 对 Amazon 托管式策略的 Amazon Web Services Support 更新

查看有关 Amazon Web Services Support 和 Trusted Advisor 的 Amazon 托管式策略更新的详细信息（从这些服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅 文档历史记录 (p. 140) 页面上的 RSS 源。

下表介绍了自 2022 年 2 月 17 日以来对 Amazon Web Services Support 托管式策略的重要更新。

Amazon Web Services Support

| 更改 | 说明 | 日期 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy (p. 96) – 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：<br>• Amazon CloudWatch Logs – 帮助排查 CloudWatch Logs 相关问题。<br>• Amazon Interactive Video Service – 帮助 Amazon Web Services Support 检查现有的 Amazon IVS 资源，了解有关欺诈或账户遭盗用的支持案例。<br>• Amazon Inspector – 对 Amazon Inspector 相关问题进行问题排查。<br>删除了服务（例如 Amazon WorkLink）的权限。Amazon WorkLink 已在 2022 年 4 月 19 日弃用。 | 2022 年 6 月 23 日 |
| AWSSupportServiceRolePolicy (p. 96) – 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： | 2022 年 4 月 27 日 |

| 更改 | 说明 | 日期 |
| --- | --- | --- |
| | • Amazon Amplify UI Builder – 排查与组件和主题生成相关的问题。<br>• Amazon AppStream – 通过检索最近启动的功能的相关资源来排查问题。<br>• Amazon Backup – 排查与备份作业相关的问题。<br>• Amazon CloudFormation – 诊断与 IAM、扩展和版本控制相关的问题。<br>• Amazon Kinesis – 排查与 Kinesis 相关的问题。<br>• Amazon Transfer Family – 排查与 Transfer Family 相关的问题。 | |
| AWSSupportServiceRolePolicy (p. 97) – 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：<br>• Amazon Elastic Compute Cloud<br>  • 解决与客户和 Amazon 管理的前缀列表相关的问题。<br>  • 解决与 Amazon VPC IP 地址管理器 (IPAM) 相关的问题。<br>• Amazon 网络管理器 – 解决与网络管理器相关的问题。<br>• Savings Plans – 获取有关未完成 Savings Plan 承诺的元数据。<br>• Amazon Serverless Application Repository – 作为研究和解决支持案例的一部分，改进和支持响应操作。<br>• Amazon WorkSpaces Web – 调试和解决 WorkSpaces Web 服务的问题。 | 2022 年 3 月 14 日 |

| 更改 | 说明 | 日期 |
| --- | --- | --- |
| AWSSupportServiceRolePolicy (p. 97) – 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：<br>• Amazon Application Migration Service - 在应用程序迁移服务中支持无代理复制。<br>• Amazon CloudFormation - 对 IAM、扩展和版本控制相关问题执行诊断。<br>• Amazon CloudWatch Logs - 验证资源策略。<br>• Amazon EC2 回收站 - 获取有关回收站保留规则的元数据。<br>• Amazon Elastic Disaster Recovery - 解决客户账户中的复制问题和启动问题。<br>• Amazon FSx - 查看 Amazon FSx 快照的描述。<br>• Amazon Lightsail - 查看 Lightsail 存储桶的元数据和配置详细信息。<br>• 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。<br>• Simple Storage Service (Amazon S3) - 收集 Simple Storage Service (Amazon S3) 存储桶的元数据和配置。<br>• Amazon Storage Gateway - 查看有关客户自动创建磁带策略的元数据。<br>• Elastic Load Balancing - 查看使用 Service Quotas 控制台时的资源限制的说明。<br><br>有关更多信息，请参阅AWSSupportServiceRolePolicy 的权限更改 (p. 98)。 | 2022 年 2 月 17 日 |
| 已发布的更改日志 | Amazon Web Services Support 托管策略的更改日志。 | 2022 年 2 月 17 日 |

## AWSSupportServiceRolePolicy 的权限更改

添加到 `AWSSupportServiceRolePolicy` 的大多数权限允许 Amazon Web Services Support 使用相同名称调用 API 操作。但是，某些 API 操作需要具有不同名称的权限。

下表仅列出了需要具有不同名称的权限的 API 操作。下表介绍了这些从 2022 年 2 月 17 日开始的差异。

| 日期 | API 操作名称 | 所需的策略权限 |
| --- | --- | --- |
| 2022 年 2 月 17 日添加了权限 | s3.GetBucketAnalyticsConfiguration<br>s3.ListBucketAnalyticsConfiguration | s3:GetAnalyticsConfiguration |
| | s3.GetBucketNotificationConfiguration | s3:GetBucketNotification |
| | s3.GetBucketEncryption | s3:GetEncryptionConfiguration |
| | s3.GetBucketIntelligentTieringConfiguration<br>s3.ListBucketIntelligentTieringConfiguration | s3:GetIntelligentTieringConfiguratio |
| | s3.GetBucketInventoryConfiguration<br>s3.ListBucketInventoryConfiguration | s3:GetInventoryConfiguration |
| | s3.GetBucketLifecycleConfiguration | s3:GetLifecycleConfiguration |
| | s3.GetBucketMetricsConfiguration<br>s3.ListBucketMetricsConfiguration | s3:GetMetricsConfiguration |
| | s3.GetBucketReplication | s3:GetReplicationConfiguration |
| | s3.HeadBucket<br>s3.ListObjects | s3:ListBucket |
| | s3.ListBuckets | s3:ListAllMyBuckets |
| | s3.ListMultipartUploads | s3:ListBucketMultipartUploads |
| | s3.ListObjectVersions | s3:ListBucketVersions |
| | s3.ListParts | s3:ListMultipartUploadParts |

# Amazon适用于 Amazon Trusted Advisor 的托管策略

Trusted Advisor 具有以下托管式策略。

目录



## Amazon 托管策略：AWSTrustedAdvisorServiceRolePolicy

此策略附加到 `AWSServiceRoleForTrustedAdvisor` 服务相关角色。它使服务相关角色能够代表您执行操作。您不能将 AWSTrustedAdvisorServiceRolePolicy 附加到您的 IAM 实体。有关更多信息，请参阅将服务相关角色用于 Trusted Advisor (p. 92)。

此策略授予管理权限，允许服务相关角色访问 Amazon 服务。这些权限允许 Trusted Advisor 的检查来评估您的账户。

权限详细信息

此策略包含以下权限。

- `Auto Scaling` – 描述 Amazon EC2 Auto Scaling 账户配额和资源
- `cloudformation` – 描述 Amazon CloudFormation (CloudFormation) 账户配额和堆栈
- `cloudfront` – 描述 Amazon CloudFront 分配
- `cloudtrail` – 描述 Amazon CloudTrail (CloudTrail) 跟踪
- `dynamodb` – 描述 Amazon DynamoDB 账户配额和资源
- `ec2` – 描述 Amazon Elastic Compute Cloud (Amazon EC2) 账户配额和资源
- `elasticloadbalancing` – 描述 Elastic Load Balancing 账户配额和资源
- `iam` – 获取 IAM 资源，如证书、密码策略和证书
- `kinesis` – 描述 Amazon Kinesis (Kinesis) 账户配额
- `rds` – 描述 Amazon Relational Database Service (Amazon RDS) 资源
- `redshift` – 描述 Amazon Redshift 资源
- `route53` – 描述 Amazon Route 53 账户配额和资源
- `s3` – 描述 Amazon Simple Storage Service (Amazon S3) 资源
- `ses` – 获取 Amazon Simple Email Service (Amazon SES) 发送配额
- `sqs` – 列出 Amazon Simple Queue Service (Amazon SQS) 队列
- `cloudwatch` – 获取 Amazon CloudWatch Events (CloudWatch Events) 指标统计数据
- `ce` – 获取 Cost Explorer 服务 (Cost Explorer) 建议

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "autoscaling:DescribeAccountLimits",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "cloudformation:DescribeAccountLimits",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStacks",
                "cloudfront:ListDistributions",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetTrailStatus",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListTables",
                "ec2:DescribeAddresses",
                "ec2:DescribeReservedInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeImages",
                "ec2:DescribeVolumes",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:DescribeLaunchTemplateVersions",
```

```
                "elasticloadbalancing:DescribeAccountLimits",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancerAttributes",
                "elasticloadbalancing:DescribeLoadBalancerPolicies",
                "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "iam:GenerateCredentialReport",
                "iam:GetAccountPasswordPolicy",
                "iam:GetAccountSummary",
                "iam:GetCredentialReport",
                "iam:GetServerCertificate",
                "iam:ListServerCertificates",
                "kinesis:DescribeLimits",
                "rds:DescribeAccountAttributes",
                "rds:DescribeDBClusters",
                "rds:DescribeDBEngineVersions",
                "rds:DescribeDBInstances",
                "rds:DescribeDBParameterGroups",
                "rds:DescribeDBParameters",
                "rds:DescribeDBSecurityGroups",
                "rds:DescribeDBSnapshots",
                "rds:DescribeDBSubnetGroups",
                "rds:DescribeEngineDefaultParameters",
                "rds:DescribeEvents",
                "rds:DescribeOptionGroupOptions",
                "rds:DescribeOptionGroups",
                "rds:DescribeOrderableDBInstanceOptions",
                "rds:DescribeReservedDBInstances",
                "rds:DescribeReservedDBInstancesOfferings",
                "rds:ListTagsForResource",
                "redshift:DescribeClusters",
                "redshift:DescribeReservedNodeOfferings",
                "redshift:DescribeReservedNodes",
                "route53:GetAccountLimit",
                "route53:GetHealthCheck",
                "route53:GetHostedZone",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListHostedZonesByName",
                "route53:ListResourceRecordSets",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketPublicAccessBlock",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "ses:GetSendQuota",
                "sqs:ListQueues",
                "cloudwatch:GetMetricStatistics",
                "ce:GetReservationPurchaseRecommendation",
                "ce:GetSavingsPlansPurchaseRecommendation"
            ],
            "Resource": "*"
        }
    ]
}
```

## Amazon 托管策略：AWSTrustedAdvisorReportingServiceRolePolicy

此策略附加到 AWSServiceRoleForTrustedAdvisorReporting 服务相关角色，使 Trusted Advisor 能够执行组织视图功能的操作。您不能将 AWSTrustedAdvisorReportingServiceRolePolicy 附加到您的 IAM 实体。有关更多信息，请参阅将服务相关角色用于 Trusted Advisor (p. 92)。

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

此策略包含以下权限。

- organizations – 描述您的组织并列出服务访问权限、账户、父级、子级和组织单位

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations: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 Amazon Web Services Support 和 Trusted Advisor 的 Amazon 托管策略更新的详细信息（从这些服务开始跟踪这些更改开始）。要获得有关此页面更改的自动提示，请订阅 文档历史记录 (p. 140) 页面上的 RSS 源。

下表介绍了自 2021 年 8 月 10 日以来对 Trusted Advisor 托管式策略的重要更新。

Trusted Advisor

| 更改 | 说明 | 日期 |
| --- | --- | --- |
| AWSTrustedAdvisorServiceRolePolicy (p. 99) – 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。<br><br>Auto Scaling 组运行状况检查需要 DescribeTargetGroup 权限， | 2021 年 8 月 10 日 |

| 更改 | 说明 | 日期 |
| --- | --- | --- |
| | 以检索附加到 Auto Scaling 组的非 Classic Load Balancer。<br><br>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。 | |
| 已发布的更改日志 | Trusted Advisor 托管策略的更改日志。 | 2021 年 8 月 10 日 |

# 管理对 Amazon Trusted Advisor 的访问

您可以从 Amazon Web Services Management Console访问 Amazon Trusted Advisor。所有 Amazon 账户都有权访问特色级核心 Trusted Advisor 检查。如果您拥有商业、Enterprise On-Ramp 或企业 Support 计划，则可以访问所有检查。有关更多信息，请参阅 Amazon Trusted Advisor 检查引用 (p. 59)。

您可以使用 Amazon Identity and Access Management (IAM) 控制对 Trusted Advisor 的访问权限。

主题



## Trusted Advisor 控制台的权限

要访问 Trusted Advisor 控制台，用户必须拥有一组最低的权限。这些权限必须允许用户列出和查看有关您的 Amazon Web Services 账户 中的 Trusted Advisor 资源的详细信息。

可以使用以下选项来控制对 Trusted Advisor 的访问：

- 使用 Trusted Advisor 控制台的标签筛选条件功能。用户或角色必须具有与标签关联的权限。

  可以使用 Amazon 托管策略或自定义策略来按标签分配权限。有关更多信息，请参阅 使用标签控制对 IAM 用户和角色的访问。
- 使用 `trustedadvisor` 命名空间创建 IAM policy。您可以使用此策略来指定操作和资源的权限。

创建策略时，可以指定服务的命名空间来允许或拒绝操作。Trusted Advisor 的命名空间为 `trustedadvisor`。但是，不能使用 `trustedadvisor` 命名空间来允许或拒绝 Amazon Web Services Support API 中的 Trusted Advisor API 操作。相反，您必须使用 Amazon Web Services Support 的 `support` 命名空间。

> **Note**
>
> 如果您具有 Amazon Web Services Support API 的权限，则 Amazon Web Services Management Console 中的 Trusted Advisor 小部件将显示 Trusted Advisor 结果的摘要视图。要在 Trusted Advisor 控制台中查看结果，您必须具有 `trustedadvisor` 命名空间的权限。

# Trusted Advisor 操作

可以在控制台中执行以下 Trusted Advisor 操作。还可以在 IAM policy 中指定这些 Trusted Advisor 操作以允许或拒绝特定操作。

| 操作 | 描述 |
| --- | --- |
| DescribeAccount | 授予权限以查看 Amazon Web Services Support 计划和各种 Trusted Advisor 首选项。 |
| DescribeAccountAccess | 授予权限以查看 Amazon 账户启用还是禁用了 Trusted Advisor。 |
| DescribeCheckItems | 授予权限以查看检查项目的详细信息。 |
| DescribeCheckRefreshStatuses | 授予权限以查看 Trusted Advisor 检查的刷新状态。 |
| DescribeCheckSummaries | 授予权限以查看 Trusted Advisor 检查摘要。 |
| DescribeChecks | 授予权限以查看 Trusted Advisor 检查的详细信息。 |
| DescribeNotificationPreferences | 授予权限以查看 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 | 授予权限以刷新 Trusted Advisor 检查。 |
| SetAccountAccess | 授予权限以便为账户启用或禁用 Trusted Advisor。 |
| UpdateNotificationPreferences | 授予权限以更新 Trusted Advisor 的通知首选项。 |

## 组织视图的 Trusted Advisor 操作

以下 Trusted Advisor 操作用于组织视图功能。有关更多信息，请参阅Amazon Trusted Advisor 的组织视图 (p. 37)。

| 操作 | 描述 |
| --- | --- |
| DescribeOrganization | 授予权限以查看 Amazon 账户是否满足启用组织视图功能的要求。 |
| DescribeOrganizationAccounts | 授予权限以查看组织中的关联 Amazon 账户。 |
| DescribeReports | 授予权限以查看组织视图报告的详细信息（例如，报告名称、运行时间、创建日期、状态和格式）。 |
| DescribeServiceMetadata | 授予权限以查看有关组织视图报告的信息（例如，Amazon 区域、检查类别、检查名称和资源状态）。 |
| GenerateReport | 授予权限以便为组织中的 Trusted Advisor 检查创建报告。 |
| ListAccountsForParent | 授予在 Trusted Advisor 控制台中查看 Amazon 组织中由根或组织单位 (OU) 包含的所有账户的权限。 |

| 操作 | 描述 |
| --- | --- |
| `ListOrganizationalUnitsForParent` | 授予在 Trusted Advisor 控制台中查看父组织单位或根中所有组织单位 (OU) 的权限。 |
| `ListRoots` | 授予在 Trusted Advisor 控制台中查看 Amazon 组织中定义的所有根的权限。 |
| `SetOrganizationAccess` | 授予权限以便为 Trusted Advisor 启用组织视图功能。 |

### Amazon Trusted Advisor Priority 操作

如果为您的账户启用了 Amazon Trusted Advisor Priority，则可以在控制台中执行以下 Trusted Advisor 操作；您还可以在 IAM policy 中添加这些 Trusted Advisor 操作来允许或拒绝特定操作。有关更多信息，请参阅Amazon Trusted Advisor Priority 的 IAM policy 示例 (p. 108)。

> **Note**
>
> Amazon Trusted Advisor Priority 中出现的风险是您的技术客户经理 (TAM) 为您的账户确定的建议。系统会自动为您创建来自服务的建议，例如 Trusted Advisor 检查。来自 TAM 的建议是手动为您创建的。接下来，您的 TAM 会发送这些建议，以便它们出现在您账户的 Amazon Trusted Advisor Priority 中。

有关更多信息，请参阅Amazon Trusted Advisor Priority 入门 (p. 56)。

| 操作 | 描述 |
| --- | --- |
| `DescribeRisks` | 授予权限以查看 Amazon Trusted Advisor Priority 中的风险。 |
| `DescribeRisk` | 授予权限以查看 Amazon Trusted Advisor Priority 中的风险详细信息。 |
| `DescribeRiskResources` | 授予权限以查看 Amazon Trusted Advisor Priority 中受影响的风险资源。 |
| `UpdateRiskStatus` | 授予权限以更新 Amazon Trusted Advisor Priority 中的风险状态。 |
| `DownloadRisk` | 授予权限以下载包含 Amazon Trusted Advisor Priority 中风险详细信息的文件。 |

## IAM policy 示例

以下策略介绍如何允许和拒绝对 Trusted Advisor 的访问。您可以使用下面的策略之一来在 IAM 控制台中创建客户托管策略。例如，您可以复制示例策略，然后将其粘贴到 IAM 控制台的 JSON 选项卡中。然后，将策略附加您的 IAM 用户、组或角色。

有关如何创建 IAM policy 的更多信息，请参阅 IAM 用户指南中的创建 IAM policy（控制台）。

示例

- 对 Trusted Advisor 的完全访问权限 (p. 106)
- 对 Trusted Advisor 的只读访问权限 (p. 106)
- 拒绝对 Trusted Advisor 的访问 (p. 106)

## 对 Trusted Advisor 的完全访问权限

以下策略允许用户在 Trusted Advisor 控制台中查看和执行针对所有 Trusted Advisor 检查的所有操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

## 对 Trusted Advisor 的只读访问权限

以下策略允许用户对 Trusted Advisor 控制台进行只读访问。用户无法进行任何更改，例如刷新检查或更改通知首选项。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:Describe*",
            "Resource": "*"
        }
    ]
}
```

## 拒绝对 Trusted Advisor 的访问

以下策略不允许用户在 Trusted Advisor 控制台中查看或执行针对 Trusted Advisor 检查的操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        }
    ]
}
```

## 允许和拒绝特定操作

以下策略允许用户在 Trusted Advisor 控制台中查看所有 Trusted Advisor 检查，但不允许用户刷新任何检查。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:RefreshCheck",
            "Resource": "*"
        }
    ]
}
```

## 控制对 Trusted Advisor 的 Amazon Web Services Support API 操作的访问

在 Amazon Web Services Management Console中，单独的 `trustedadvisor` IAM 命名空间控制对 Trusted Advisor 的访问。不能使用 `trustedadvisor` 命名空间来允许或拒绝 Amazon Web Services Support API 中的 Trusted Advisor API 操作。相反，可以使用 `support` IAM 命名空间。您必须具有对 Amazon Web Services Support API 的权限才能以编程方式调用 Trusted Advisor。

例如，如果您要调用 RefreshTrustedAdvisorCheck 操作，则必须在策略中具有此操作的权限。

### Example ：仅允许 Trusted Advisor API 操作

以下策略允许用户访问 Trusted Advisor 的 Amazon Web Services Support API 操作，而不允许用户访问其余的 Amazon Web Services Support API 操作。例如，用户可以使用 API 查看和刷新检查。它们无法创建、查看、更新或解析 Amazon Web Services Support 案例。

您可以使用此策略以编程方式调用 Trusted Advisor API 操作，但您无法使用此策略在 Trusted Advisor 控制台中查看或刷新检查。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "support:DescribeTrustedAdvisorCheckRefreshStatuses",
                "support:DescribeTrustedAdvisorCheckResult",
                "support:DescribeTrustedAdvisorChecks",
                "support:DescribeTrustedAdvisorCheckSummaries",
                "support:RefreshTrustedAdvisorCheck",
                "trustedadvisor:Describe*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "support:AddAttachmentsToSet",
                "support:AddCommunicationToCase",
                "support:CreateCase",
                "support:DescribeAttachment",
                "support:DescribeCases",
                "support:DescribeCommunications",
                "support:DescribeServices",
                "support:DescribeSeverityLevels",
                "support:ResolveCase"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

有关 IAM 如何使用 Amazon Web Services Support 和 Trusted Advisor 的更多信息，请参阅 操作 (p. 88)。

## Amazon Trusted Advisor Priority 的 IAM policy 示例

您可以使用以下示例策略来管理对 Amazon Trusted Advisor Priority 的访问。有关更多信息，请参阅Amazon Trusted Advisor Priority 入门 (p. 56)。

### 对 Amazon Trusted Advisor Priority 进行完全访问

以下策略允许用户对 Amazon Trusted Advisor Priority 进行完全访问。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:DescribeRisk*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:DownloadRisk*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:UpdateRiskStatus",
            "Resource": "*"
        }
    ]
}
```

## 对 Amazon Trusted Advisor Priority 进行只读访问

以下策略允许对 Amazon Trusted Advisor Priority 进行只读访问。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:DescribeRisk*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:DownloadRisk*",
            "Resource": "*"
        }
    ]
}
```

## 拒绝访问 Amazon Trusted AdvisorPriority

以下策略不允许用户访问 Amazon Trusted Advisor Priority。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:DescribeRisk*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:DownloadRisk*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:UpdateRiskStatus",
            "Resource": "*"
        }
    ]
}
```

### 允许和拒绝 Amazon Trusted Advisor Priority 的操作

以下策略允许用户查看 Amazon Trusted Advisor Priority 中的风险，但不能下载有关风险的文件。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "trustedadvisor:DescribeRisk*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "trustedadvisor:DownloadRisk*",
            "Resource": "*"
        }
    ]
}
```

## 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

# 对 Amazon Web Services Support 身份和访问进行故障排除

使用以下信息可帮助您诊断和修复在使用 Amazon Web Services Support 和 IAM 时可能遇到的常见问题。

主题

- 我希望允许我的 Amazon 账户之外的人员访问我的 Amazon Web Services Support 资源 (p. 110)

## 未授权我执行 iam:PassRole

如果您收到错误消息，提示您无权执行 `iam:PassRole` 操作，则必须联系您的管理员寻求帮助。您的管理员是指为您提供用户名和密码的那个人。请求该人员更新您的策略，以便允许您将角色传递给 Amazon Web Services Support。

有些 Amazon Web Services允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 `marymajor` 的 IAM 用户尝试使用控制台在 Amazon Web Services Support 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行操作。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，Mary 请求她的管理员来更新其策略，以允许她执行 `iam:PassRole` 操作。

## 我想要查看我的访问密钥

在创建 IAM 用户访问密钥后，您可以随时查看您的访问密钥 ID。但是，您无法再查看您的秘密访问密钥。如果您丢失了私有密钥，则必须创建一个新的访问密钥对。

访问密钥包含两部分：访问密钥 ID（例如 `AKIAIOSFODNN7EXAMPLE`）和秘密访问密钥（例如 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`）。与用户名和密码一样，您必须同时使用访问密钥 ID 和秘密访问密钥对请求执行身份验证。像对用户名和密码一样，安全地管理访问密钥。

> **Important**
>
> 请不要向第三方提供访问密钥，即便是为了帮助找到您的规范用户 ID 也不行。如果您这样做，可能会向某人提供对您的账户的永久访问权限。

当您创建访问密钥对时，系统会提示您将访问密钥 ID 和秘密访问密钥保存在一个安全位置。秘密访问密钥仅在您创建它时可用。如果丢失了您的秘密访问密钥，您必须为 IAM 用户添加新的访问密钥。您最多可拥有两个访问密钥。如果您已有两个密钥，则必须删除一个密钥对，然后再创建新的密钥。要查看说明，请参阅 IAM 用户指南中的管理访问密钥。

## 我是管理员并希望允许其他人访问 Amazon Web Services Support

要允许其他人访问 Amazon Web Services Support，您必须为需要访问权限的人员或应用程序创建一个 IAM 实体（用户或角色）。它们将使用该实体的凭证访问 Amazon。然后，您必须将策略附加到实体，以便在 Amazon Web Services Support 中向其授予正确的权限。

要立即开始使用，请参阅 IAM 用户指南中的创建您的第一个 IAM 委派用户和组。

## 我希望允许我的 Amazon 账户之外的人员访问我的 Amazon Web Services Support 资源

您可以创建一个角色，以便其它账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon Web Services Support 是否支持这些功能，请参阅 Amazon Web Services Support 如何与 IAM 协同工作 (p. 88)。

- 要了解如何为您拥有的 Amazon Web Services 账户 中的资源提供访问权限，请参阅 IAM 用户指南中的为您拥有的另一个 Amazon Web Services 账户 中的 IAM 用户提供访问权限。
- 要了解如何为第三方Amazon Web Services 账户提供您的资源的访问权限，请参阅 IAM 用户指南中的为第三方拥有的Amazon Web Services 账户提供访问权限。
- 要了解如何通过联合身份验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（联合身份验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅 IAM 用户指南中的 IAM 角色与基于资源的策略有何不同。

# 事件响应

Amazon Web Services Support 的事件响应是一项 Amazon 责任。Amazon 拥有正式的、已归档的策略和程序来管理事件响应。有关更多信息，请参阅"Amazon 安全事件响应简介"白皮书。

使用以下选项可自行获知操作性问题：

- 具有广泛影响的 Amazon 操作性问题将在 Amazon Service Health Dashboard 上发布。例如，影响非账户特定的服务或区域的事件。
- 在 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。

# Amazon Web Services Support 和 Amazon Trusted Advisor 中的日志记录和监控

监控是保持 Amazon Web Services Support 和 Amazon Trusted Advisor 以及您的其他 Amazon 解决方案的可靠性、可用性和性能的重要方面。Amazon 提供了以下监控工具来监控 Amazon Web Services Support 和 Amazon Trusted Advisor、在出现错误时进行报告，并适时采取措施。

- Amazon CloudWatch 实时监控您的 Amazon 资源以及在 Amazon 上运行的应用程序。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，您可以让 CloudWatch 跟踪 CPU 使用率或 Amazon Elastic Compute Cloud (Amazon EC2) 的其他指标，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，并将日志文件传送到您指定的 Amazon Simple Storage Service (Amazon S3) 存储桶。您可以标识哪些用户和账户调用了 Amazon、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 Amazon CloudTrail 用户指南。

有关更多信息，请参阅 Amazon Web Services Support 的监控和日志记录 (p. 114) 和 Amazon Trusted Advisor 的监控和日志记录 (p. 123)。

# Amazon Web Services Support 的合规性验证

作为多个 Amazon 合规性计划的一部分，第三方审核员将评估 Amazon Web Services的安全性与合规性，例如 SOC、PCI、FedRAMP 和 HIPAA。

要了解此服务或其他 Amazon Web Services 是否在特定合规性计划范围内，请参阅合规性计划范围内的 Amazon Web Services。有关常规信息，请参阅Amazon Web Services合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅、在 Amazon Artifact 中下载报告。

您使用 Amazon Web Services 的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。Amazon 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在Amazon上部署注重安全性和合规性的基准环境的步骤。
- Amazon Web Services 上的 HIPAA 安全性和合规性架构设计– 该白皮书介绍了公司如何使用 Amazon Web Services 创建符合 HIPAA 标准的应用程序。

  Note

  并非所有 Amazon Web Services都符合 HIPAA 要求。有关更多信息，请参阅符合 HIPAA 要求的服务参考。
- Amazon合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config 开发人员指南中的使用规则评估资源 – 此 Amazon Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub：此 Amazon Web Service 提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践规范。

# Amazon Web Services Support 中的故障恢复能力

Amazon全球基础设施围绕Amazon区域和可用区构建。Amazon区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 Amazon 区域和可用区的更多信息，请参阅 Amazon 全球基础设施。

# Amazon Web Services Support 中的基础设施安全性

作为一项托管式服务，Amazon Web Services Support 由 Amazon Web Services：安全流程概览白皮书中所述的Amazon全球网络安全程序提供保护。

您可以使用 Amazon 发布的 API 调用通过网络访问 Amazon Web Services Support。客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 Amazon Security Token Service (Amazon STS) 生成临时安全凭证来对请求进行签名。

# Amazon Web Services Support 中的配置和漏洞分析

对于 Amazon Trusted Advisor，Amazon 负责处理来宾操作系统 (OS) 和数据库补丁、防火墙配置和灾难恢复等基本安全任务。

配置和 IT 控制是Amazon和您（我们的客户）之间的共同责任。有关更多信息，请参阅Amazon责任共担模型。

# Amazon Web Services Support 的监控和日志记录

监控是保持 Amazon Web Services Support 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 Support、在出现错误时进行报告并适时自动采取措施.

- Amazon EventBridge 提供近乎实时的系统事件流，这些系统事件描述了 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 Simple Storage Service（Amazon S3）存储桶。您可以标识哪些用户和账户调用了 Amazon、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 Amazon CloudTrail 用户指南。

主题



# 使用 Amazon EventBridge 来监控 Amazon Web Services Support 案例

> Note
>
> 此功能在中国区域中不可用。

您可以使用 Amazon EventBridge 检测并响应对您的 Amazon Web Services Support 案例的更改。然后，EventBridge 会根据您创建的规则，在事件与在规则中指定的值匹配时,调用一个或多个目标操作。

根据具体事件，您可以发送通知、捕获事件信息、采取纠正措施、启动事件或采取其他操作。例如，每当您的账户中发生以下操作时，您都可以收到通知：

- 创建支持案例
- 将案例通信添加到现有支持案例
- 解析支持案例
- 重新打开支持案例

> Note
>
> Amazon Web Services Support 将尽最大效能传送事件。并不总是能保证将事件传送到 EventBridge。

## 为 Amazon Web Services Support 案例创建 EventBridge 规则

您可以创建 EventBridge 规则，以针对 Amazon Web Services Support 案例事件获得通知。该规则将监控针对您账户中的支持案例的更新，包括您、您的 IAM 用户或支持代理执行的操作。在为 Amazon Web Services Support 案例事件创建规则之前，请执行以下操作：

- 熟悉 EventBridge 中的事件、规则和目标。有关更多信息，请参阅 Amazon EventBridge 用户指南中的什么是 Amazon EventBridge？。
- 创建要在您的事件规则中使用的目标。例如，您可以创建 Amazon Simple Notification Service (Amazon SNS) 主题，以便每当更新支持案例时，您都会收到短信或电子邮件。有关更多信息，请参阅 EventBridge 目标。

### 为 Amazon Web Services Support 案例事件创建 EventBridge 规则

1. 访问 https://console.aws.amazon.com/events/，打开 Amazon EventBridge 控制台。
2. 如果您尚未这样做，请使用页面的右上角的 Region selector（区域选择器），然后选择 US East (N. Virginia)（美国东部（弗吉尼亚北部））。
3. 在导航窗格中，选择 Rules (规则)。
4. 选择 Create rule (创建规则)。
5. 在 Define rule detail（定义规则详细信息）页面上，输入规则名称和描述。
6. 对于 Event bus（事件总线）和 Rule type（规则类型），保留默认值，然后选择 Next（下一步）。
7. 在 Build event pattern（构建事件模式）页面上，对于 Event source（事件源），选择 Amazon events or EventBridge partner events（ 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）。
9. 对于 Amazon Web Service，选择 Support。
10. 对于 Event type（事件类型），选择 Support Case Update（支持案例更新）。
11. 选择 Next (下一步)。
12. 在 Select targets（选择目标）部分中，选择您为此规则创建的目标，然后配置该类型所需的任何其他选项。例如，如果您选择 Amazon SNS，请确保正确配置 SNS 主题，以便通过电子邮件或短信通知您。
13. 选择 Next (下一步)。
14. （可选）在 Configure tags（配置标签）页面上，添加任意标签，然后选择 Next（下一步）。
15. 在 Review and create（检查并创建）页面上，检查您的规则设置并确保其符合您的事件监控要求。
16. 请选择 Create rule (创建规则)。您的规则现在将监控 Amazon Web Services Support 案例事件，然后将它们发送到您指定的目标。

**注意**

- 当您收到事件时，可以使用 `origin` 参数来确定是您还是 Amazon Web Services Support 代理向支持案例添加了案例通信。`origin` 的值可以是 `CUSTOMER` 或 `Amazon`。

  目前，仅 `AddCommunicationToCase` 操作的事件将具有此值。
- 有关创建事件模式的更多信息，请参阅《Amazon EventBridge 用户指南》中的 事件模式。
- 您还可以为通过 CloudTrail 进行 Amazon API 调用事件类型创建其他规则。此规则将监控您的账户中 Amazon Web Services Support API 调用的 Amazon CloudTrail 日志。

# 示例 Amazon Web Services Support 事件

当您的账户中发生支持操作时，将创建以下事件。

### Example ：创建支持案例

当创建支持案例时，将创建以下事件。

```
{
    "version": "0",
    "id": "3433df007-9285-55a3-f6d1-536944be45d7",
```

```
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "CreateCase",
        "origin": ""
    }
}
```

### Example ：更新支持案例

当 Amazon Web Services Support 回复支持案例时，将创建以下事件。

```
{
    "version": "0",
    "id": "f90cb8cb-32be-1c91-c0ba-d50b4ca5e51b",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "ekko:us-east-1:12345678-268a-424b-be08-54613cab84d2",
        "event-name": "AddCommunicationToCase",
        "origin": "AWS"
    }
}
```

### Example ：解析支持案例

当解析支持案例时，将创建以下事件。

```
{
    "version": "0",
    "id": "1aa4458d-556f-732e-ddc1-4a5b2fbd14a5",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:51:31Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2022-7118885805350839",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ResolveCase",
        "origin": ""
    }
}
```

### Example ：重新打开支持案例

当重新打开支持案例时，将创建以下事件。

```
{
    "version": "0",
    "id": "3bb9d8fe-6089-ad27-9508-804209b233ad",
    "detail-type": "Support Case Update",
    "source": "aws.support",
    "account": "111122223333",
    "time": "2022-02-21T15:47:19Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "case-id": "case-111122223333-muen-2021-27f40618fe0303ea",
        "display-id": "1234563851",
        "communication-id": "",
        "event-name": "ReopenCase",
        "origin": ""
    }
}
```

## 另请参阅

有关如何将 EventBridge 与 Amazon Web Services Support 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 Support API
- GitHub 上的 Amazon Web Services Support 案例活动通知程序

# 使用 Amazon Web Services Support 记录 Amazon CloudTrail API 调用

Amazon Web Services Support 与 Amazon CloudTrail 集成，后者是在 Amazon 中记录用户、角色或 Amazon Web Services Support 服务所执行操作的服务。CloudTrail 将 Amazon Web Services Support 的 API 调用作为事件捕获。捕获的调用包含来自 Amazon Web Services Support 控制台和代码的 Amazon Web Services Support 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 Support 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 Support 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 SupportCloudTrail 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 Support 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 Support 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 Simple Storage Service（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：

- 创建跟踪概览
- 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 Support API 操作，Amazon Web Services Support 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身份用户的临时安全凭证发出的。
- 请求是否由其它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 Support 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 Support 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 Support 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 (p. 133)。

# 了解 Amazon Web Services Support 日志文件条目

跟踪记录是一种配置，可用于将事件作为日志文件传送到您指定的 Simple Storage Service（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": "aws-cli/1.18.140 Python/3.6.12
 Linux/4.9.217-0.3.ac.206.84.332.metal1.x86_64 botocore/1.17.63",
    "requestParameters": {
        "checkId": "Pfx0RwqBli"
    },
    "responseElements": null,
    "requestID": "4c4d5fc8-c403-4f82-9544-41f820e0fa01",
```

```
    "eventID": "2f4630ac-5c27-4f0d-b93f-63742d6fc85e",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

# 记录对您的 Amazon Web Services Support 计划的更改

当您更改或查看 Support 计划 页面上的 Support 计划时，CloudTrail 会记录以下控制台操作：

- `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 Support 计划时，此操作显示在您的日志中。

**注意**

- 只有 Amazon 账户中的根用户才可以在 Support 计划页面执行这些操作。有关更多信息，请参阅 更改您的 Amazon Web Services Support 计划 (p. 16)。
- `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 Simple Storage Service（Amazon S3）存储桶。您可以标识哪些用户和账户调用了 Amazon、从中发出调用的源 IP 地址以及调用的发生时间。有关更多信息，请参阅 Amazon CloudTrail 用户指南。

主题



## 通过 Amazon EventBridge 监控 Amazon Trusted Advisor 的检查结果

您可以使用 EventBridge 来检测对 Trusted Advisor 的检查何时会更改状态。随后，当您在规则中指定的某个值的状态更改时，EventBridge 会根据您创建的规则调用一个或多个目标操作。

根据具体的状态更改，您可以发送通知、捕获状态信息、采取纠正措施、启动事件或采取其他操作。例如，如果检查状态由未检测到的问题（绿色）更改为建议的操作（红色），则可以指定以下目标类型。

- 使用 Amazon Lambda 函数将通知传入 Slack 通道。
- 将有关检查的数据推送到 Amazon Kinesis 流，以支持全面、实时的状态监控。
- 将 Amazon Simple Notification Service 主题发送到您的电子邮件。
- 通过 Amazon CloudWatch 告警操作获取通知。

有关如何使用 EventBridge 和 Lambda 函数自动响应 Trusted Advisor 的更多信息，请参阅 GitHub 中的 Trusted Advisor 工具。

注意

- Trusted Advisor 将尽最大效能传送事件。并不总是能保证将事件传送到 EventBridge。

- 您必须拥有 Amazon Web Services Support 计划才能为 Trusted Advisor 检查创建规则。有关更多信息，请参阅更改您的 Amazon Web Services Support 计划 (p. 16)。

按照以下过程为 Trusted Advisor 创建 EventBridge 规则。在创建事件规则之前，请执行以下操作：

- 熟悉 EventBridge 中的事件、规则和目标。有关更多信息，请参阅 Amazon EventBridge 用户指南中的什么是 Amazon EventBridge？。
- 创建将在事件规则中使用的目标。

### 为 Trusted Advisor 创建 EventBridge 规则

1. 访问 https://console.aws.amazon.com/events/，打开 Amazon EventBridge 控制台。
2. 要更改区域，请使用页面右上角的 Region selector（区域选择器），然后选择 US East (N. Virginia)（美国东部（弗吉尼亚北部））。
3. 在导航窗格中，选择 Rules (规则)。
4. 选择 Create rule (创建规则)。
5. 在 Define rule detail（定义规则详细信息）页面上，输入规则名称和描述。
6. 对于 Event bus（事件总线）和 Rule type（规则类型），保留默认值，然后选择 Next（下一步）。
7. 在 Build event pattern（构建事件模式）页面上，对于 Event source（事件源），选择 Amazon events or EventBridge partner events（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）。
9. 对于 Amazon Web Service，选择 Trusted Advisor。
10. 对于 Event type（事件类型），选择 Check Item Refresh Status（检查项目刷新状态）。
11. 为检查状态选择以下选项之一：
    - 选择 Any status（任何状态）以创建监控任何状态更改的规则。
    - 选择 Specific status(es)（特定状态），然后选择要让您的规则监控的值。
      - ERROR（错误）– Trusted Advisor 为检查建议某一操作。
      - INFO（信息）– Trusted Advisor 无法确定检查的状态。
      - OK（正常）– Trusted Advisor 没有检测到检查的问题。
      - WARN（警告）–Trusted Advisor 检测到检查可能存在问题并建议调查。
12. 为您的检查选择以下选项之一：
    - 选择 Any check（任何检查）。
    - 选择 Specific check(s)（特定检查），然后从列表中选择一个或多个检查名称。
13. 为 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 Specific resource ID(s) by ARN（按 ARN 排列的特定资源 ID），然后输入您想要的 Amazon Resource Name (ARN)。
14. 选择 Next (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 Next (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. 请选择 Create rule (创建规则)。您的规则现在将监控 Trusted Advisor 检查，然后将事件发送到您指定的目标。

# 创建 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）。例如，您可以创建告警，以跟踪 Service Limits 类别中的检查的状态变化。当您达到或超出您的 Amazon 账户的服务配额时，告警会通知您。

按照以下步骤为特定的 Trusted Advisor 指标创建 CloudWatch 告警。

主题



## 先决条件

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 Support API 来刷新您的检查并获取最新的检查结果。有关更多信息，请参阅刷新检查结果 (p. 32)。

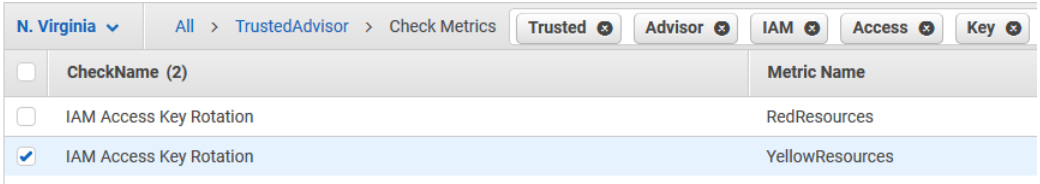
### 要为 Trusted Advisor 指标创建 CloudWatch 告警

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
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 Alarms (告警)。
4. 选择 Create Alarm (创建警报)。
5. 选择选择指标。
6. 对于指标，输入一个或多个维度值，以筛选指标列表。例如，您可以输入指标名称 ServiceLimitUsage 或维度，例如 Trusted Advisor 检查名称。

   Tip

   - 您可以搜索 **`Trusted Advisor`** 以列出服务的所有指标。
   - 有关指标和维度名称的列表，请参阅 Trusted Advisor 指标和维度 (p. 132)。
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。



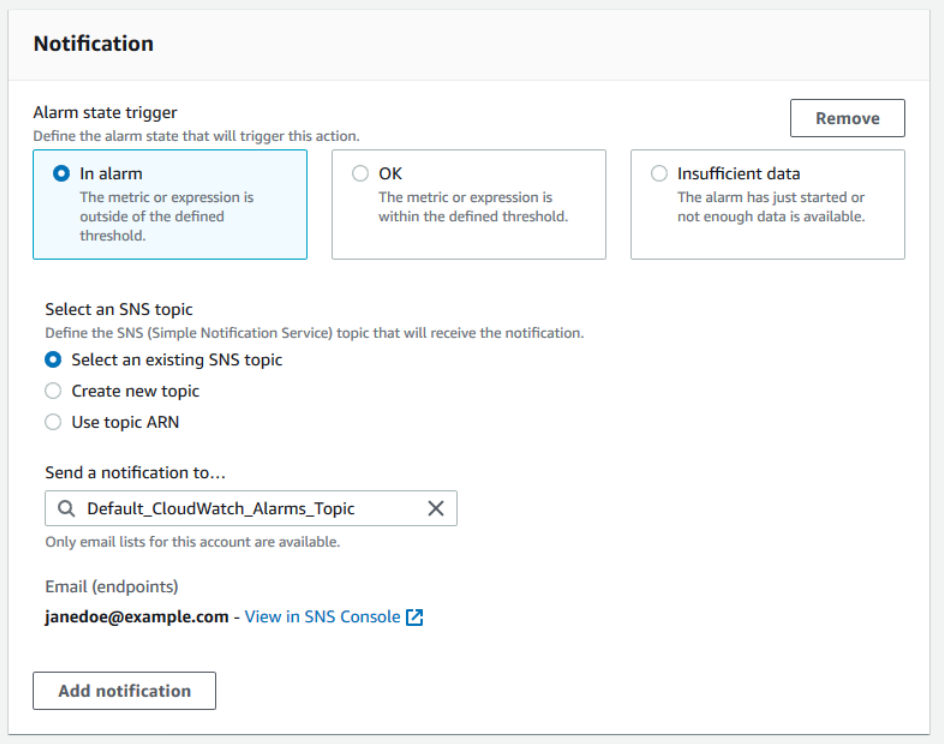

8. 选择选择指标。
9. 在 Specify metric and conditions（指定指标和条件）页面上，验证您选择的 Metric name（指标名称）和 CheckName（检查名称）显示在页面上。

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 Next (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 Next (下一步)。
16. 对于名称和描述，输入告警的名称和描述。
17. 选择 Next (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 Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-
east-1#s=Alarms&alarm=IAMAcessKeyRotationCheckAlarm

Alarm Details:
- Name:                       IAMAcessKeyRotationCheckAlarm
- Description:                This alarm starts when one or more 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。

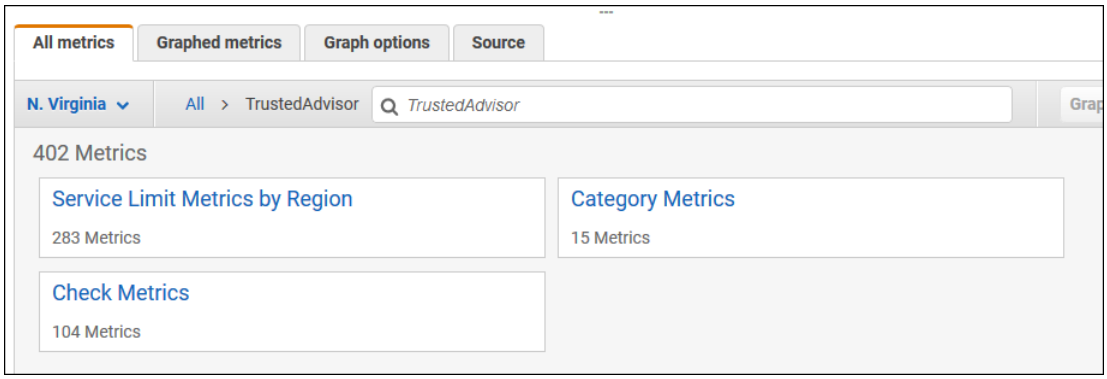
## 查看 Trusted Advisor 指标（控制台）

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. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
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 Metrics（指标）。
4. 输入指标命名空间，例如 **`TrustedAdvisor`**。

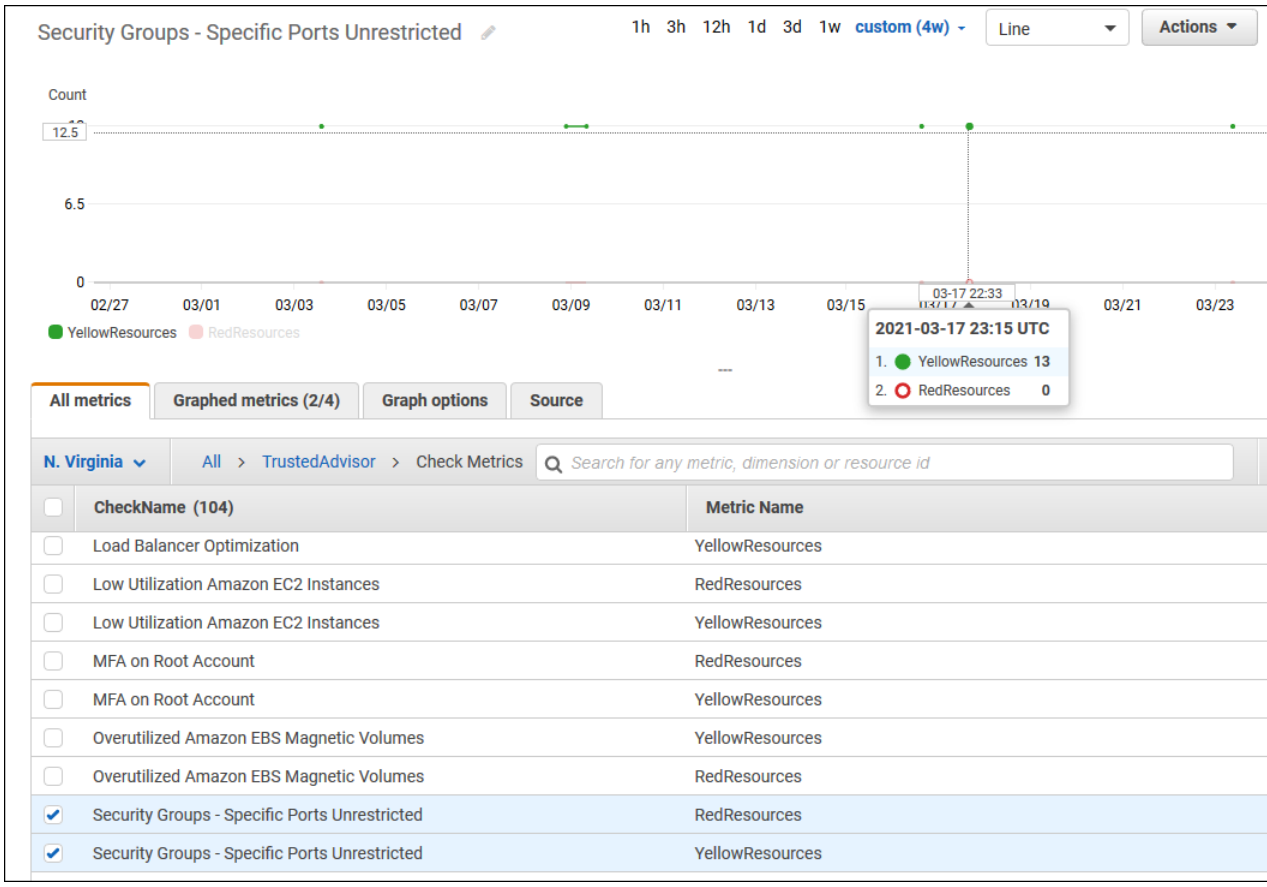
5. 选择指标维度，例如检查指标。




6. All metrics（所有指标）选项卡显示命名空间中该维度的指标。您可执行以下操作：

   a. 要对表进行排序，请选择列标题。
   b. 要为指标绘制图表，请选中该指标旁的复选框。要选择所有指标，请选中表的标题行中的复选框。
   c. 要按指标进行筛选，请选择指标名称，然后选择 Add to search（添加到搜索）。

   以下示例显示了安全组 - 不受限制的特定端口检查的结果。该检查标识 13 个黄色的资源。Trusted Advisor 建议您调查黄色的检查。




7. （可选）要将此图表添加到 CloudWatch 控制面板，请选择 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 类别级别指标

您可以将以下指标用于 Trusted Advisor 类别。

| 指标 | 描述 |
| --- | --- |
| GreenChecks | 处于绿色状态（未检测到任何问题）的 Trusted Advisor 检查的数量。 |
| RedChecks | 处于红色状态的 Trusted Advisor 检查数量（建议采取操作）。 |
| YellowChecks | 处于黄色状态的 Trusted Advisor 检查数量（建议调查）。 |

## Trusted Advisor 服务配额级指标

您可以使用以下有关 Amazon Web Service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。<br><br>您可以在 Trusted Advisor 控制台或 Amazon Trusted Advisor 检查引用 (p. 59) 中找到所有检查名称。 |

### 类别级别指标的维度

您可以将以下维度用于 Trusted Advisor 检查类别。

| 维度 | 描述 |
| --- | --- |
| Category | Trusted Advisor 检查类别的名称。<br><br>您可以在 Trusted Advisor 控制台或 查看检查类别 (p. 30) 页面中找到所有检查类别。 |

### 服务配额指标的维度

您可以将以下维度用于 Trusted Advisor 服务配额指标。

| 维度 | 描述 |
| --- | --- |
| Region | 服务限额的 Amazon Web Services 区域。 |
| ServiceName | Amazon Web Service 的名称。 |
| ServiceLimit | 服务配额的名称。<br><br>有关服务限额的更多信息，请参阅《Amazon 一般参考》中的 Amazon Web Service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》https://docs.amazonaws.cn/awscloudtrail/latest/userguide/。

## CloudTrail 中的 Trusted Advisor 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 Simple Storage Service（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：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

Trusted Advisor 支持将 Trusted Advisor 控制台操作的子集作为 CloudTrail 日志文件中的事件记录。CloudTrail 记录以下操作：

- `DescribeAccount`
- `DescribeAccountAccess`
- `DescribeChecks`
- `DescribeCheckItems`
- `DescribeCheckRefreshStatuses`
- `DescribeCheckSummaries`
- `DescribeNotificationPreferences`
- `DescribeOrganization`
- `DescribeOrganizationAccounts`
- `DescribeReports`
- `DescribeRisk`
- `DescribeRisks`
- `DescribeRiskResources`
- `DescribeServiceMetadata`
- `DownloadRisk`
- `ExcludeCheckItems`
- `GenerateReport`
- `IncludeCheckItems`
- `ListAccountsForParent`
- `ListRoots`
- `ListOrganizationalUnitsForParent`
- `RefreshCheck`
- `SetAccountAccess`
- `SetOrganizationAccess`
- `UpdateNotificationPreferences`
- `UpdateRiskStatus`

有关 Trusted Advisor 控制台操作的完整列表，请参阅 Trusted Advisor 操作 (p. 104)。

Note

CloudTrail 还会记录 Amazon Web Services Support API 参考中的 Trusted Advisor API 操作。有关更多信息，请参阅使用 Amazon Web Services Support 记录 Amazon CloudTrail API 调用 (p. 117)。

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身份用户的临时安全凭证发出的。
- 请求是否由其它 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

跟踪记录是一种配置，可用于将事件作为日志文件传送到您指定的 Simple Storage Service（Amazon S3）存储桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 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，该条目说明了 `UpdateNotificationPreferences` 操作。

```
{
   "eventVersion":"1.04",
   "userIdentity":{
      "type":"IAMUser",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/janedoe",
      "accountId":"123456789012",
      "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
      "userName":"janedoe",
      "sessionContext":{
         "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2020-10-21T22:06:18Z"
         }
      }
   },
   "eventTime":"2020-10-21T22:09:49Z",
   "eventSource":"trustedadvisor.amazonaws.com",
   "eventName":"UpdateNotificationPreferences",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"100.127.34.167",
   "userAgent":"signin.amazonaws.com",
   "requestParameters":{
      "contacts":[
         {
            "id":"billing",
            "type":"email",
            "active":false
         },
         {
            "id":"operational",
            "type":"email",
            "active":false
         },
         {
            "id":"security",
            "type":"email",
            "active":false
         }
      ],
      "language":"en"
   },
   "responseElements":null,
   "requestID":"695295f3-c81c-486e-9404-fa148EXAMPLE",
   "eventID":"5f923d8c-d210-4037-bd32-997c6EXAMPLE",
   "eventType":"AwsApiCall",
   "recipientAccountId":"123456789012"
}
```

### Example ：GenerateReport 的日志条目

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 `GenerateReport` 操作。此操作会为您的 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

Amazon EC2 为 Windows 实例提供了 EC2Rescue，客户可使用该工具检查其 Windows 实例以帮助识别常见问题、收集日志文件，以及帮助 Amazon Web Services Support 排查问题。您还可以使用 EC2Rescue 分析无法运行的实例的引导卷。有关更多信息，请参阅我如何使用 EC2Rescue 在自己的 EC2 Windows 实例上排除并修复问题？

## 特定于服务的问题排查

大多数 Amazon Web Service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 Support。下表提供了指向问题排查主题的链接（按服务排列）。

| 服务 | Link |
| --- | --- |
| Amazon Web Services | 排除 Amazon 签名版本 4 错误 |
| Amazon AppStream | Amazon AppStream 故障排除 |
| Amazon EC2 Auto Scaling | Auto Scaling 故障排除 |
| Amazon Certificate Manager (ACM) | 故障排除 |
| Amazon CloudFormation | Amazon CloudFormation 故障排除 |
| Amazon CloudFront | 问题排查 \| RTMP 分配问题排查 |
| Amazon CloudHSM | 故障排除 |
| Amazon CloudSearch | Amazon CloudSearch 故障排除 |
| Amazon CodeDeploy | Amazon CodeDeploy 故障排除 |
| Amazon Data Pipeline | 故障排除 |
| Amazon Direct Connect | Amazon Direct Connect 故障排除 |
| Amazon Directory Service | 排查 Amazon Directory Service 管理问题 |
| Amazon DynamoDB | 故障排除 |
| Amazon Elastic Beanstalk | 故障排除 |
| Amazon Elastic Compute Cloud (Amazon EC2) | 实例问题排查 \| Windows 实例问题排查 \| VM Import/Export 问题排查 \| API 请求错误排查 \| Amazon 管理包问题排查 \| Amazon Systems Manager for Microsoft SCVMM 问题排查 \| 适用于 Microsoft Windows 服务器的 Amazon 诊断 |
| Amazon Elastic Container Service (Amazon ECS) | Amazon ECS 故障排除 |
| Elastic Load Balancing | 对 Application Load Balancer 进行问题排查 \| 对 Classic Load Balancer 进行问题排查 |
| Amazon EMR (Amazon EMR) | 集群问题排查 |

| 服务 | Link |
| --- | --- |
| Amazon ElastiCache for Memcached | 对应用程序进行问题排查 |
| Amazon ElastiCache for Redis | 对应用程序进行问题排查 |
| Amazon Flow Framework | 问题排查和调试提示 |
| Amazon GovCloud (US) | 故障排除 |
| Amazon Identity and Access Management (IAM) | IAM 故障排除 |
| Kinesis | Kinesis 创建器问题排查 \| Kinesis 使用器问题排查 |
| Amazon Lambda | 使用 CloudWatch 诊断和监控 Amazon Lambda 函数 |
| Amazon OpsWorks | 调试和问题排查指南 |
| Amazon Redshift | 查询问题排查 \| 数据负载问题排查 \| Amazon Redshift 连接问题排查 \| Amazon Redshift 审核记录问题排查 |
| Amazon Relational Database Service (Amazon RDS) | 问题排查 \| 应用程序问题排查 |
| Amazon Route 53 | Amazon Route 53 问题排查 |
| Amazon Silk | 故障排除 |
| Amazon Simple Email Service (Amazon SES) | Amazon SES 故障排除 |
| Amazon Simple Storage Service (Amazon S3) | CORS 问题排查 \| 处理 REST 和 SOAP 错误 |
| 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 Virtual Private Cloud (Amazon VPC) | 故障排除 |
| Amazon WorkMail | Amazon WorkMail Web 应用程序故障排除 |
| Amazon WorkSpaces | Amazon WorkSpaces 管理问题排查 \| Amazon WorkSpaces 客户端问题排查 |
| Amazon WorkSpaces Application Manager (Amazon WAM) | Amazon WAM 应用程序故障排除 |

# 文档历史记录

下表介绍了自 Amazon Web Services Support 服务上一次发布以来对文档所做的重要更改。

- API 版本：2013-04-15

下表介绍了自 2021 年 5 月 10 日以来对 Amazon Web Services Support 和 Amazon Trusted Advisor 文档的重要更新。您可以订阅 RSS 源来接收有关更新的通知。

| update-history-change | update-history-description | update-history-date |
| --- | --- | --- |
| 更新了 Trusted Advisor 的文档 (p. 140) | Trusted Advisor 控制台中的 Preferences（首选项）页面进行了更新。有关更多信息，请参阅 Amazon Trusted Advisor 入门。 | 2022 年 7 月 15 日 |
| 更新了 Trusted Advisor 的文档 (p. 140) | 更新了检查以包含以下信息：<br>• Alert Criteria（提醒条件）<br>• Recommended Action（建议的操作）<br>• 其他资源<br>• Report columns（报告列）<br><br>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 Amazon Web Services Support 的文档 (p. 140) | 添加了介绍如何管理您的支持案例的文档。<br>• 更新现有的支持案例<br>• 故障排除 | 2022 年 6 月 28 日 |
| 更新了 `AWSSupportServiceRolePolicy` 的文档 (p. 140) | 更新了为服务相关角色提供账单、管理和支持服务的权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。 | 2022 年 6 月 23 日 |
| 更新了 Trusted Advisor 的文档 (p. 140) | Trusted Advisor 支持源自 Amazon Security Hub 的其他 Amazon 基础安全最佳实践安全标准控件。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查的日志。 | 2022 年 6 月 23 日 |
| 更新了 Trusted Advisor 的文档 (p. 140) | 添加了有关如何请求增加服务限额的更多信息。有关更多信息，请参阅服务限制。 | 2022 年 6 月 21 日 |
| 更新了 Amazon Web Services Support 的文档 (p. 140) | Support 中心控制台中的工单创建体验已经更新。有关更多信息，请参阅创建支持工单和工单管理。 | 2022 年 5 月 18 日 |

| | | |
|---|---|---|
| 更新了 Trusted Advisor 的文档 (p. 140) | 增加了适用于 Amazon EBS 和 Amazon Lambda 的四项检查。有关更多信息，请参阅启用 Amazon Compute Optimizer 以增加 Trusted Advisor 检查。 | 2022 年 5 月 4 日 |
| 更新了 `AWSSupportServiceRolePolicy` 的文档 (p. 140) | 增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 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 (p. 140) | 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 检查的日志。 | 2022 年 4 月 25 日 |
| 更新了 Trusted Advisor 的文档 (p. 140) | 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 检查的日志。 | 2022 年 3 月 29 日 |
| 更新了 `AWSSupportServiceRolePolicy` 的文档 (p. 140) | 增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。 | 2022 年 3 月 14 日 |
| 添加了 Amazon Trusted Advisor Priority 的文档 (p. 140) | 您可以使用 Amazon Trusted Advisor Priority 查看技术客户经理 (TAM) 提供的优先建议列表。有关更多信息，请参阅 Amazon Trusted Advisor Priority 入门。 | 2022 年 2 月 28 日 |
| 更新了将 Amazon EventBridge 用于 Trusted Advisor 的文档 (p. 140) | 您可以创建 EventBridge 规则以监控对您的 Trusted Advisor 检查的更改。有关更多信息，请参阅使用 EventBridge 监控 Amazon Trusted Advisor 检查结果。 | 2022 年 2 月 21 日 |
| 对于使用 Amazon EventBridge 来监控 Amazon Web Services Support 案例的新文档 (p. 140) | 您可以创建 EventBridge 规则以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 EventBridge 监控 Amazon Web Services Support 案例。 | 2022 年 2 月 21 日 |
| 更新了 `AWSSupportServiceRolePolicy` 的文档 (p. 140) | 增加了为服务相关角色提供账单、管理和支持服务的新权限。有关更多信息，请参阅 Amazon 托管策略：AWSSupportServiceRolePolicy。 | 2022 年 2 月 17 日 |
| 增加了有关与 Amazon Security Hub 集成的文档 (p. 140) | 现在，您可以在 Trusted Advisor 控制台中查看 Amazon 基础安全最佳实践安全标准中的 Security Hub 控件检查结果。有关更多信息，请参阅在 Amazon Trusted Advisor 控制台中查看 Amazon Security Hub 控件。 | 2022 年 1 月 18 日 |

| | | |
|---|---|---|
| 已更新的文档 (p. 140) | 如果您拥有 Enterprise On-Ramp Support 计划，则可以访问所有的 Trusted Advisor 检查和 Amazon Web Services Support API。 | 2021 年 11 月 24 日 |
| 更新了 Trusted Advisor 的文档 (p. 140) | Amazon Elasticsearch Reserved Instance Optimization 的检查名称已重命名为 Amazon OpenSearch Service Reserved Instance Optimization。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查的日志。 | 2021 年 9 月 8 日 |
| 更新了 Trusted Advisor 检查的文档 (p. 140) | 增加了所有 Trusted Advisor 检查的参考主题。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 (p. 140) | 更新了 Trusted Advisor 托管策略的文档 有关更多信息，请参阅 Amazon Web Services Support 和 Amazon Trusted Advisor 的 Amazon 托管策略。 | 2021 年 8 月 10 日 |
| 更新了 Trusted Advisor 的文档 (p. 140) | 更新了 Trusted Advisor 控制台的文档。有关更多信息，请参阅 Amazon Trusted Advisor 入门。 | 2021 年 7 月 16 日 |
| 更新了创建 Amazon Web Services Support 案例的文档 (p. 140) | 增加了有关如何为永久关闭的案例创建相关支持案例的文档。有关更多信息，请参阅重新打开已关闭的案例和创建相关案例。 | 2021 年 6 月 8 日 |
| 更新了 Trusted Advisor 的文档 (p. 140) | Trusted Advisor 增加了两个 Amazon Elastic Block Store (Amazon EBS) 卷存储的新检查。有关更多信息，请参阅更改 Amazon Trusted Advisor 检查的日志。 | 2021 年 6 月 8 日 |
| 已更新的文档 (p. 140) | 更新了以下主题：<br>• 更新了过程并将内容添加到创建 Amazon CloudWatch 告警以监控 Amazon Trusted Advisor 指标主题<br>• 增加了 Amazon Web Services Support API 的服务限额部分 | 2021 年 5 月 12 日 |

# 早期更新

| 更改 | 说明 | 日期 |
|---|---|---|
| 更新了 Trusted Advisor 的文档 | 增加了用于筛选、刷新和下载检查结果的文档。有关详细信息，请参阅以下章节： | 2021 年 3 月 16 日 |

| 更改 | 说明 | 日期 |
| --- | --- | --- |
| | • 筛选您的检查 (p. 31)<br>• 刷新检查结果 (p. 32)<br>• 下载检查结果 (p. 32) | |
| 更新了有关 Amazon 托管策略的文档 | 增加了有关 `AWSSupportServiceRolePolicy` Amazon 托管策略的信息。有关更多信息，请参阅将服务相关角色用于 Amazon Web Services Support (p. 91)。 | 2021 年 3 月 16 日 |
| 增加了 Amazon Lambda 的检查 | 在 更改 Amazon Trusted Advisor 检查的日志 (p. 80) 中增加了 Lambda 的 4 个 Amazon Trusted Advisor 检查。 | 2021 年 3 月 8 日 |
| 更新了 Amazon Elastic Block Store 的服务限制检查 | 在 更改 Amazon Trusted Advisor 检查的日志 (p. 80) 中更新了 Amazon EBS 的 5 个 Amazon Trusted Advisor 检查。 | 2021 年 3 月 5 日 |
| 更新了 CloudTrail 日志记录的文档 | CloudTrail 支持在您更改 Amazon Web Services Support 计划时对控制台操作进行日志记录。有关更多信息，请参阅记录对您的 Amazon Web Services Support 计划的更改 (p. 120)。 | 2021 年 2 月 9 日 |
| 更新了 Trusted Advisor 的文档 | 更新了 开始使用 Amazon Trusted Advisor (p. 29) 主题。 | 2021 年 1 月 29 日 |
| 更新了 Trusted Advisor 报告的文档 | 增加了将 Trusted Advisor 报告与其他 Amazon 服务结合使用的 Troubleshooting (p. 50) 部分。 | 2020 年 12 月 4 日 |
| 增加了对 Amazon CloudTrail 日志记录的 Amazon Trusted Advisor 支持 | CloudTrail 支持对 Trusted Advisor 控制台操作的子集进行日志记录。有关更多信息，请参阅使用 Amazon CloudTrail 记录 Amazon Trusted Advisor 控制台操作 (p. 133)。 | 2020 年 11 月 23 日 |
| 增加了更改日志主题 | 查看对 更改 Amazon Trusted Advisor 检查的日志 (p. 80) 中的 Amazon Trusted Advisor 检查和类别的更改。 | 2020 年 11 月 18 日 |
| 增加了对组织单位的支持 | 您现在可以为组织单位 (OU) 的 Trusted Advisor 检查创建报告。有关更多信息，请参阅创建组织视图报告 (p. 38)。 | 2020 年 11 月 17 日 |
| 使用 Amazon CloudTrail 主题更新了日志记录 | 增加了 Trusted Advisor API 操作的示例日志条目。请参阅Amazon Trusted AdvisorCloudTrail 日志记录中的 信息 (p. 118)。 | 2020 年 10 月 22 日 |
| 增加了 Amazon Web Services Support 配额 | 增加了有关 Amazon Web Services Support 的当前配额和限制的信息。请参阅 Amazon 一般参考中的 Amazon Web Services Support 终端节点和配额。 | 2020 年 8 月 4 日 |
| Amazon Trusted Advisor 的组织视图 | 您现在可以为属于 Amazon Organizations 部分的账户的 Trusted Advisor 检查创建报告。请参阅Amazon Trusted Advisor 的组织视图 (p. 37)。 | 2020 年 7 月 17 日 |
| 安全性和 Amazon Web Services Support | 更新了有关使用 Amazon Web Services Support 和 Trusted Advisor 时的安全注意事项的信息。请参阅 Amazon Web Services Support 中的安全性 (p. 84) | 2020 年 5 月 5 日 |

| 更改 | 说明 | 日期 |
| --- | --- | --- |
| 安全性和 Amazon Web Services Support | 添加了有关使用 Amazon Web Services Support 时的安全注意事项的信息。 | 2020 年 1 月 10 日 |
| 使用 Trusted Advisor 即 Web 服务 | 添加了有关在获取 Trusted Advisor 检查的列表后刷新 Trusted Advisor 的更新说明。 | 2018 年 11 月 1 日 |
| 使用服务相关角色 | 增加了新部分。 | 2018 年 7 月 11 日 |
| 入门：问题排查 | 增加了 Route 53 和 Amazon Certificate Manager 的问题排查链接。 | 2017 年 9 月 1 日 |
| 案例管理示例：创建案例 | 为拥有“基本”支持计划的用户添加了有关 CC 框的注释。 | 2017 年 8 月 1 日 |
| 通过 CloudWatch Events 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 Amazon CloudTrail 记录 Amazon Web Services Support 调用 | 增加了新部分。 | 2016 年 4 月 21 日 |
| 入门：问题排查 | 增加了更多问题排查链接。 | 2015 年 5 月 19 日 |
| 入门：问题排查 | 增加了更多问题排查链接。 | 2014 年 11 月 18 日 |
| 入门：案例管理 | 已更新以反映 Amazon Web Services Management Console中的 Amazon Service Catalog。 | 2014 年 10 月 30 日 |
| Amazon Web Services Support 案例生命周期编程 | 增加了有关新 API 元素的信息，通过这些元素可为案例添加附件并在检索案例历史记录时省略案例通信信息。 | 2014 年 7 月 16 日 |
| 访问 Amazon Web Services Support | 删除了指定支持联系人的访问方式。 | 2014 年 5 月 28 日 |
| 入门 | 增加了“入门”章节。 | 2013 年 12 月 13 日 |
| 初次发布 | 发布了新的 Amazon Web Services Support 服务。 | 2013 年 4 月 30 日 |

# Amazon术语表

最新的Amazon术语，请参阅Amazon术语表中的Amazon一般参考。