入门指南

AWS Management Console

版本 1.0

AWS Management Console: 入门指南

Table of Contents

那是什么 AWS Management Console？

AWS Management Console是一个 Web 应用程序，它包含并引用了用于管理 AWS 资源的广泛服务控制台。首次登录时，您会看到控制台主页。主页提供了对每个服务控制台的访问权限，并提供了访问执行 AWS 相关任务所需信息的单一位置。它还允许您通过添加、移除和重新排列诸如 “最近访问过”、“Healt AWS h” 等控件来自定义 Console Home 体验。

> **Note**
>
> 语言选择选项已移至新的 Unified Settings（统一设置）页面。有关更多信息，请参阅更改AWS Management Console的语言。

另一方面，单独的服务控制台提供了广泛的云计算工具，以及有关您账户和账单的信息。

使用您选择的设备

AWS Management Console适合在平板电脑以及其他种类的设备上工作：

- 水平和垂直空间最大化，可在屏幕上显示更多内容。
- 按钮和选择器更大，可获得更好的触控体验。

也可以作为一款适用于安卓和 iOS 的应用程序提供。 AWS Management Console 此应用程序提供移动相关任务，是完整 Web 体验的好搭档。例如，您可以通过手机轻松查看和管理现有的 Amazon EC2 实例和亚马逊 CloudWatch 警报。

你可以从亚马逊应用商店、Google Play 或 iTunes 下载 AWS 控制台移动应用程序。

配置 AWS Management Console

本主题介绍如何配置您的 AWS Management Console 以及如何使用统一设置页面来设置适用于所有服务控制台的默认设置。它还解释了小组件，这是控制台主页仪表板的一项功能，可让您添加用于跟踪 AWS 服务和资源信息的自定义组件。

主题

使用小组件

Console Home 控制面板包含一些小部件，用于显示有关您的 AWS 环境的重要信息并提供服务的快捷方式。您可以通过添加和删除小组件、重新排列它们或更改它们的大小来自定义体验。

添加小组件

1. 在控制台主页控制面板的右上角或右下角，选择 +添加小组件按钮。
2. 选择拖动指示器（由小组件标题栏左上角的六个垂直点表示），然后将其拖到控制台主页控制面板上。

删除小组件

1. 选择省略号，由小组件标题栏右上角的三个垂直点表示。
2. 选择 Remove widget（删除小组件）。

重新排列小组件

- 选择拖动指示器（由小组件标题栏左上角的六个垂直点表示），然后将小组件拖到控制台主页控制面板上的新位置。

调整小组件大小

- 选择小组件右下角的调整大小图标，然后拖动以调整小组件的大小。

如果您想重新组织和设置小组件，可以将控制台主页控制面板重置为默认布局。这将撤消对控制台主页控制面板布局的更改，并将所有小组件还原为其默认位置和大小。

将页面重置为默认布局

1. 在页面的右上角，选择重置为默认布局按钮。
2. 要确认，请选择重置。

> **Note**
>
> 这将撤消您对控制台主页控制面板布局的所有更改。

在控制台主页控制面板中请求新的小组件

1. 从控制台主页控制面板的左下角，选择想要有更多的小组件？ 那就告诉我们吧！

   描述您希望看到的在控制台主页控制面板中添加的小组件。
2. 选择提交。

> **Note**
>
> 您的建议会定期受到审查，并可能在将来对 AWS Management Console的更新中添加新的小组件。

配置统一设置

您可以从 “ AWS Management Console 统一设置” 页面配置设置和默认值，例如显示屏、语言和区域。视觉模式和默认语言也可以直接从导航栏进行设置。这些更改应用于所有服务控制台。

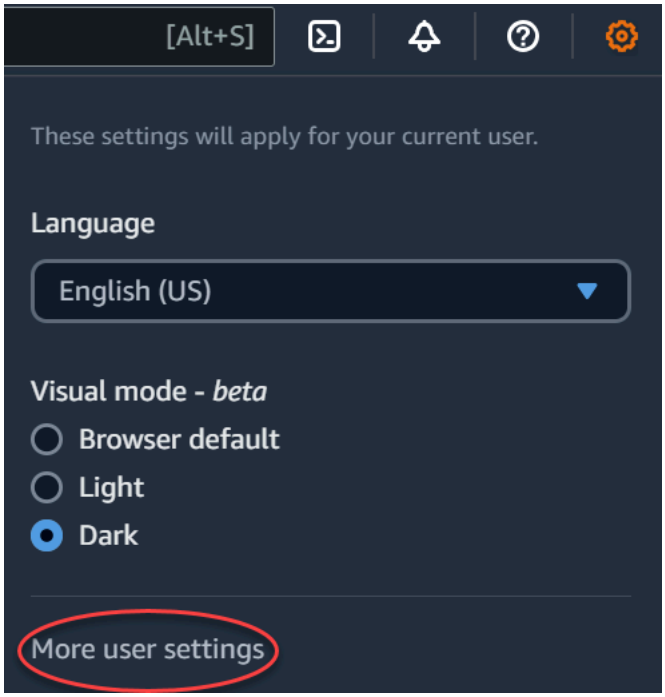
> **Important**
>
> 为确保您的设置、常用服务和最近访问的服务在全球范围内持续存在，这些数据将存储在所有区域 AWS 区域，包括默认禁用的区域。这些区域是非洲（开普敦）、亚太地区（香港）、亚太地区（海得拉巴）、亚太地区（雅加达）、欧洲（米兰）、欧洲（西班牙）、欧洲（苏黎世）、中东（巴林）和中东（阿联酋）。您还需要手动启用区域以访问它，并在该区域中创建和管理资源。如果您不想全部存储这些数据 AWS 区域，请选择 “全部重置” 以清除您的设置，然后在 “设置” 管理中选择不记住最近访问过的服务。

访问统一设置

以下过程描述了如何访问统一设置。

访问统一设置

1. 登录到 AWS Management Console。
2. 在导航栏中，选择齿轮图标。
3. 要打开统一设置页面，请选择更多用户设置。



重置统一设置

您可以删除所有统一设置配置并通过重置统一设置恢复默认设置。

> **Note**
>
> 这会影响多个区域 AWS，包括导航和 “服务” 菜单中的收藏服务、控制台主页小部件和中最近访问过的服务，以及适用于所有服务的设置，例如默认语言、默认区域和视觉模式。 AWS Console Mobile Application

重置所有统一设置

1. 登录到 AWS Management Console。
2. 在导航栏中，选择齿轮图标。
3. 选择 “更多用户设置”，打开 “统一设置” 页面。
4. 选择 “全部重置”。

编辑统一设置

以下过程描述了如何编辑您的首选设置。

编辑统一设置

1. 登录到 AWS Management Console。
2. 在导航栏中，选择齿轮图标。
3. 选择 “更多用户设置”，打开 “统一设置” 页面。
4. 选择首选设置旁的编辑：

   - 本地化和区域设置：
     - 语言可让您为控制台文本选择默认语言。
     - 默认区域可让您选择每次登录时应用的默认区域。您可为您的账户选择任何可用区域。还可以选择上次使用的区域作为默认区域。

       要了解 AWS Management Console中的区域路由的更多信息，请参阅选择区域。
   - 显示：
     - 视觉模式允许您将控制台设置为浅色模式、深色模式或浏览器的默认显示模式。

深色模式是一项测试版特征，可能不适用于所有 AWS 服务控制台。

- 收藏夹栏显示在带有图标的完整服务名称或仅服务图标之间切换收藏夹栏显示。
- 使用收藏夹栏图标大小可以将收藏夹栏显示上服务图标的大小在小（16x16 像素）和大（24x24 像素）之间切换。

- 设置管理：
  - 记住最近访问的服务允许你选择是否 AWS Management Console 记住你最近访问过的服务。关闭此功能还会删除您最近访问的服务历史记录，因此您将无法再在 “服务” 菜单或 Console Home 小组件中看到最近访问过的服务。 AWS Console Mobile Application

5. 选择保存更改。

更改视觉模式 AWS Management Console

您的视觉模式将您的主机设置为浅色模式、深色模式或浏览器的默认显示模式。

从导航栏更改视觉模式

1. 登录到 AWS Management Console。
2. 在导航栏中，选择齿轮图标。
3. 对于视觉模式，选择浅色表示浅色模式，选择深色表示深色模式，选择浏览器默认值则表示浏览器的默认显示模式。

在统一设置中更改默认语言

以下过程介绍如何使用导航栏更改默认语言。

从导航栏更改默认语言

1. 登录到 AWS Management Console。
2. 在导航栏中，选择齿轮图标。
3. 对于语言，选择浏览器默认值，或者从下拉列表中选择首选语言。

选择区域

对于许多服务，您可以选择一个 AWS 区域 来指定资源管理位置。区域是位于同一地理区域的一组 AWS 资源。您无需为AWS Management Console或某些服务选择区域，例如 AWS Identity and

Access Management。要了解有关 AWS 区域的更多信息，请参阅《AWS 一般参考》中的管理 AWS 区域。

选择区域

1. 登录到 AWS Management Console。
2. 选择某项服务可转到该服务的控制台。
3. 在导航栏中，选择当前所显示区域的名称。然后选择要切换到的区域。

选择默认区域

1. 在导航栏中，选择“设置”图标，然后选择更多用户设置以导航到统一设置页面。
2. 选择本地化和默认区域旁边的编辑。
3. 选择您的默认区域，然后选择保存设置。如果您没有选择默认区域，则您上次访问的区域将是默认区域。
4. （可选）选择 “转到新的默认区域” 以立即转到新的默认区域。

> **Note**
>
> 如果您已创建 AWS 资源，但在控制台中看不到这些资源，则控制台可能会显示来自其他地区的资源。某些资源（如 Amazon EC2 实例）特定于在其中创建它们的区域。要查看它们，请使用区域选择器选择包含您的资源的区域。

添加和删除收藏夹

要更快地访问常用服务，您可以将其服务控制台保存到收藏夹列表中。

向收藏夹列表中添加服务

1. 登录到 AWS Management Console。
2. 选择页面右上角或右下角的添加小组件按钮。
3. 在添加小组件菜单中，选择收藏夹以添加到控制台，然后选择添加。

   “收藏夹”将添加到控制台主页的底部。您可以通过选择小组件顶部的标题栏来拖放收藏夹，然后将小组件拖到页面上的新位置。

4. 在导航栏中，选择服务。
5. 在最近访问列表或所有服务列表中，将鼠标指针悬停在要添加为收藏项的服务的名称上。
6. 选择服务名称左侧的星号。
7. 重复前面的两个步骤，将更多服务添加到收藏夹列表。

从收藏夹列表中移除服务

1. 在导航栏中，选择 Services（服务）。
2. 请执行以下操作之一：
   - 在收藏夹列表中，请将鼠标指针悬停在服务的名称上。然后选择服务名称右侧的 x。
   - 在最近访问列表或所有服务列表中，取消选择收藏夹列表中服务名称旁边的星号。

更改密码

如果您是账户所有者，则可以从中更改您的 AWS 账户密码AWS Management Console。

更改 密码

1. 登录到 AWS Management Console。
2. 在导航栏中，选择您的账户名称。
3. 选择安全凭证。
4. 显示的选项将因您的 AWS 账户 类型而异。请按照控制台中显示的说明更改密码。
5. 输入一次您的当前密码，再输入两次新密码。

   新密码长度必须至少为 8 个字符，且必须包含以下内容：
   - 至少有一个符号
   - 至少有一个数字
   - 至少有一个大写字母
   - 至少有一个小写字母
6. 选择 Change Password（更改密码）或 Save changes（保存更改）。

更改语言 AWS Management Console

该 AWS Console Home 体验包括统一设置页面，您可以在其中更改 AWS 服务的默认语言 AWS Management Console。您也可以从“设置”菜单中快速更改默认语言，您可以从导航栏访问该菜单。可以在控制台的任何位置进行此更改。

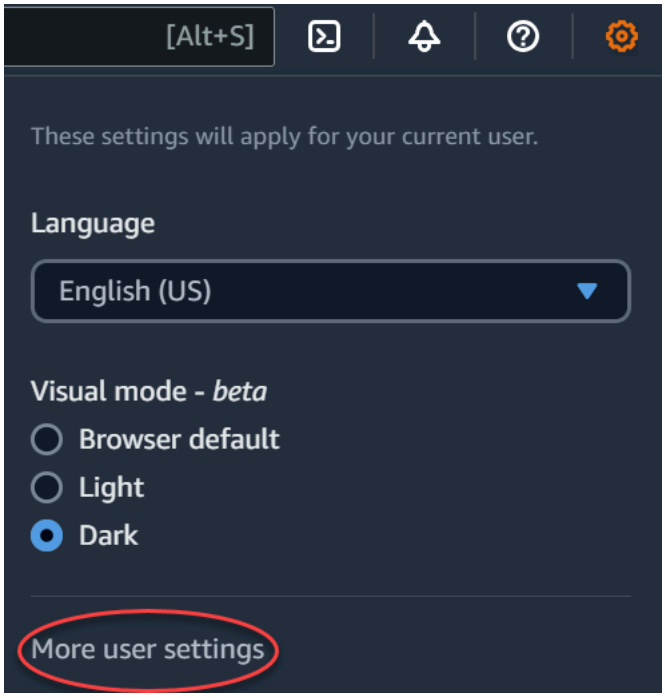
> **Note**
>
> 此过程会更改所有控制台的语言，但不会更改 AWS 文档的语言。要更改文档所用的语言，请使用任何文档页面右上角的语言菜单。

AWS Management Console 目前支持以下语言：

- 英语（美国）
- 英语（英国）
- 印度尼西亚语
- 德语
- French
- 日语
- 西班牙语
- 意大利语
- 葡萄牙语
- 韩语
- 中文（简体）
- 中文（繁体）

在“统一设置”中更改默认语言

1. 登录到 AWS Management Console。
2. 在导航栏中，选择“设置”图标。
3. 要打开统一设置页面，请选择更多用户设置。



4. 在统一设置中，选择本地化和默认区域旁边的编辑。
5. 要为控制台选择所需的语言，请选择以下选项之一：

   - 从下拉列表中选择浏览器默认样式，然后选择保存设置。

     所有 AWS 服务的控制台文本均以您在浏览器设置中设置的首选语言显示。

     > **Note**
     >
     > 浏览器默认仅支持 AWS Management Console支持的语言。

   - 从下拉列表中选择首选的语言，然后选择保存设置。

     所有 AWS 服务的控制台文本均以您的首选语言显示。

从导航栏更改默认语言

1. 登录到 AWS Management Console。
2. 在导航栏中，选择“设置”图标。
3. 对于语言，请选择浏览器默认值，或者从下拉列表中选择首选语言。

开始使用服务

AWS Management Console提供多种方式来导航到各个服务控制台。

要打开某项服务的控制台

请执行下列操作之一：

- 在导航栏上的搜索框中，输入服务的全部或部分名称。在 Services (服务) 下方，从搜索结果列表中选择您需要的服务。有关更多信息，请参阅使用统一搜索搜索产品、服务、功能等。
- 在最新访问的服务小组件中，选择一个服务名称。
- 在最新访问的服务小组件中，选择查看所有 AWS 服务. 然后，在所有 AWS 服务页面上，选择一个服务名称。
- 在导航栏中，选择 Services (服务) 可打开完整的服务列表。然后在最新访问或所有服务的下方选择服务。

使用统一搜索搜索产品、服务、功能等

导航栏中的搜索框提供了一个统一的搜索工具，用于追踪 AWS 服务和功能、服务文档和 AWS Marketplace。只需输入几个字符即可查看所有这些类别的结果。键入的字符越多，搜索就越优化搜索结果。

搜索服务、功能、文档或 AWS Marketplace 产品

1. 在导航栏的搜索框中 AWS Management Console，输入全部或部分搜索词。
2. 执行以下任一操作来优化您的搜索并获得更多详细信息：
   - 要将结果缩小到所需的内容类型，请选择左侧的类别之一。
   - 要查看特定类别的更多结果，请按每个类别标题选择查看所有 ***n*** 个结果。要返回到主结果列表，请选择左上角的返回。
   - 要快速导航到服务的热门功能，请暂停结果中的服务名称并选择链接。
   - 要获取有关文档或 AWS Marketplace 结果的更多详细信息，请将鼠标悬停在结果标题上。
3. 选择任何链接以导航到您的预期服务、主题或 AWS Marketplace 页。

> **Tip**
>
> 您还可以使用键盘快速导航到顶部搜索结果。首先，按 Alt+S (Windows) 或 Option+s (macOS) 访问搜索栏。然后开始输入您的搜索词。当预期的结果显示在列表顶部时，按 Enter。例如，要快速导航到 Amazon EC2 控制台，请输入 ec2，然后按 Enter。

与 Amazon Q 开发者交谈

Amazon Q Developer 是一款生成式人工智能 (AI) 驱动的对话助手，可以帮助您理解、构建、扩展和操作 AWS 应用程序。您可以向 Amazon Q 询问任何相关问题 AWS，包括 AWS 架构、您的 AWS 资源、最佳实践、文档等方面的问题。您还可以创建支持案例并从在线客服那里获得帮助。有关更多信息，请参阅什么是 Amazon Q？ 在 Amazon Q 开发者用户指南中。

开始使用 Amazon Q

您可以通过选择六角形的 Amazon Q 图标开始在 AWS Management Console、 AWS 文档网站、AWS 网站或 C AWS onsole Mobile Application 中与 Amazon Q 聊天。有关更多信息，请参阅 Amazon Q 开发者用户指南中的 Amazon Q 开发者入门。

示例问题

以下是您可以向 Amazon Q 提问的一些示例问题：

- How do I get billing support?
- How do I create an EC2 instance?
- How do I troubleshoot a "Failed to load" error?
- How do I close an AWS account?
- Can you connect me with a person?

我的应用程序在开 AWS什么？

myApplications 是控制台主页的一个扩展，可帮助您在 AWS上管理和监控应用程序的成本、运行状况、安全状况和性能。您可以通过一个视图访问账户中的所有应用程序、所有应用程序的关键指标，以及来自多个服务控制台的成本、安全和运营指标的概述以及见解 AWS Management Console。myApplications 包括以下内容：

- 控制台主页上的应用程序小组件
- 可用于查看应用程序资源成本和安全性调查发现的 myApplications
- 提供成本、性能和安全性调查发现等关键应用程序指标视图的 myApplications 控制面板

myApplications 的功能

- 创建应用程序 – 创建新应用程序并组织其资源。您的应用程序会自动显示在 MyApplications 中，因此您可以在 AWS Management Console、API、CLI 和 SDK 中执行操作。基础设施即代码 (IaC) 是在您创建应用程序时生成的，可从 myApplication 控制面板进行访问。IaC 可用于 IaC 工具，包括 AWS CloudFormation 和 Terraform。
- 访问您的应用程序 – 通过从 myApplications 小组件进行选择即可快速访问您的任何应用程序。
- 比较应用程序指标 – 使用 myApplications 比较应用程序的关键指标，例如多个应用程序的应用程序资源成本和关键安全性调查发现的数量。
- 监控和管理应用程序 — 使用警报、金丝雀和服务级别目标、调查结果和成本趋势 Amazon CloudWatch，评估应用程序的运行状况和性能。 AWS Security Hub AWS Cost Explorer Service您还可以从 AWS Systems Manager中找到计算指标摘要和优化，并管理资源合规性和配置状态。

相关服务

myApplicions 使用以下服务：

- AppRegistry
- AppManager
- Amazon CloudWatch
- Amazon EC2
- AWS Lambda
- AWS 资源探索器

- AWS Security Hub
- Systems Manager
- AWS Service Catalog
- 标记

访问 myApplications

您可以通过在 AWS Management Console的左侧边栏中选择 myApplications 来访问 myApplications。

定价

MyApplic AWS ations on 不收取额外费用。没有安装费或预先承诺。myApplication 控制面板汇总的底层资源和服务的使用费仍按这些资源的公布费率收取。

支持的区域

MyApplications 有以下 AWS 区域版本：

- 美国东部（俄亥俄）
- 美国东部（弗吉尼亚州北部）
- 美国西部（加利福尼亚北部）
- 美国西部（俄勒冈州）
- 亚太地区（孟买）
- 亚太地区（大阪）
- 亚太地区（首尔）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（东京）
- 加拿大（中部）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲地区（伦敦）
- 欧洲地区（巴黎）

- 欧洲（斯德哥尔摩）
- 南美洲（圣保罗）

选择加入的区域

默认情况下未启用选择加入区域 您必须手动启用这些区域才能对这些区域使用 myApplications。有关的更多信息 AWS 区域，请参阅管理 AWS 区域。支持以下选择加入区域：

- Africa (Cape Town)
- 亚太地区（香港）
- 亚太地区（海得拉巴）
- 亚太地区（雅加达）
- 亚太地区（墨尔本）
- 欧洲地区（米兰）
- 欧洲（西班牙）
- 欧洲（苏黎世）
- 中东（巴林）
- 中东（阿联酋）
- 以色列（特拉维夫）

开始使用 myApplications

要开始使用 myApplications 创建、监控和管理您的应用程序，请按照以下步骤操作。

步骤 1：创建 应用程序

创建新应用程序或加入在 2023 年 11 月 8 日之前创建的现有 AppRegistry 应用程序，开始使用 MyApplications。

Create an application

创建应用程序

1. 登录到 AWS Management Console。
2. 在左侧边栏中，选择 myApplications。

3. 选择创建应用程序。
4. 输入应用程序的名称。
5. （可选）输入应用程序的描述。
6. （可选）添加标签。标签是应用于资源的键值对，用于保存有关该资源的元数据。

> **Note**
>
> AWS 应用程序标签会自动应用于新创建的应用程序，并可用于识别与您的应用程序关联的资源。有关更多信息，请参阅《AWS Service Catalog AppRegistry 管理员指南》中的 AWS 应用程序标签。

7. （可选）添加属性组。您可以使用属性组来存储应用程序元数据。
8. 选择下一步。
9. （可选）添加现有资源：

> **Note**
>
> 要搜索和添加资源，必须开启 AWS 资源探索器。有关更多信息，请参阅入门 AWS 资源探索器。
> 所有添加的资源都使用 AWS 应用程序标签进行标记。

   a. 选择选择资源。
   b. （可选）选择视图。
   c. 搜索资源。您可以按关键字、名称或类型进行搜索，也可以选择资源类型。

> **Note**
>
> 如果找不到要查找的资源，请使用进行故障排除 AWS 资源探索器。有关更多信息，请参阅《资源探索器用户指南》中的资源探索器搜索问题排查。

   d. 选中要添加的资源旁的复选框。
   e. 选择添加。
   f. 选择下一步。
10. 查看您的选择。
11. 如果要关联堆 AWS CloudFormation 栈，请选中页面底部的复选框。

> **Note**
>
> 向应用程序添加 AWS CloudFormation 堆栈需要更新堆栈，因为添加到应用程序的所有资源都标有 AWS 应用程序标签。在此更新后，堆栈上次更新后执行的手动配置可能不会反映出来。这可能会导致停机或其他应用程序问题。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的堆栈资源的更新行为。

12. 选择创建应用程序。

Onboard existing application

载入现有 AppRegistry 应用程序

1. 登录到 AWS Management Console。
2. 在左侧边栏中，选择 myApplications。
3. 使用搜索栏查找应用程序。
4. 选择您的应用程序。
5. 选择载入######。
6. 如果要关联 CloudFormation 堆栈，请选中警报框中的复选框。
7. 选择载入应用程序。

步骤 2：查看应用程序

您可以通过卡片视图或表格视图，查看所有区域或特定地区的应用程序及其相关信息。

查看应用程序

1. 在左侧边栏中，选择 myApplications。
2. 在区域中，选择当前区域或支持的区域。
3. 要查找特定应用程序，请在搜索栏中输入其名称、关键字或描述。
4. （可选）默认视图是卡片视图。要自定义您的应用程序页面，请执行以下操作：
   a. 选择齿轮图标。
   b. （可选）选择页面大小。
   c. （可选）选择卡片视图或表格视图。

d. （可选）选择页面大小。

e. （可选）如果使用表格视图，请选择表格视图的属性。

f. （可选）切换哪些应用程序属性可见及其显示顺序。

g. 选择确认。

管理 应用程序

本主题介绍如何管理应用程序。

编辑应用程序

将打开编辑您的应用程序 AppRegistry ，以便您可以更新其描述。您还可以 AppRegistry 使用编辑应用程序的标签和属性组。

编辑应用程序

1. 打开 AWS Management Console。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 选择要编辑的应用程序。
4. 在 myApplication 控制面板上，选择操作，然后选择编辑应用程序。
5. 在编辑应用程序描述中，更新描述，然后选择保存更改。

编辑标签

- 按照《AWS Service Catalog AppRegistry 管理员指南》中的 “管理标签” 中的步骤进行操作。

编辑属性组

- 按照《AWS Service Catalog AppRegistry 管理员指南》中编辑属性组中的步骤进行操作。

删除应用程序

您可以删除不再需要的应用程序。

删除应用程序

1. 打开 AWS Management Console。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 选择要删除的应用程序。
4. 在 myApplication 控制面板上，选择操作。
5. 选择删除应用程序。
6. 选择删除。
7. 确认删除，然后选择删除应用程序。

创建代码段

myApplications 会为您的所有应用程序创建代码段。您可以使用代码段，通过基础设施即代码 (IaC) 工具将新创建的资源自动添加到应用程序中。所有添加的资源都使用 AWS 应用程序标签进行标记，以将其与您的应用程序关联。

为应用程序创建代码段

1. 打开 AWS Management Console。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 搜索并选择一个应用程序。
4. 选择操作。
5. 选择获取代码段。
6. 选择代码段类型。
7. 选择复制将代码复制到剪贴板。
8. 将代码粘贴到 IaC 工具中。

管理资源

本主题介绍如何管理资源。

添加资源

向应用程序添加资源使您能够对它们进行分组并管理其安全性、性能和合规性。

添加资源

1. 打开 AWS Management Console。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 搜索并选择一个应用程序。
4. 选择管理资源。
5. 选择 Add resource (添加资源)。
6. （可选）选择视图。
7. 搜索资源。您可以按关键字、名称或类型进行搜索，也可以选择资源类型。

> **Note**
>
> 如果找不到要查找的资源，请使用进行故障排除 AWS 资源探索器。有关更多信息，请参阅《资源探索器用户指南》中的资源探索器搜索问题排查。

8. 选中要添加的资源旁的复选框。
9. 选择添加。

移除资源

您可以移除资源以取消它们与应用程序的关联。

移除资源

1. 打开 AWS Management Console。
2. 在控制台的左侧边栏中，选择 myApplications。
3. 搜索并选择一个应用程序。
4. 选择管理资源。
5. （可选）选择视图。
6. 搜索资源。您可以按关键字、名称或类型进行搜索，也可以选择资源类型。

> **Note**
>
> 如果找不到要查找的资源，请使用进行故障排除 AWS 资源探索器。有关更多信息，请参阅《资源探索器用户指南》中的资源探索器搜索问题排查。

7. 选择移除。
8. 通过选择移除资源，确认您要移除该资源。

myApplications 控制面板

您创建或载入的每个应用程序都有自己的 myApplications 控制面板。MyApplications 仪表板包含成本、安全和操作小部件，可显示来自多个 AWS 服务的见解。您可以对每个小组件执行收藏、重新排序、移除或调整大小操作。有关更多信息，请参阅 使用小组件。

应用程序控制面板设置小组件

此小组件包含建议的入门活动列表，您可以使用这些活动来帮助您 AWS 服务 进行配置以管理应用程序资源。

应用程序摘要小组件

此小组件显示应用程序的名称、描述和 AWS 应用程序标签。您可以在基础设施即代码 (IAC) 中访问和复制应用程序标签以手动标记资源。

计算小组件

此小组件显示您添加到应用程序中的计算资源的信息和指标。这包括警报总数和计算资源类型总数。该小组件还显示了 Amazon EC2 实例 CPU 利用率和 Lambda 调 Amazon CloudWatch 用的资源性能指标趋势图。

配置计算小组件

要在计算小组件中填充数据，请为您的应用程序设置至少一个 Amazon EC2 实例或一个 Lambda 函数。有关更多信息，请参阅 Amazon Elastic Compute Cloud 文档和《AWS Lambda 开发人员指南》中的 Lambda 入门。

成本和使用情况小组件

此小组件显示您的应用程序资源 AWS 的成本和使用情况数据。您可以使用这些数据来比较每月成本并按 AWS 服务查看成本明细。此小组件仅汇总标有 AWS 应用程序标签的资源的成本，不包括税费、费用和其他与资源没有直接关联的共享成本。显示的成本是非混合的，每 24 小时至少更新一次。有关更多信息，请参阅《AWS Cost Management User Guide》中的 Analyzing your costs with AWS 资源探索器。

配置成本和使用情况小组件

要配置 “成本和使用情况” 微件，请 AWS Cost Explorer Service 为您的应用程序和账户启用。这项服务不收取额外费用，也没有安装费或预先承诺。有关更多信息，请参阅《AWS Cost Management User Guide》中的 Enabling Cost Explorer。

AWS 安全控件

此小组件显示来自应用程序 AWS 安全性的安全调查结果。 AWS Security 为您的应用程序提供了全面的安全发现视图 AWS。您可以按严重性访问最近的高优先级调查发现，监控其安全状况，访问最近的关键或高严重性调查发现，并深入了解后续步骤。有关更多信息，请参阅 AWS Security Hub。

配置 “ AWS 安全” 微件

要配置 “ AWS 安全” 小组件，请 AWS Security Hub 为您的应用程序和帐户进行设置。有关更多信息，请参阅什么是 AWS Security Hub？ 在《AWS Security Hub 用户指南》中。有关定价信息，请参阅《AWS Security Hub User Guide》中的 AWS Security Hub free trial, usage, and pricing。

AWS Security Hub 需要您配置 AWS Config 录制。该服务提供与您的 AWS 账户关联的资源的详细视图。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 AWS Systems Manager。

DevOps 小部件

此小组件显示运维洞察，使您可以评估合规性并对应用程序采取行动。这些洞察包括：

- 队列管理
- 状态管理
- 补丁管理
- 配置和 OpsItems 管理

配置 DevOps 小部件

要配置 DevOps 微件，请 AWS Systems Manager OpsCenter 为您的应用程序和帐户启用。有关更多信息，请参阅 S ystems Manager Explorer 入门和 OpsCenter《AWS Systems Manager 用户指南》。启用 OpsCenter AWS Systems Manager Explorer 允许配置 AWS Config 和， Amazon CloudWatch 以便 OpsItems 根据常用的规则和事件自动创建其事件。有关更多信息，请参阅《AWS Systems Manager 用户指南》 OpsCenter中的设置。

您可以将实例配置为让 Systems Manager 代理运行并应用权限以启用补丁扫描。有关更多信息，请参阅《AWS Systems Manager 用户指南》中的 AWS Systems Manager Quick Setup。

您还可以通过设置补丁管理器为您的应用程序设置自动修补 Amazon EC2 实例。 AWS Systems Manager 有关更多信息，请参阅《AWS Systems Manager 用户指南》中的使用 Quick Setup 补丁策略。

有关定价信息，请参阅 AWS Systems Manager 定价。

监控和运维小组件

此小组件显示：

- 与应用程序关联的资源的警报和提醒
- 应用程序服务级别目标 (SLO) 和指标
- 可用 AWS 应用程序信号指标

配置监控和运维小组件

要配置 “监控和操作” 微件，请在您的 AWS 账户中创建 CloudWatch 警报和金丝雀。有关更多信息，请参阅《亚马逊 CloudWatch 用户指南》中的 “使用亚马逊 CloudWatch 警报” 和 “创建金丝雀”。有关 CloudWatch 警报和合成金丝雀定价，请分别参阅 Amazon CloudWatch 定价和AWS 云运营和迁移博客。

有关 CloudWatch 应用程序信号的更多信息，请参阅《亚马逊 CloudWatch 用户指南》中的 “启用亚马逊 CloudWatch 应用程序见解”。

标签小组件

此小组件显示与您的应用程序关联的所有标签。您可以使用此小组件来跟踪和管理应用程序元数据（重要程度、环境、成本中心）。有关更多信息，请参阅什么是标签？ 在《标记 AWS 资源的最佳实践》AWS 白皮书中。

AWS Management Console 私密访问权限

AWS Management Console 私人访问是一项高级安全功能，用于控制对的访问 AWS Management Console。 AWS Management Console 当您想要防止用户从您的网络中意外 AWS 账户 登录时，私有访问权限非常有用。使用此功能，当流量来自您的网络内部 AWS 账户 时，您可以将访问权限限制为 AWS Management Console 仅限于一组已知的指定人群。

主题

支持 AWS 区域的、服务控制台和功能

AWS Management Console 私有访问仅支持部分区域和 AWS 服务。不受支持的服务控制台在 AWS Management Console中将处于非活动状态。此外，在使用 AWS Management Console 私有访问权限时，某些 AWS Management Console 功能可能会被禁用，例如，统一设置中的默认区域选择。

支持以下区域和服务控制台。

支持的区域

- 美国东部（俄亥俄）
- 美国东部（弗吉尼亚州北部）
- 美国西部（加利福尼亚北部）
- 美国西部（俄勒冈）
- 亚太地区（海得拉巴）
- 亚太地区（孟买）
- 亚太地区（首尔）
- 亚太地区（大阪）

- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（东京）
- 加拿大（中部）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲地区（伦敦）
- 欧洲地区（巴黎）
- 欧洲（斯德哥尔摩）
- 南美洲（圣保罗）
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- 亚太地区（雅加达）
- 亚太地区（墨尔本）
- 加拿大西部（卡尔加里）
- 欧洲地区（米兰）
- 欧洲（西班牙）
- 欧洲（苏黎世）
- 中东（巴林）
- 中东（阿联酋）
- 以色列（特拉维夫）

支持的服务控制台

- Amazon API Gateway
- AWS App Mesh
- AWS Application Migration Service
- Amazon Athena
- AWS Auto Scaling
- AWS Billing Conductor
- AWS Certificate Manager

- AWS Cloud Map
- Amazon CloudFront
- Amazon CloudWatch
- AWS CodeArtifact
- AWS CodeBuild
- Amazon CodeGuru
- Amazon Comprehend
- Amazon Comprehend Medical
- AWS Compute Optimizer
- AWS Console Home
- AWS Database Migration Service
- AWS DeepRacer
- Amazon DocumentDB
- Amazon DynamoDB
- Amazon EC2
- Amazon EC2 全局视图
- EC2 Image Builder
- Amazon EC2 Instance Connect
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- AWS Elastic Disaster Recovery
- Amazon Elastic File System
- Amazon Elastic Kubernetes Service
- Amazon ElastiCache
- Amazon EMR
- Amazon EventBridge
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue DataBrew
- AWS Ground Station

- Amazon GuardDuty
- AWS Identity and Access Management
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- Amazon Kendra
- AWS Key Management Service
- Amazon Kinesis
- 适用于 Apache Flink 的亚马逊托管服务
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- AWS License Manager
- Amazon Managed Grafana
- Amazon Managed Streaming for Apache Kafka
- Amazon Managed Workflows for Apache Airflow (MWAA)
- AWS Migration Hub 策略建议
- Amazon MQ
- 网络访问分析器
- AWS Network Manager
- 亚马逊 OpenSearch 服务
- AWS Organizations
- Amazon S3 on Outposts
- 亚马逊 SageMaker Runtime
- Amazon SageMaker 合成数据
- AWS Secrets Manager
- 服务限额
- AWS Signer
- Amazon Simple Email Service
- Amazon Simple Queue Service

- Amazon Simple Storage Service (Amazon S3)
- AWS SQL Workbench
- AWS Step Functions
- AWS Support
- AWS Systems Manager
- AWS Transfer Family
- 统一设置
- Amazon VPC IP 地址管理器

AWS Management Console 私密访问安全控制概述

AWS Management Console 上来自您的网络的账户限制

AWS Management Console 当您希望将 AWS Management Console 来自网络的访问权限限制为仅限于组织中已知 AWS 账户 的指定集合时，私有访问非常有用。这样，您可以防止用户从您的网络内登录到意外的 AWS 账户 。您可以使用 AWS Management Console VPC 端点策略实现这些控制。有关更多信息，请参阅 实施服务控制策略和 VPC 端点策略。

从您的网络到互联网的连接

要访问使用的资产，例如静态内容（、CSS AWS Management Console JavaScript、图像）以及所有 AWS 服务 未由启用的资产，仍需要您的网络连接AWS PrivateLink。有关使用的顶级域的列表 AWS Management Console，请参阅故障排除。

> **Note**
>
> 目前， AWS Management Console 私有访问不支持`status.aws.amazon.com`、`health.aws.amazon.com`和之类的终端节点`docs.aws.amazon.com`。您需要将这些域路由到公共互联网。

所需的 VPC 端点和 DNS 配置

AWS Management Console 私有访问每个区域需要以下两个 VPC 终端节点。将 *region* 替换为您自己的区域信息。

1. com.amazonaws。 ## .console 适用于 AWS Management Console
2. com.amazonaws。 ## .signin for AWS 登录

> **Note**
>
> 始终为美国东部（弗吉尼亚州北部）（us-east-1）区域预调配基础设施和网络连接，而与用于 AWS Management Console的其他区域无关。您可以使用 AWS Transit Gateway 设置美国东部（弗吉尼亚州北部）与每个其它区域之间的连接。有关更多信息，请参阅《Amazon VPC Transit Gateway 指南》中的开始使用中转网关。您也可以使用 Amazon VPC 对等连接。有关更多信息，请参阅《Amazon VPC 对等连接指南》中的什么是 VPC 对等连接。要比较这些选项，请参阅《Amazon Virtual Private Cloud 连接选项》白皮书中的 Amazon VPC 到 Amazon VPC 连接选项。

DNSAWS Management Console 和的配置 AWS 登录

要将您的网络流量路由到相应的 VPC 端点，请在您的用户将从中访问 AWS Management Console的网络中配置 DNS 记录。这些 DNS 记录会将您的用户浏览器流量引导至您创建的 VPC 端点。

您可以创建单个托管区。但是，诸如 `health.aws.amazon.com` 和 `docs.aws.amazon.com` 之类的端点将无法访问，因为它们没有 VPC 端点。您需要将这些域路由到公共互联网。我们建议您为每个区域创建两个私有托管区（一个用于 `signin.aws.amazon.com`，一个用于 `console.aws.amazon.com`）以及以下 CNAME 记录：

- 区域 CNAME 记录（所有区域）
- region.signin.aws.amazon.com 指向登录区域中的 VPC 终端节点 AWS 登录 DNS
- region.console.aws.amazon.com 指向控制台区域中的 VPC 终端节 AWS Management Console 点 DNS
- 仅针对美国东部（弗吉尼亚州北部）区域的无区域 CNAME 记录。您必须始终设置美国东部（弗吉尼亚州北部）区域。
  - signin.aws.amazon.com 指向美国东部（弗吉尼亚北部）的 VP AWS 登录 C 终端节点 (us-east-1)
  - console.aws.amazon.com 指向美国东部（弗吉尼亚北部）的 VP AWS Management Console C 终端节点 (us-east-1)

有关创建 CNAME 记录的说明，请参阅《Amazon Route 53 开发人员指南》中的处理记录。

一些 AWS 游戏机（包括 Amazon S3）的DNS名称使用不同的模式。下面是两个示例：

- support.console.aws.amazon.com
- s3.console.aws.amazon.com

为了能够将此流量定向到您的 AWS Management Console VPC 终端节点，您需要单独添加这些名称。我们建议您为所有端点配置路由，以获得完全私密的体验。但是，使用 AWS Management Console 私有访问权限并不是必需的。

以下json文件包含要按区域配置的 AWS 服务完整列表和控制台终端节点。使用 `com.amazonaws.region.console` 端点下方的 `PrivateIpv4DnsNames` 字段作为 DNS 名称。

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

> **Note**
>
> 随着我们向 AWS Management Console 私有访问的范围中添加其他端点，此列表每月都会更新。要保持更新您的私有托管区，请定期提取前面的文件列表。

如果您使用 Route 53 来配置 DNS，请前往 https://console.aws.amazon.com/route53/v2/hostedzones# 验证 DNS 设置。对于 Route 53 中的每个私有托管区，验证是否存在以下记录集。

- console.aws.amazon.com
- signin.aws.amazon.com
- region.console.aws.amazon.com
- region.signin.aws.amazon.com
- support.console.aws.amazon.com
- global.console.aws.amazon.com
- 先前列出的 JSON 文件中存在的其他记录

VPC 终端节点和 AWS 服务DNS配置

AWS 服务 通过直接浏览器请求和由 Web 服务器代理的请求组合进行的 AWS Management Console 调用。要将此流量定向到您的 AWS Management Console VPC 终端节点，您必须添加 VPC 终端节点 DNS并为每项依赖 AWS 服务进行配置。

以下json文件列出了可供您 AWS 服务 使用的 AWS PrivateLink 支持文件。如果某项服务未与集成 AWS PrivateLink，则该服务不会包含在这些文件中。

- https://configuration.private-access.console.amazonaws.com/us-east-1.config.json
- https://configuration.private-access.console.amazonaws.com/us-east-2.config.json
- https://configuration.private-access.console.amazonaws.com/us-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-northeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-southeast-2.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-1.config.json
- https://configuration.private-access.console.amazonaws.com/ap-south-2.config.json
- https://configuration.private-access.console.amazonaws.com/ca-central-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-1.config.json
- https://configuration.private-access.console.amazonaws.com/eu-west-2.config.json
- https://configuration.private-access.console.amazonaws.com/il-central-1.config.json

对于要添加到 VPC 的相应服务的 VPC 端点使用 `ServiceName` 字段。

> **Note**
>
> 随着我们增加对更多服务控制台的 AWS Management Console 私有访问的支持，我们每个月都会更新此列表。为了保持最新状态，请定期提取前面的文件列表并更新您的 VPC 端点。

实施服务控制策略和 VPC 端点策略

您可以使用服务控制策略 (SCP) 和 VPC 终端节点策略进行 AWS Management Console 私有访问，以限制允许 AWS Management Console 从您的 VPC 及其连接的本地网络中使用该策略的账户集。

将 AWS Management Console 私有访问权限与 AWS Organizations 服务控制策略配合使用

如果您的 AWS 组织正在使用允许特定服务的服务控制策略 (SCP)，则必须添加`signin:*`允许的操作。之所以需要此权限，是因为 AWS Management Console 通过私有访问 VPC 终端节点登录会执行 IAM 授权，SCP 会在未经许可的情况下阻止该授权。例如，以下服务控制策略允许在组织中使用 Amazon EC2 和 CloudWatch 服务，包括使用 AWS Management Console 私有访问终端节点访问它们的时间。

```
{
  "Effect": "Allow",
  "Action": [
    "signin:*",
    "ec2:*",
    "cloudwatch:*",
    ... Other services allowed
  },
  "Resource": "*"
}
```

有关 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略 (SCP)。

仅允许 AWS Management Console 用于预期的账户和组织（可信身份）

AWS Management Console 并 AWS 登录 支持专门控制登录账户身份的 VPC 终端节点策略。

与其它 VPC 端点策略不同，该策略在身份验证之前进行评估。因此，它专门控制登录和使用经过身份验证的会话，而不控制会话采取的任何 AWS 特定于服务的操作。例如，当会话访问 AWS 服务控制台（例如 Amazon EC2 控制台）时，将不会根据为显示该页面而采取的 Amazon EC2 操作来评估这些

VPC 终端节点策略。相反，您可以使用与已登录的 IAM 委托人关联的 IAM 策略来控制其对服务操作的权限。 AWS

> **Note**
>
> AWS Management Console 和 VPC 终端节点的 SignIn VPC 终端节点策略仅支持有限的策略公式子集。每个 `Principal` 和 `Resource` 均应设置为 `*`，而 `Action` 应设置为 `*` 或 `signin:*`。您可以使用 `aws:PrincipalOrgId` 和 `aws:PrincipalAccount` 条件键控制对 VPC 端点的访问。

对于控制台和 SignIn VPC 终端节点，建议使用以下策略。

此 VPC 终端节点策略允许 AWS 账户 在指定 AWS 组织中登录，并禁止登录任何其他账户。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgId": "o-xxxxxxxxxxx"
        }
      }
    }
  ]
}
```

此 VPC 终端节点策略将登录限制为特定账户列表， AWS 账户 并禁止登录任何其他账户。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
```

```
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": [ "111122223333", "222233334444" ]
        }
      }
    }
  ]
}
```

在登录时会对限制 AWS 账户 或组织使用 AWS Management Console 和登录 VPC 端点的策略进行评估，并定期针对现有会话进行重新评估。

实施基于身份的策略和其他策略类型

您可以 AWS 通过创建策略并将其附加到 IAM 身份（用户、用户组或角色）或 AWS 资源来管理中的访问权限。本页介绍策略与 AWS Management Console 私有访问权限配合使用时的工作原理。

支持的 AWS 全局条件上下文密钥

AWS Management Console 私有访问不支持`aws:SourceVpce`和`aws:VpcSourceIp` AWS 全局条件上下文密钥。在使用 AWS Management Console 私有访问时，您可以在策略中改用 `aws:SourceVpc` IAM 条件。

AWS Management Console 私有访问权限如何与 aws 配合使用：SourceVpc

本节介绍由您生成的请求 AWS Management Console 可以进入的各种网络路径 AWS 服务。通常， AWS 服务控制台是通过直接浏览器请求和由 AWS Management Console Web 服务器代理的请求混合实现的。 AWS 服务这些实现可能会发生变化，恕不另行通知。如果您的安全要求包括 AWS 服务 使用 VPC 终端节点进行访问，我们建议您为打算从 VPC 使用的所有服务（无论是直接使用还是通过 AWS Management Console 私有访问）配置 VPC 终端节点。此外，您必须在`aws:SourceVpc`策略中使用 IAM 条件，而不是在 AWS Management Console 私有访问权限功能中使用特定`aws:SourceVpce`值。本节提供有关不同网络路径的工作原理的详细信息。

用户登录后 AWS Management Console，他们 AWS 服务 通过直接浏览器请求和由 AWS Management Console Web 服务器代理到服务器的请求的组合向 AWS 发出请求。例如， CloudWatch 图形数据请求是直接从浏览器发出的。而某些 AWS 服务控制台请求（例如 Amazon S3）则由 Web 服务器代理到 Amazon S3。

对于直接的浏览器请求，使用 AWS Management Console 私有访问权限不会有任何改变。与以前一样，请求通过 VPC 已配置为到达 monitoring.region.amazonaws.com 的任何网络路径到达服务。如果 VPC 配置了的 VPC 终端节点com.amazonaws.region.monitoring，则请求将 CloudWatch通过该 CloudWatch VPC 终端节点到达。如果没有 VPC 终端节点 CloudWatch，则请求将通过 VPC CloudWatch 上的 Internet Gateway 到达其公有终端节点。 CloudWatch 通过 CloudWatch VPC 终端节点到达的请求将具有 IAM 条件`aws:SourceVpc`并`aws:SourceVpce`设置为各自的值。那些 CloudWatch 通过其公共端点到达的用户将`aws:SourceIp`设置为请求的源 IP 地址。有关这些 IAM 条件键的更多信息，请参阅《IAM 用户指南》中的全局条件键。

对于由 AWS Management Console Web 服务器代理的请求，例如 Amazon S3 控制台在您访问 Amazon S3 控制台时发出的列出您的存储桶的请求，则网络路径会有所不同。这些请求不是从您的 VPC 发起的，因此不使用您可能已在 VPC 上为该服务配置的 VPC 端点。在这种情况下，即使您具有用于 Amazon S3 的 VPC 端点，您的会话向 Amazon S3 发出的旨在列出桶的请求也不会使用 Amazon S3 VPC 端点。但是，当您对支持的服务使用 AWS Management Console 私有访问权限时，这些请求（例如，对 Amazon S3 的请求）将在其请求上下文中包含`aws:SourceVpc`条件密钥。`aws:SourceVpc`条件密钥将设置为部署用于登录和控制台的 AWS Management Console 私有访问终端节点的 VPC ID。因此，如果您在基于身份的策略中使用 `aws:SourceVpc` 限制，则必须添加用于托管 AWS Management Console 私有访问登录和控制台端点的此 VPC 的 VPC ID。`aws:SourceVpce` 条件将设置为相应的登录或控制台 VPC 端点 ID。

> **Note**
>
> 如果您的用户要求访问 AWS Management Console 私有访问不支持的服务控制台，则必须在用户的基于身份的策略中使用 `aws:SourceIP` 条件键包括预期公有网络地址的列表（例如本地网络范围）。

不同的网络路径如何反映在 CloudTrail

您生成的请求所使用的不同网络路径 AWS Management Console 会反映在您的 CloudTrail 事件历史记录中。

对于直接的浏览器请求，使用 AWS Management Console 私有访问权限不会有任何改变。 CloudTrail 事件将包括有关连接的详细信息，例如用于调用服务 API 的 VPC 终端节点 ID。

对于由 AWS Management Console Web 服务器代理的请求， CloudTrail 事件将不包含任何与 VPC 相关的细节。但是，建立浏览器会话所需的初始请求（例如`AwsConsoleSignIn`事件类型）将在事件详细信息中包含 AWS 登录 VPC 终端节点 ID。 AWS 登录

试试 AWS Management Console 私密访问

本节介绍如何在新账户中设置和测试 AWS Management Console 私有访问权限。

AWS Management Console 私有访问是一项高级安全功能，需要具备网络和设置 VPC 的相关知识。本主题介绍如何在没有全面基础设施的情况下试用 AWS Management Console 私有访问。

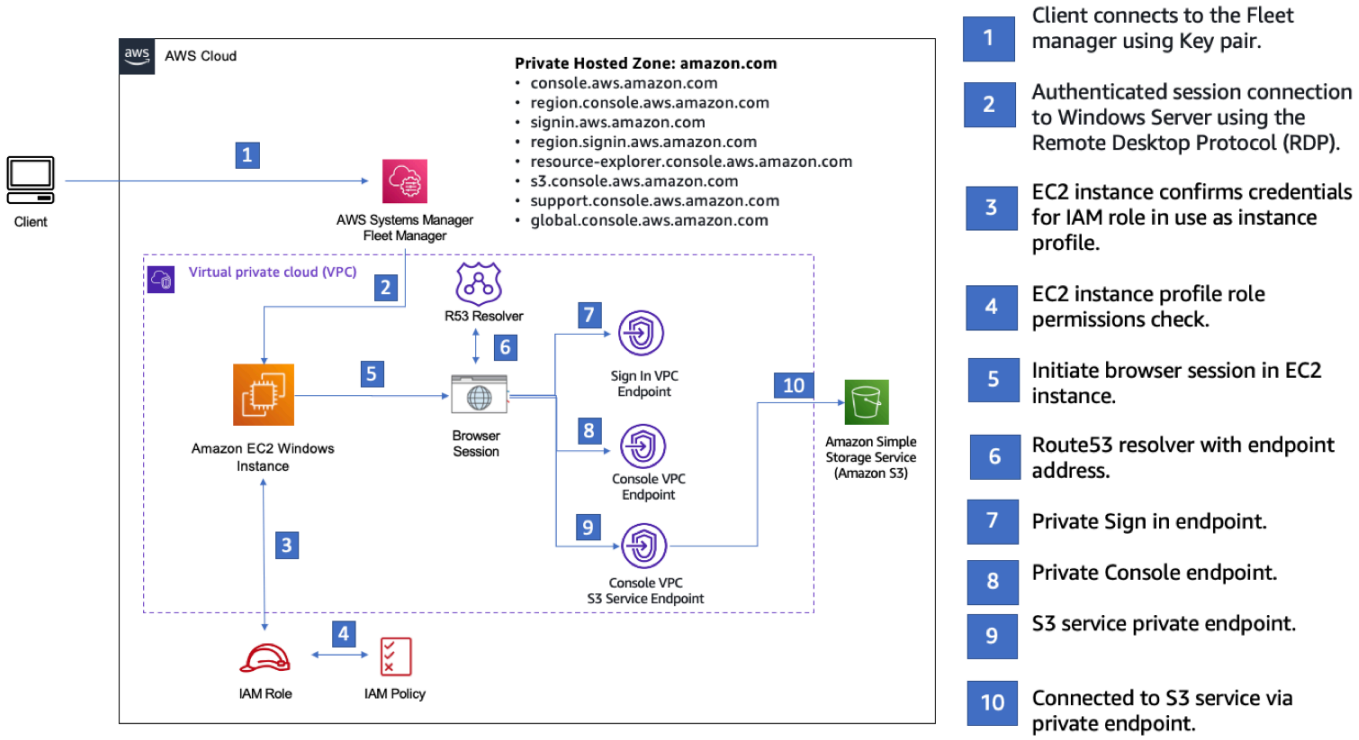
主题

使用 Amazon EC2 测试设置

Amazon Elastic Compute Cloud (Amazon EC2) 在 Amazon Web Services 云中提供可扩展的计算容量。您可以使用 Amazon EC2 启动所需数量的虚拟服务器，配置安全性和联网以及管理存储。在此设置中，我们使用 Fleet Manager（ AWS Systems Manager的一项功能），通过远程桌面协议（RDP）连接到 Amazon EC2 Windows 实例。

本指南演示了一个测试环境，用于设置和体验从 Amazon EC2 实例到亚马逊简单存储服务的 AWS Management Console 私有访问连接。本教程 AWS CloudFormation 用于创建和配置 Amazon EC2 用于可视化此功能的网络设置。

下图描述了使用 Amazon EC2 访问 AWS Management Console 私有访问设置的工作流程。它显示了用户如何使用私有端点连接到 Amazon S3。



复制以下 AWS CloudFormation 模板并将其保存到您将在设置网络过程的第三步中使用的文件中。

> **Note**
>
> 此 AWS CloudFormation 模板使用的配置目前在以色列（特拉维夫）地区不受支持。

AWS Management Console 私有访问环境 Amazon EC2 AWS CloudFormation 模板

```
Description: |
  AWS Management Console Private Access.
Parameters:
  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  Ec2KeyPair:
    Type: AWS::EC2::KeyPair::KeyName
    Description: The EC2 KeyPair to use to connect to the Windows instance
```

```
  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PublicSubnet3CIDR:
    Type: String
    Default: 172.16.2.0/24
    Description: CIDR range for Public Subnet C

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

  PrivateSubnet3CIDR:
    Type: String
    Default: 172.16.3.0/24
    Description: CIDR range for Private Subnet C

  LatestWindowsAmiId:
    Type: 'AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>'
    Default: '/aws/service/ami-windows-latest/Windows_Server-2022-English-Full-Base'

  InstanceTypeParameter:
    Type: String
    Default: 't2.medium'


Resources:

##########################
# VPC AND SUBNETS
##########################
```

```
AppVPC:
  Type: 'AWS::EC2::VPC'
  Properties:
    CidrBlock: !Ref VpcCIDR
    InstanceTenancy: default
    EnableDnsSupport: true
    EnableDnsHostnames: true

PublicSubnetA:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet1CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 0
        - Fn::GetAZs: ""

PublicSubnetB:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet2CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 1
        - Fn::GetAZs: ""

PublicSubnetC:
  Type: 'AWS::EC2::Subnet'
  Properties:
    VpcId: !Ref AppVPC
    CidrBlock: !Ref PublicSubnet3CIDR
    MapPublicIpOnLaunch: true
    AvailabilityZone:
      Fn::Select:
        - 2
        - Fn::GetAZs: ""

PrivateSubnetA:
  Type: 'AWS::EC2::Subnet'
```

```
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone:
        Fn::Select:
          - 0
          - Fn::GetAZs: ""

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone:
        Fn::Select:
          - 1
          - Fn::GetAZs: ""

  PrivateSubnetC:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet3CIDR
      AvailabilityZone:
        Fn::Select:
          - 2
          - Fn::GetAZs: ""

  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
```

```
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

########################
# Route Tables
########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PrivateSubnetRouteTableAssociation3:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetC

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
```

```
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB

  PublicSubnetBRouteTableAssociation3:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetC


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock

  EC2SecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Default EC2 Instance SG
```

```
      VpcId: !Ref AppVPC

########################
# VPC ENDPOINTS
########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSSM:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssm'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceEc2messages:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ec2messages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSsmmessages:
    Type: 'AWS::EC2::VPCEndpoint'
```

```
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.ssmmessages'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
        - !Ref PrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

##########################
# ROUTE53 RESOURCES
##########################
```

```
  ConsoleHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleSupportProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "support.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ExplorerProxyRecordGlobal:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: "resource-explorer.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 ConsoleRecordRegional:
   Type: AWS::Route53::RecordSet
   Properties:
     HostedZoneId: !Ref 'ConsoleHostedZone'
     Name: !Sub "${AWS::Region}.console.aws.amazon.com"
     AliasTarget:
       DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
       HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
     Type: A

 SigninHostedZone:
   Type: "AWS::Route53::HostedZone"
   Properties:
     HostedZoneConfig:
```

```
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# EC2 INSTANCE
#########################

  Ec2InstanceRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          -
            Effect: Allow
            Principal:
```

```
            Service:
              - ec2.amazonaws.com
          Action:
            - sts:AssumeRole
    Path: /
    ManagedPolicyArns:
      - arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore

Ec2InstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Path: /
    Roles:
     - !Ref Ec2InstanceRole

EC2WinInstance:
  Type: 'AWS::EC2::Instance'
  Properties:
    ImageId: !Ref LatestWindowsAmiId
    IamInstanceProfile: !Ref Ec2InstanceProfile
    KeyName: !Ref Ec2KeyPair
    InstanceType:
      Ref: InstanceTypeParameter
    SubnetId: !Ref PrivateSubnetA
    SecurityGroupIds:
      - Ref: EC2SecurityGroup
    BlockDeviceMappings:
      - DeviceName: /dev/sda1
        Ebs:
          VolumeSize: 50
    Tags:
    - Key: "Name"
      Value: "Console VPCE test instance"
```

设置网络

1. 登录您所在组织的管理账户并打开 AWS CloudFormation 控制台。
2. 选择创建堆栈。
3. 选择使用新资源（标准）。上传您之前创建的 AWS CloudFormation 模板文件，然后选择 “下一步”。
4. 输入堆栈的名称（例如 **PrivateConsoleNetworkForS3**），然后选择下一步。

5. 对于 VPC 和子网，输入您的首选 IP CIDR 范围，或使用提供的默认值。如果您使用默认值，请确认它们不与您的现有 VPC 资源重叠 AWS 账户。
6. 对于 E KeyPair c 2 参数，请从您账户中的现有 Amazon EC2 密钥对中选择一个。如果您没有现有的 Amazon EC2 密钥对，必须先创建一个密钥对，然后转至下一步。有关更多信息，请参阅 Amazon EC2 用户指南中的使用 Amazon EC2 创建密钥对。
7. 选择创建堆栈。
8. 创建堆栈后，选择资源选项卡以查看已创建的资源。

连接到 Amazon EC2 实例

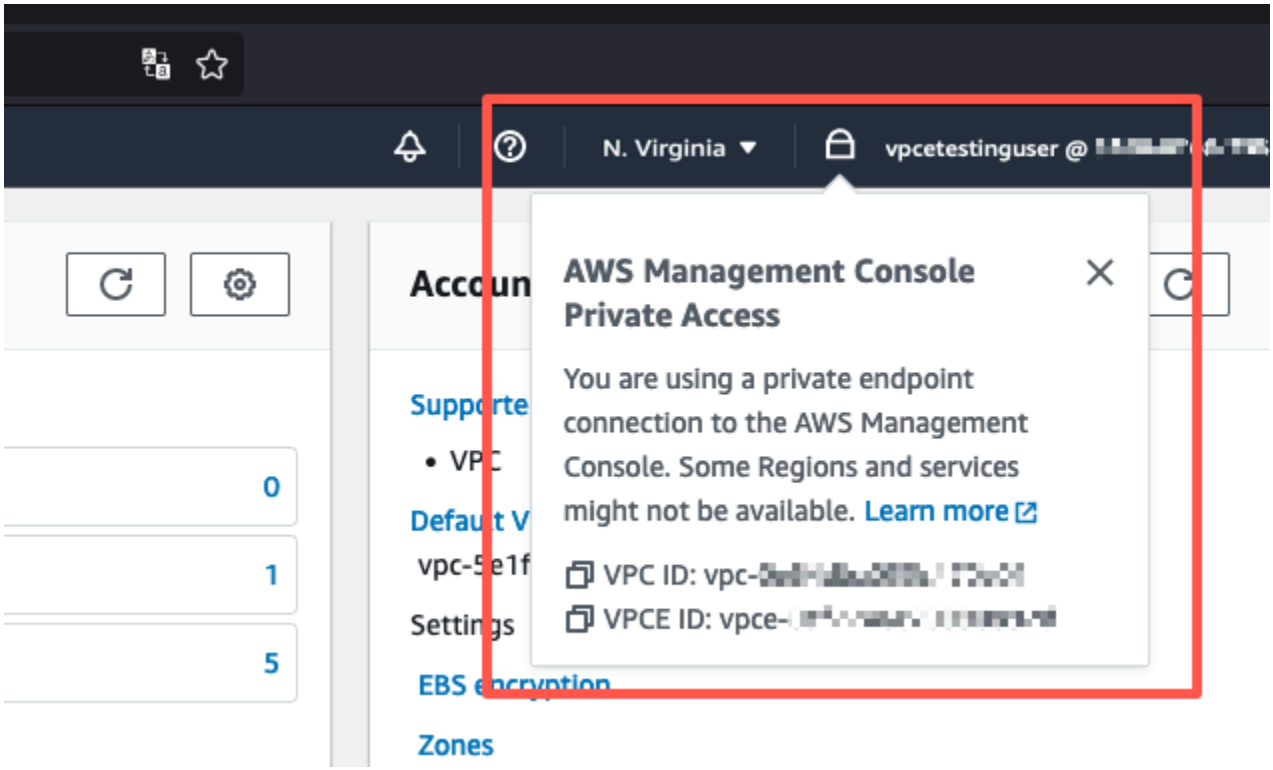
1. 登录您所在组织的管理账户并打开 Amazon EC2 控制台。
2. 在导航窗格中，选择实例。
3. 在 “实例” 页面上，选择由模板创建的 Cons ole VPCE 测试实例。 AWS CloudFormation 然后选择连接。

> **Note**
>
> 此示例使用队列管理器（一种功能）连接到您的 Windows 服务器。 AWS Systems Manager Explorer可能需要几分钟才能开始连接。

4. 在连接到实例页面上，选择 RDP 客户端，然后使用 Fleet Manager 进行连接。
5. 选择 Fleet Manager 远程桌面。
6. 要获取 Amazon EC2 实例的管理密码并使用网页界面访问 Windows 桌面，请使用与您在创建 AWS CloudFormation 模板时使用的 Amazon EC2 密钥对关联的私钥。
7. 在 Amazon EC2 Windows 实例中， AWS Management Console 在浏览器中打开。
8. 使用 AWS 凭证登录后，打开 Amazon S3 控制台并确认您已使用 AWS Management Console 私有访问权限进行连接。

测试 AWS Management Console 私有访问设置

1. 登录您所在组织的管理账户并打开 Amazon S3 控制台。
2. 在导航栏中选择锁定私有图标，以查看所使用的 VPC 端点。以下屏幕截图显示了锁定私有图标的位置和 VPC 信息。



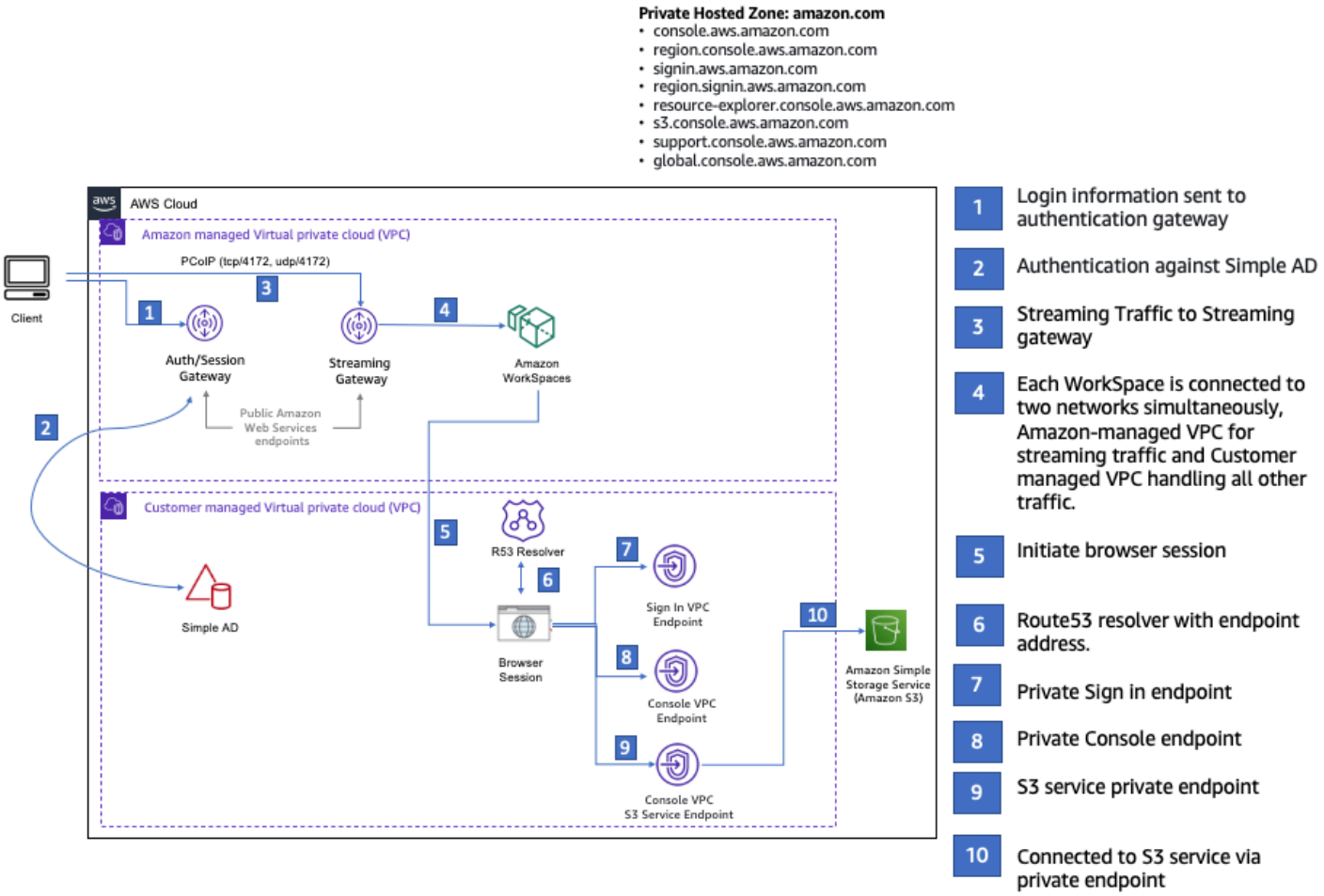
使用 Amazon 测试设置 WorkSpaces

亚马逊 WorkSpaces 允许您为用户配置虚拟的、基于云的 Windows、Amazon Linux 或 Ubuntu Linux 桌面，称为。 WorkSpaces您可以根据需求的变更，快速添加或删除用户。用户可以从多个设备或 Web 浏览器访问自己的虚拟桌面。要了解更多信息 WorkSpaces，请参阅《Amazon WorkSpaces 管理指南》。

本节中的示例描述了一个测试环境，在该环境中，用户环境使用在上运行的 Web 浏览器登录 P AWS Management Console ri WorkSpace vate Access。然后，用户访问 Amazon Simple Storage Service 控制台。 WorkSpace 这旨在模拟企业用户在连接到 VPC 的网络上使用笔记本电脑，通过浏览器访问 AWS Management Console 的体验。

本教程用于创建和配置网络设置和要使用的简单 Active Directory， WorkSpaces 以及 WorkSpace 使用设置的分步说明 AWS Management Console。 AWS CloudFormation

下图描述了使用测试 AWS Management Console 私有 WorkSpace 访问设置的工作流程。它显示了客户端 WorkSpace、Amazon 托管 VPC 和客户托管 VPC 之间的关系。



复制以下 AWS CloudFormation 模板并将其保存到一个文件中，您将在步骤的第 3 步中使用该文件来设置网络。

AWS Management Console 私有访问环境 AWS CloudFormation 模板

```
Description: |
  AWS Management Console Private Access.
Parameters:

  VpcCIDR:
    Type: String
    Default: 172.16.0.0/16
    Description: CIDR range for VPC

  PublicSubnet1CIDR:
    Type: String
    Default: 172.16.1.0/24
```

```
    Description: CIDR range for Public Subnet A

  PublicSubnet2CIDR:
    Type: String
    Default: 172.16.0.0/24
    Description: CIDR range for Public Subnet B

  PrivateSubnet1CIDR:
    Type: String
    Default: 172.16.4.0/24
    Description: CIDR range for Private Subnet A

  PrivateSubnet2CIDR:
    Type: String
    Default: 172.16.5.0/24
    Description: CIDR range for Private Subnet B

# Amazon WorkSpaces is available in a subset of the Availability Zones for each
 supported Region.
# https://docs.aws.amazon.com/workspaces/latest/adminguide/azs-workspaces.html
Mappings:
  RegionMap:
    us-east-1:
      az1: use1-az2
      az2: use1-az4
      az3: use1-az6
    us-west-2:
      az1: usw2-az1
      az2: usw2-az2
      az3: usw2-az3
    ap-south-1:
      az1: aps1-az1
      az2: aps1-az2
      az3: aps1-az3
    ap-northeast-2:
      az1: apne2-az1
      az2: apne2-az3
    ap-southeast-1:
      az1: apse1-az1
      az2: apse1-az2
    ap-southeast-2:
      az1: apse2-az1
      az2: apse2-az3
    ap-northeast-1:
```

```
      az1: apne1-az1
      az2: apne1-az4
    ca-central-1:
      az1: cac1-az1
      az2: cac1-az2
    eu-central-1:
      az1: euc1-az2
      az2: euc1-az3
    eu-west-1:
      az1: euw1-az1
      az2: euw1-az2
    eu-west-2:
      az1: euw2-az2
      az2: euw2-az3
    sa-east-1:
      az1: sae1-az1
      az2: sae1-az3

Resources:

  iamLambdaExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
              - lambda.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWSLambdaBasicExecutionRole
      Policies:
        - PolicyName: describe-ec2-az
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - 'ec2:DescribeAvailabilityZones'
                Resource: '*'
      MaxSessionDuration: 3600
```

```
      Path: /service-role/

  fnZoneIdtoZoneName:
    Type: AWS::Lambda::Function
    Properties:
      Runtime: python3.8
      Handler: index.lambda_handler
      Code:
        ZipFile: |
          import boto3
          import cfnresponse

          def zoneId_to_zoneName(event, context):
              responseData = {}
              ec2 = boto3.client('ec2')
              describe_az = ec2.describe_availability_zones()
              for az in describe_az['AvailabilityZones']:
                  if event['ResourceProperties']['ZoneId'] == az['ZoneId']:
                      responseData['ZoneName'] = az['ZoneName']
                      cfnresponse.send(event, context, cfnresponse.SUCCESS,
responseData, str(az['ZoneId']))

          def no_op(event, context):
              print(event)
              responseData = {}
              cfnresponse.send(event, context, cfnresponse.SUCCESS, responseData,
str(event['RequestId']))

          def lambda_handler(event, context):
              if event['RequestType'] == ('Create' or 'Update'):
                  zoneId_to_zoneName(event, context)
              else:
                  no_op(event,context)
      Role: !GetAtt iamLambdaExecutionRole.Arn

  getAZ1:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az1 ]
  getAZ2:
    Type: "Custom::zone-id-zone-name"
    Properties:
      ServiceToken: !GetAtt fnZoneIdtoZoneName.Arn
```

```
      ZoneId: !FindInMap [ RegionMap, !Ref 'AWS::Region', az2 ]

#########################
# VPC AND SUBNETS
#########################

  AppVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: !Ref VpcCIDR
      InstanceTenancy: default
      EnableDnsSupport: true
      EnableDnsHostnames: true

  PublicSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet1CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PublicSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PublicSubnet2CIDR
      MapPublicIpOnLaunch: true
      AvailabilityZone: !GetAtt getAZ2.ZoneName

  PrivateSubnetA:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet1CIDR
      AvailabilityZone: !GetAtt getAZ1.ZoneName

  PrivateSubnetB:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref AppVPC
      CidrBlock: !Ref PrivateSubnet2CIDR
      AvailabilityZone: !GetAtt getAZ2.ZoneName
```

```
  InternetGateway:
    Type: AWS::EC2::InternetGateway

  InternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      InternetGatewayId: !Ref InternetGateway
      VpcId: !Ref AppVPC

  NatGatewayEIP:
    Type: AWS::EC2::EIP
    DependsOn: InternetGatewayAttachment

  NatGateway:
    Type: AWS::EC2::NatGateway
    Properties:
      AllocationId: !GetAtt NatGatewayEIP.AllocationId
      SubnetId: !Ref PublicSubnetA

#########################
# Route Tables
#########################

  PrivateRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref AppVPC

  DefaultPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref NatGateway

  PrivateSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetA

  PrivateSubnetRouteTableAssociation2:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
```

```
      RouteTableId: !Ref PrivateRouteTable
      SubnetId: !Ref PrivateSubnetB

  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref AppVPC

  DefaultPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: InternetGatewayAttachment
    Properties:
      RouteTableId: !Ref PublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref InternetGateway

  PublicSubnetARouteTableAssociation1:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetA

  PublicSubnetBRouteTableAssociation2:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      RouteTableId: !Ref PublicRouteTable
      SubnetId: !Ref PublicSubnetB


##########################
# SECURITY GROUPS
##########################

  VPCEndpointSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: Allow TLS for VPC Endpoint
      VpcId: !Ref AppVPC
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 443
          ToPort: 443
          CidrIp: !GetAtt AppVPC.CidrBlock
```

```
#########################
# VPC ENDPOINTS
#########################

  VPCEndpointGatewayS3:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.s3'
      VpcEndpointType: Gateway
      VpcId: !Ref AppVPC
      RouteTableIds:
        - !Ref PrivateRouteTable

  VPCEndpointInterfaceSignin:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.signin'
      VpcId: !Ref AppVPC

  VPCEndpointInterfaceConsole:
    Type: 'AWS::EC2::VPCEndpoint'
    Properties:
      VpcEndpointType: Interface
      PrivateDnsEnabled: false
      SubnetIds:
        - !Ref PrivateSubnetA
        - !Ref PrivateSubnetB
      SecurityGroupIds:
        - !Ref VPCEndpointSecurityGroup
      ServiceName: !Sub 'com.amazonaws.${AWS::Region}.console'
      VpcId: !Ref AppVPC

#########################
# ROUTE53 RESOURCES
#########################

  ConsoleHostedZone:
```

```
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Console VPC Endpoint Hosted Zone'
      Name: 'console.aws.amazon.com'
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  ConsoleRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  GlobalConsoleRecord:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 'global.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleS3ProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: 's3.console.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
```

```
      Type: A

  ConsoleSupportProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "support.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ExplorerProxyRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: "resource-explorer.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  ConsoleRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'ConsoleHostedZone'
      Name: !Sub "${AWS::Region}.console.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
VPCEndpointInterfaceConsole.DnsEntries]]]
      Type: A

  SigninHostedZone:
    Type: "AWS::Route53::HostedZone"
    Properties:
      HostedZoneConfig:
        Comment: 'Signin VPC Endpoint Hosted Zone'
      Name: 'signin.aws.amazon.com'
```

```
      VPCs:
        -
          VPCId: !Ref AppVPC
          VPCRegion: !Ref "AWS::Region"

  SigninRecordGlobal:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: 'signin.aws.amazon.com'
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

  SigninRecordRegional:
    Type: AWS::Route53::RecordSet
    Properties:
      HostedZoneId: !Ref 'SigninHostedZone'
      Name: !Sub "${AWS::Region}.signin.aws.amazon.com"
      AliasTarget:
        DNSName: !Select ['1', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
        HostedZoneId: !Select ['0', !Split [':', !Select ['0', !GetAtt
 VPCEndpointInterfaceSignin.DnsEntries]]]
      Type: A

#########################
# WORKSPACE RESOURCES
#########################
  ADAdminSecret:
    Type: AWS::SecretsManager::Secret
    Properties:
      Name: "ADAdminSecret"
      Description: "Password for directory services admin"
      GenerateSecretString:
        SecretStringTemplate: '{"username": "Admin"}'
        GenerateStringKey: password
        PasswordLength: 30
        ExcludeCharacters: '"@/\'

  WorkspaceSimpleDirectory:
```

```
    Type: AWS::DirectoryService::SimpleAD
    DependsOn: AppVPC
    DependsOn: PrivateSubnetA
    DependsOn: PrivateSubnetB
    Properties:
      Name: "corp.awsconsole.com"
      Password: '{{resolve:secretsmanager:ADAdminSecret:SecretString:password}}'
      Size: "Small"
      VpcSettings:
        SubnetIds:
          - Ref: PrivateSubnetA
          - Ref: PrivateSubnetB

        VpcId:
          Ref: AppVPC


Outputs:
  PrivateSubnetA:
    Description: Private Subnet A
    Value: !Ref PrivateSubnetA

  PrivateSubnetB:
    Description: Private Subnet B
    Value: !Ref PrivateSubnetB

  WorkspaceSimpleDirectory:
    Description: Directory to be used for Workspaces
    Value: !Ref WorkspaceSimpleDirectory

  WorkspacesAdminPassword:
    Description : "The ARN of the Workspaces admin's password.  Navigate to the Secrets
 Manager in the AWS Console to view the value."
    Value: !Ref ADAdminSecret
```

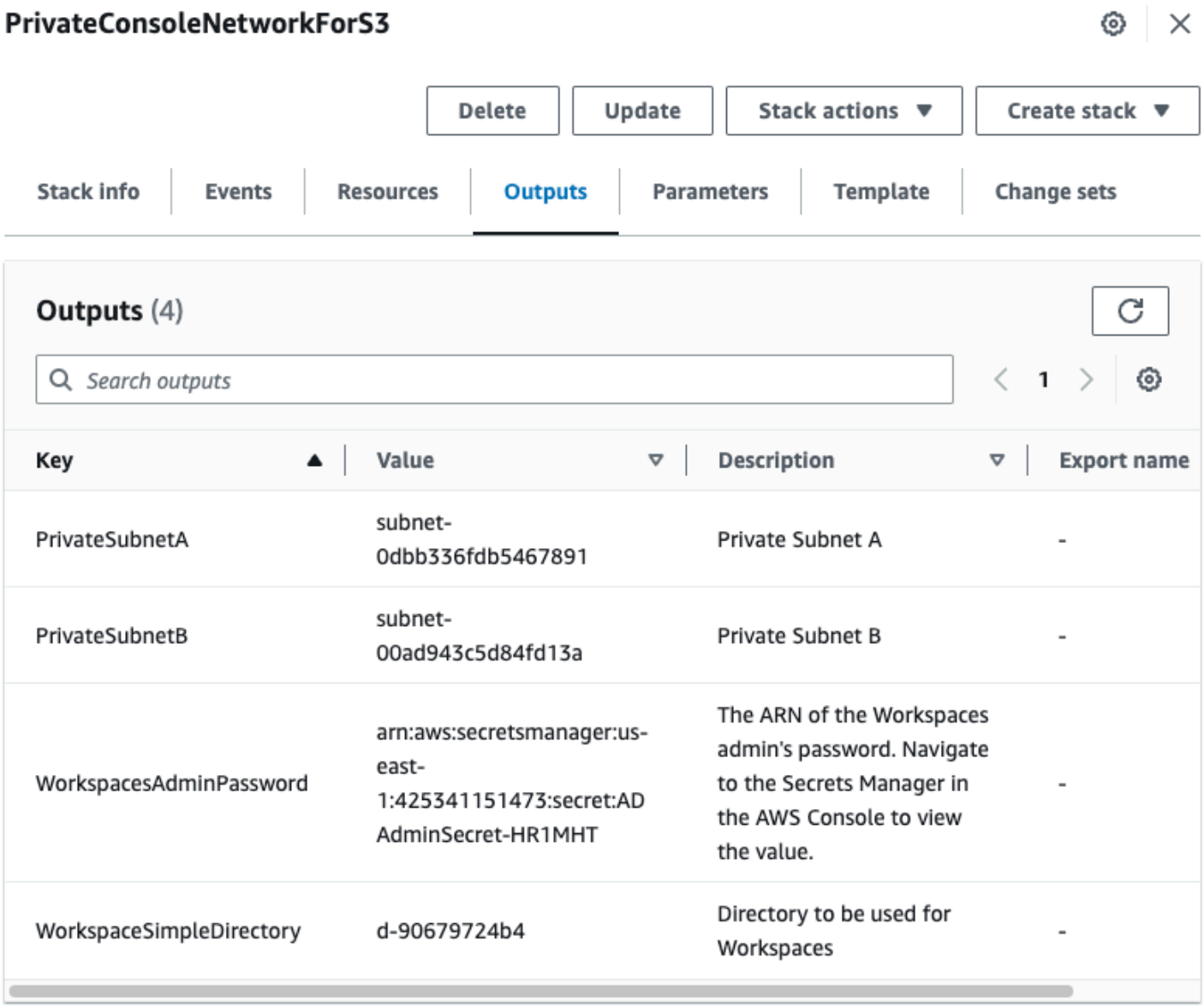
> **Note**
>
> 此测试设置设计为在美国东部（弗吉尼亚州北部）（us-east-1）区域中运行。

设置网络

1. 登录您所在组织的管理账户并打开 AWS CloudFormation 控制台。

2. 选择创建堆栈。
3. 选择使用新资源（标准）。上传您之前创建的 AWS CloudFormation 模板文件，然后选择 “下一步”。
4. 输入堆栈的名称（例如 **PrivateConsoleNetworkForS3**），然后选择下一步。
5. 对于 VPC 和子网，输入您的首选 IP CIDR 范围，或使用提供的默认值。如果您使用默认值，请确认它们不与您的现有 VPC 资源重叠 AWS 账户。
6. 选择创建堆栈。
7. 创建堆栈后，选择资源选项卡以查看已创建的资源。
8. 选择输出选项卡，以查看私有子网和工作区简单目录的值。请记下这些值，因为您将在下一个创建和配置过程的第四步中使用它们 WorkSpace。

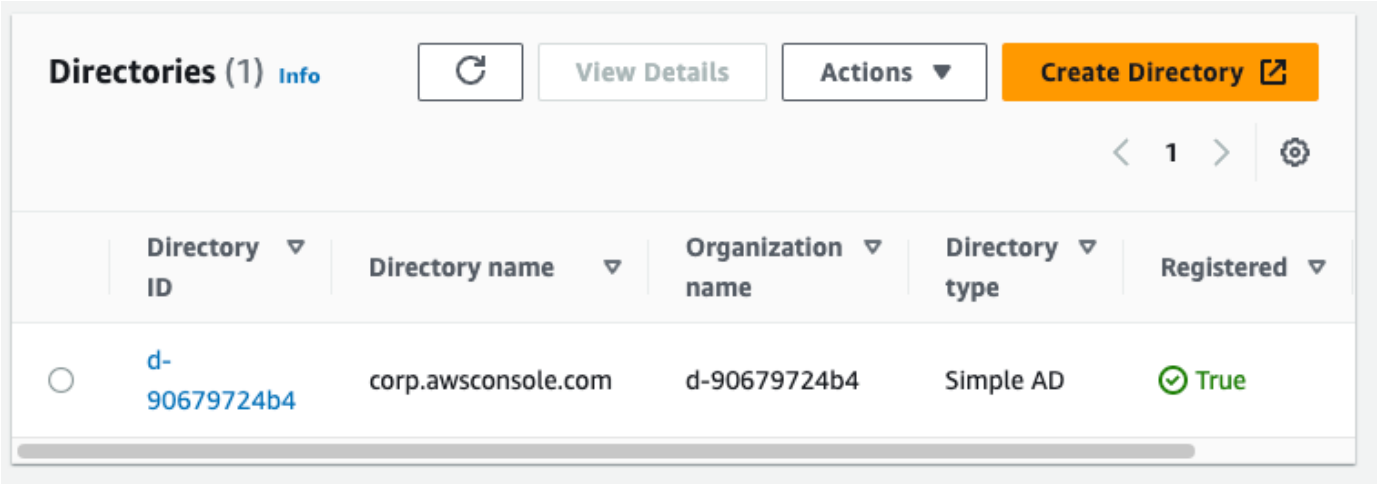
以下屏幕截图显示了输出选项卡的视图，其中显示了私有子网和工作区简单目录的值。



现在您已经创建了网络，请按照以下步骤创建和访问网络 WorkSpace。

要创建 WorkSpace

1. 打开WorkSpaces 控制台。
2. 在导航窗格中，选择目录。
3. 在目录页面上，验证目录状态是否为活动。以下屏幕截图显示了具有一个活动的目录的目录页面。



4. 要使用中的目录 WorkSpaces，必须对其进行注册。在导航窗格中，选择 WorkSpaces，然后选择创建 WorkSpaces。
5. 对于选择目录，选择 AWS CloudFormation 在前面的过程中创建的目录。在操作菜单上，选择注册。
6. 要选择子网，请选择前述过程的步骤 9 中记下的两个私有子网。
7. 选择启用自助服务权限，然后选择注册。
8. 注册目录后，继续创建 WorkSpace。选择注册的目录，然后选择下一步。
9. 在创建用户页面上，选择创建其他用户。输入您的姓名和电子邮件以使您能够使用 WorkSpace. 当 WorkSpace 登录信息发送到该电子邮件地址时，请验证该电子邮件地址是否有效。
10. 选择下一步。
11. 在标识用户页面上，选择您在步骤 9 中创建的用户，然后选择下一步。
12. 在选择服务包页面上，选择 Amazon Linux 2 标准版，然后选择下一步。
13. 对于运行模式和用户自定义使用默认值，然后选择创建工作区。 WorkSpace 开始进入`Pending`状态，然后在大约 20 分钟`Available`内过渡到状态。
14. 可用 WorkSpace 时，您将通过您在步骤九中提供的电子邮件地址收到一封包含访问说明的电子邮件。

登录后 WorkSpace，您可以测试自己是否正在使用 AWS Management Console 私有访问权限对其进行访问。

要访问 WorkSpace

1. 打开您在前述过程的步骤 14 中收到的电子邮件。
2. 在电子邮件中，选择提供的唯一链接来设置您的个人资料并下载 WorkSpaces 客户端。

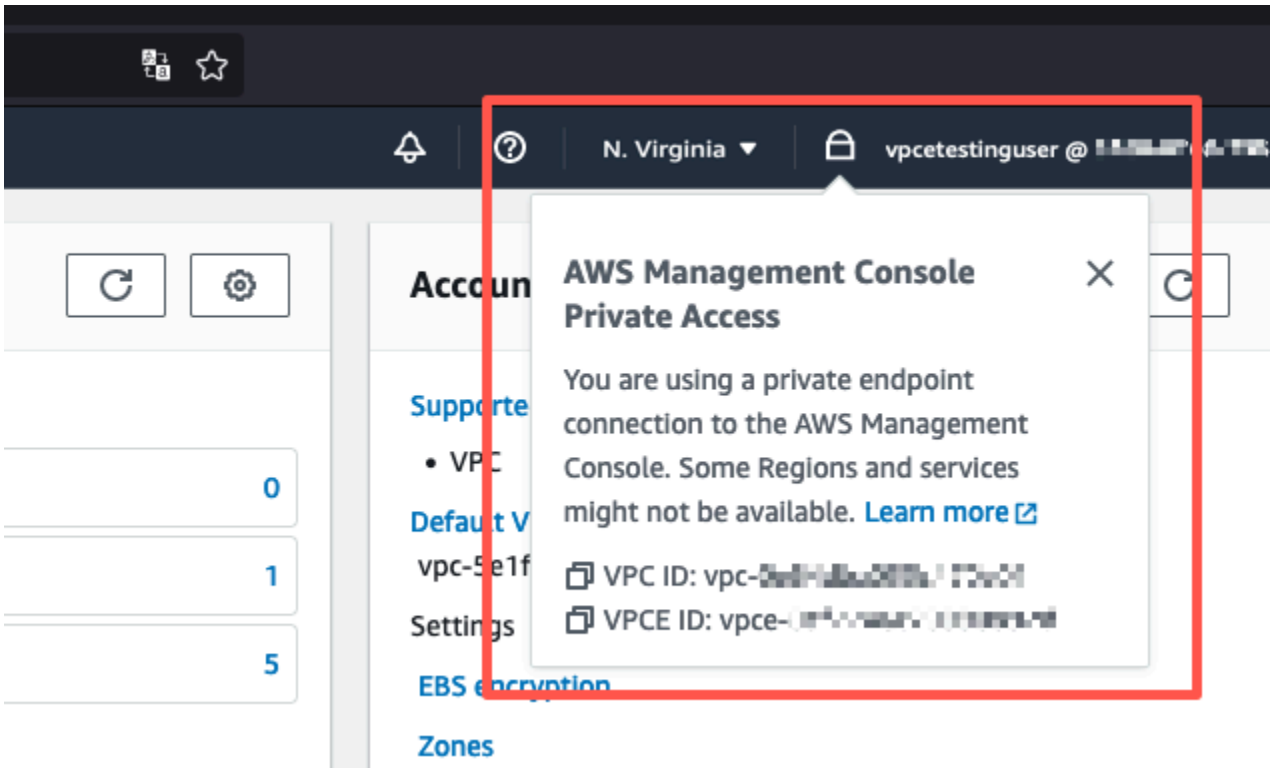
3. 设置您的密码。
4. 下载您选择的客户端。
5. 安装并启动客户端。输入电子邮件中提供的注册码，然后选择注册。
6. WorkSpaces 使用您在第三步中创建的凭证登录 Amazon。

测试 AWS Management Console 私有访问设置

1. 从您的 WorkSpace，打开浏览器。然后，导航到 AWS Management Console并使用您的凭证登录。

> **Note**
>
> 如果您使用 Firefox 作为浏览器，请验证浏览器设置中的通过 HTTPS 启用 DNS 选项已关闭。

2. 打开 Amazon S3 控制台，您可以在其中验证您是否已使用 AWS Management Console 私有访问进行连接。
3. 在导航栏上选择锁定私有图标，以查看所使用的 VPC 和 VPC 端点。以下屏幕截图显示了锁定私有图标的位置和 VPC 信息。



使用 IAM 策略测试 VPC 设置

您可以进一步测试您通过 Amazon EC2 或部署限制访问 WorkSpaces 的 IAM 策略设置的 VPC。

除非 Amazon S3 使用您指定的 VPC，否则以下策略将拒绝对 Amazon S3 的访问。

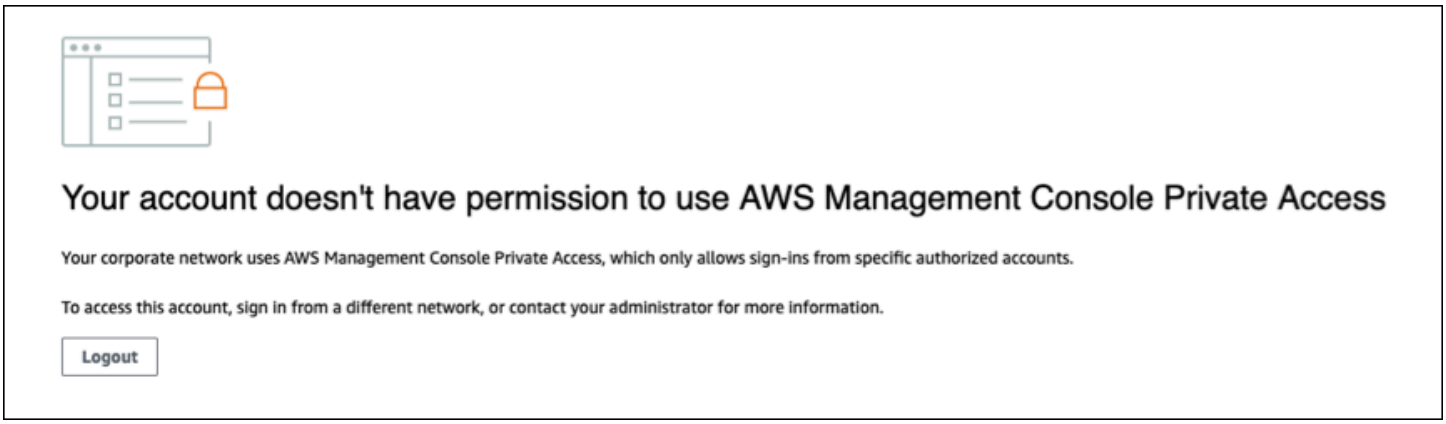
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "S3:*",
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "aws:SourceVpc": "sourceVPC"
                },
                "Bool": {
                    "aws:ViaAwsService": "false"
                }
            }
        }
    ]
}
```

以下政策限制使用登录端点的 AWS Management Console 私有访问策略登录选定 AWS 账户 ID。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": [
                        "AWSAccountID"
                    ]
                }
            }
        }
```

```
    ]
}
```

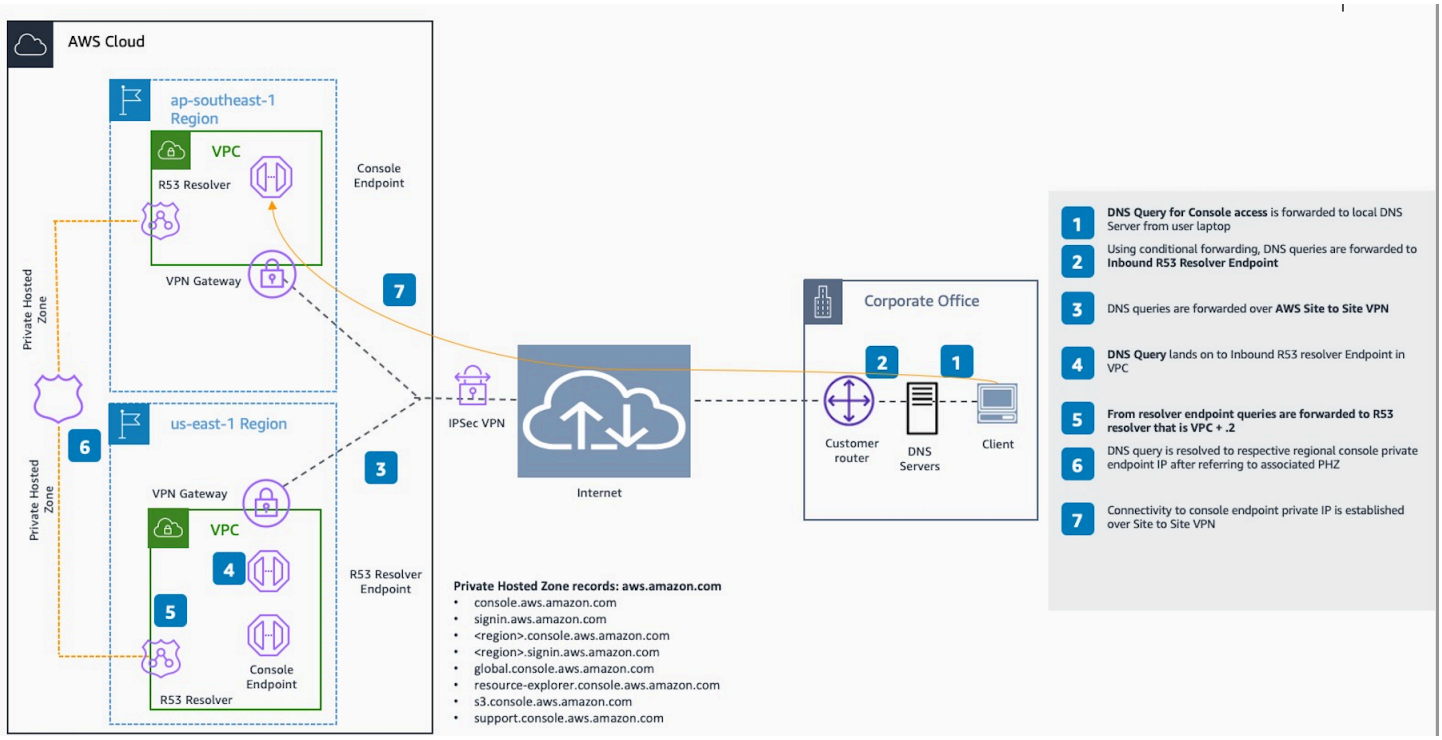
如果您进行连接时所用的身份不属于您的账户，则会显示以下错误页面。



参考架构

要通过本地网络私密连接到私 AWS Management Console 有访问权限，可以利用 AWS Site-to-Site VPN 到 AWS 虚拟专用网关 (VGW) 连接选项。 AWS Site-to-Site VPN 通过创建连接并配置路由以通过连接传递流量，允许从 VPC 访问您的远程网络。有关更多信息，请参阅《点对点 VP AWS N 用户指南》中的什么是点对点 VPN。AWS AWS 虚拟专用网关 (VGW) 是一项高度可用的区域服务，充当 VPC 和本地网络之间的网关。

AWS Site-to-Site VPN 到 AWS 虚拟专用网关 (VGW)



本参考架构设计中的一个重要组件是 Amazon Route 53 Resolver，特别是入站解析器。当您在创建 AWS Management Console 私有访问终端节点的 VPC 中进行设置时，将在指定的子网中创建解析器终端节点（网络接口）。然后，可以在本地 DNS 服务器上的条件转发器中引用解析器端点的 IP 地址，以允许查询私有托管区中的记录。当本地客户端连接到时 AWS Management Console，它们会被路由到私有访问终端节点的 AWS Management Console 私有 IP。

在设置与 AWS Management Console 私有访问终端节点的连接之前，请完成先决条件步骤，即 AWS Management Console 在您要访问的所有区域以及美国东部（弗吉尼亚北部）地区设置私有访问终端节点，并配置私有托管区域。 AWS Management Console

在 Console Toolbar 上启动 AWS CloudShell

AWS CloudShell 是一个已经事先完成身份验证的浏览器式 Shell，您可以直接从 Console Toolbar 上的 AWS Management Console启动它。您可以运行 AWS CLI 命令对服务使用您的首选 shell（Bash、PowerShell 或 Z shell）。

您可以使用以下两种方法之一在 Console Toolbar 上启动 CloudShell：

- 选择控制台左下角的 CloudShell 图标。
- 选择控制台导航栏中的 CloudShell 图标。

有关此服务的更多信息，请参阅 AWS CloudShell 用户指南。

有关 AWS CloudShell 可用的 AWS 区域的信息，请参阅 AWS 区域服务列表。控制台区域的选择与 CloudShell 区域同步。如果 CloudShell 在选定区域中不可用，则 CloudShell 将在最近的区域中运行。

获取账单信息

如果您拥有必要的权限，就可以通过控制台获取您的 AWS 费用信息。

获取账单信息

1. 在导航栏上，选择您的账户名称。
2. 选择 Billing Dashboard（账单控制面板）。
3. 在 AWS Billing and Cost Management 控制面板中可以找到每月费用的汇总和明细。要了解有关更多信息，请参阅 AWS Billing 用户指南。

在控制台中使用 Markdown

中的某些服务 AWS Management Console，例如亚马逊 CloudWatch，支持在某些领域使用 Markdown。本主题说明控制台中支持的 Markdown 格式的类型。

内容

段落、行间距和水平线

段落由空白行分隔。为了确保段落之间的空白行在转换为 HTML 时呈现，请添加一个带有不间隔空格 ( ) 的新行，然后添加一个空白行。重复这两行，依次插入多个空白行，如下例所示：

```
 

 
```

要创建分隔段落的水平规则，请添加一个连续包含三个连字符的新行：`---`

```
Previous paragraph.
---
Next paragraph.
```

要创建具有等宽类型的文本块，请添加一个带有三个反引号 (`) 的行。输入要以等宽类型显示的文本。然后，添加另一个包含三个反引号的新行。以下示例演示了在显示时格式将设置为等宽类型的文本：

```
```
This appears in a text box with a background shading.
The text is in monospace.
```
```

标题

要创建标题，请使用井号 (#)。单个井号和空格表示顶级标题。两个井号将创建一个二级标题，三个井号将创建一个三级标题。以下示例显示了顶级、二级和三级标题：

```
# Top-level heading
```

```
## Second-level heading
```

```
### Third-level heading
```

文本格式设置

要将文本的格式设置为斜体，请在文本的两端各使用一个下划线 (_) 或星号 (*) 以将其括起。

```
*This text appears in italics.*
```

要将文本的格式设置为粗体，请在文本的两端各使用两个下划线或星号以将其括起。

```
**This text appears in bold.**
```

要将文本的格式设置为带删除线，请在文本的两端各使用两个波浪线 (~) 以将其括起。

```
~~This text appears in strikethrough.~~
```

链接

要添加文本超链接，请输入用方括号 ([ ]) 括起来的链接文本，后跟放入括号 (( )) 中的完整 URL，如以下示例所示：

```
Choose [link_text](http://my.example.com).
```

列表

要将行的格式设置为项目符号列表的一部分，请将它们添加到以一个星号 (*) 后跟一个空格开头的单独行上，如以下示例所示：

```
Here is a bulleted list:
* Ant
* Bug
* Caterpillar
```

要将行的格式设置为编号列表的一部分，请将它们添加到以一个数字、句点 (.) 和一个空格开头的单独行上，如以下示例所示：

```
Here is a numbered list:
1. Do the first step
2. Do the next step
3. Do the final step
```

表格和按钮（CloudWatch 仪表板）

CloudWatch 仪表板文本控件支持 Markdown 表格和按钮。

要创建表，请使用竖线 (|) 分隔列并使用新行分隔行。要使第一行成为标题行，请在标题行和第一行值之间插入一行。然后，为表中的每一列添加至少三个连字符 (-)。使用竖线分隔各列。以下示例显示包含两列、一个标题行和两个数据行的表的 Markdown：

```
Table | Header
----|-----
Amazon Web Services | AWS
1 | 2
```

上一个示例中的 Markdown 文本创建了下表：

表	标题
Amazon Web Services	AWS
1	2

在 CloudWatch 仪表板文本控件中，您还可以设置超链接的格式，使其显示为按钮。要创建按钮，请使用 [button:*Button text*]，后跟放入括号 (( )) 中的完整 URL，如以下示例所示：

```
[button:Go to AWS](http://my.example.com)
[button:primary:This button stands out even more](http://my.example.com)
```

故障排除

请参阅本节以查找常见问题的解决方案 AWS Management Console。

您还可以使用 Amazon Q Developer 诊断和解决某些 AWS 服务的常见错误。有关更多信息，请参阅 Amazon Q 开发者用户指南中的使用 Amazon Q 开发人员诊断控制台中的常见错误。

主题

页面未正确加载

- 如果此问题只是偶尔出现，请检查您的互联网连接。尝试通过其他网络进行连接，或者使用或不使用 VPN 进行连接，或者尝试使用其他网络浏览器。
- 如果所有受影响的用户都来自同一个团队，则可能是隐私浏览器扩展程序或安全防火墙问题。隐私浏览器扩展程序和安全防火墙可以阻止对使用的域的访问。 AWS Management Console尝试关闭这些扩展程序或调整防火墙设置。要验证您的连接问题，请打开浏览器开发工具（Chrome、Firefox），并在 Console（控制台）选项卡中检查错误。 AWS Management Console 使用域名的后缀，包括以下列表。此列表并不详尽，可能会随着时间而变化。这些域的后缀并非专供 AWS使用。
  - .a2z.com
  - .amazon.com
  - .amazonaws.com
  - .aws
  - .aws.com
  - .aws.dev
  - .awscloud.com
  - .awsplayer.com
  - .awsstatic.com
  - .cloudfront.net
  - .live-video.net

> **Warning**
>
> 自 2022 年 7 月 31 日起， AWS 不再支持 Internet Explorer 11。我们建议您将与其他支持的浏览器 AWS Management Console 一起使用。有关更多信息，请参阅 AWS 新闻博客。

我的浏览器在连接时显示 “访问被拒绝” 错误 AWS Management Console

如果您使用以下所有内容，则最近对主机所做的更改可能会影响您的访问权限：

- 来自 VPC 内部的浏览器。
- VPC 终端节点。
- 包含`aws:SourceIp`全局条件密钥的 IAM 策略。

在控制台中，转到 IAM 策略页面。我们建议您查看包含`aws:SourceIp`全局条件密钥的 IAM 策略并添加`aws:SourceVpc`密钥。

或者，您可以考虑使用 AWS Management Console 私有访问功能， AWS Management Console 通过 VPC 终端节点进行访问，并在策略中使用`aws:SourceVpc`条件。有关更多信息，请参阅 AWS Management Console 私密访问权限。

我的浏览器在连接时显示超时错误 AWS Management Console

如果您的默认服务中断 AWS 区域，则您的浏览器在尝试连接时可能会显示 504 网关超时错误。 AWS Management Console要 AWS Management Console 从其他区域登录，请在 URL 中指定备用区域终端节点。例如，如果 `us-west-1`（加利福尼亚北部）区域发生中断，要访问 `us-west-2`（俄勒冈）区域，请使用以下模板：

```
https://region-code.console.aws.amazon.com
```

有关更多信息，请参阅《AWS 一般参考》中的 AWS Management Console 服务端点。

要查看所有 AWS 服务内容（包括）的状态 AWS Management Console，请参阅AWS Health Dashboard。

我想更改 AWS Management Console 的语言，但在页面底部找不到语言选择菜单

语言选择菜单已移至新的 Unified Settings（统一设置）页面。要更改的语言 AWS Management Console，请导航至 “统一设置” 页面，然后选择控制台的语言。

有关更多信息，请参阅更改 AWS Management Console的语言。

文档历史记录

下表介绍了自 2021 年 3 月起对《AWS Management Console 入门指南》的一些重要更改。

更改	描述	日期
与 Amazon Q 聊天	一个新的设置页面，详细说明了用户如何向 Amazon Q 开发者 AWS 提问。有关更多信息，请参阅与 Amazon Q 开发者聊天。	2024 年 5 月 29 日
我的应用程序	一个介绍 “我的应用程序” 的新页面。有关更多信息，请参阅 MyApplications 在 AWS做什么？ 。	2023 年 11 月 29 日
配置统一设置	一个新的设置页面，用于配置应用于当前用户的设置和原定设置，包括语言和区域。有关更多信息，请参阅配置统一设置。	2022 年 4 月 6 日
全新 AWS Console Home 用户界面	新的 AWS Console Home 用户界面，包括用于显示重要使用信息的小部件和 AWS 服务快捷方式。有关更多信息，请参阅使用小组件。	2022 年 2 月 25 日
更改控制台语言	为 AWS Management Console 选择不同的语言。有关更多信息，请参阅更改 AWS Management Console的语言。	2021 年 4 月 1 日
正在启动 CloudShell	AWS CloudShell 从中打开 AWS Management Console 并运行 AWS CLI 命令。有关	2021 年 3 月 22 日

更改	描述	日期
	更多信息，请参阅启动 AWS CloudShell。	

AWS 术语表

有关最新的 AWS 术语，请参阅《AWS 词汇表参考》中的 AWS 词汇表。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。