aws

用户指南

亚马逊 Lightsail 研究版

亚马逊 Lightsail 研究版: 用户指南

Table of Contents

什么是亚马逊 Lightsail for Research？

借助 Amazon Lightsail for Research，学者和研究人员可以在亚马逊网络服务 (AWS) 云中创建功能强大的虚拟计算机。这些虚拟计算机预装了研究应用程序，例如 RStudio 和 Scilab。

有了 Lightsail for Research，你可以直接从网络浏览器上传数据开始工作。您可以随时创建和删除虚拟计算机，这使您可以按需访问功能强大的计算资源。

只需在需要虚拟计算机时付费。Lightsail for Research 提供预算控制，当您的计算机达到预先配置的成本限制时，它可以自动停止运行，因此您不必担心超额费用。

你在 Lightsail for Research 控制台中所做的一切都得到了公开可用的 API 的支持。了解如何安装和使用适用于 Amazon Lightsail 的AWS CLI和 API。

定价

使用 Lightsail for Research，您只需为自己创建和使用的资源付费。有关更多信息，请参阅 Lightsail for Research 定价。

可用性

Lightsail for Research 在与 Amazon Lightsail 相同的 AWS 地区上市，但美国东部（弗吉尼亚北部）地区除外。Lightsail for Research 也使用与 Lightsail 相同的端点。要查看 Lightsail 当前支持的 AWS 区域和终端节点，请参阅《一般参考》中的 Lig htsail 终端节点和配额。AWS

为研究设置亚马逊 Lightsail

如果您是新 AWS 客户，请在开始使用 Amazon Lightsail for Research 之前，完成本页列出的设置先决条件。对于这些设置过程，您可以使用 AWS Identity and Access Management (IAM) 服务。有关 IAM 的完整信息，请参阅《IAM 用户指南》。

主题

报名参加 AWS

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

创建 IAM 用户

要创建管理员用户，请选择以下选项之一。

选择一种方法来管理您的管理员	目的	方式	您也可以
在 IAM Identity Center 中（建议）	使用短期凭证访问 AWS。 这符合安全最佳实操。有关最佳实践的信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。	有关说明，请参阅《AWS IAM Identity Center 用户指南》中的入门。	通过在《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中配置 AWS CLI 要使用的来配置编程访问权限。
在 IAM 中（不推荐使用）	使用长期凭证访问 AWS。	按照《IAM 用户指南》中的创建您的首个 IAM 管理员用户和组的说明操作。	按照《IAM 用户指南》中的管理 IAM 用户的访问密钥，配置编程式访问。

教程：Lightsail for Research 虚拟计算机入门

使用本教程可开始使用 Amazon Lightsail for Research 虚拟计算机。您将了解如何创建虚拟计算机、连接到虚拟计算机和使用虚拟计算机。在 Lightsail for Research 中，虚拟计算机是您在 AWS Cloud 中创建和管理的研究工作站。虚拟计算机基于采用 Ubuntu 操作系统的 Lightsail 实例。在虚拟计算机上，您可以预配置研究应用程序，例如 JupyterLab、RStudio、Scilab 等。

您在本教程中创建的虚拟计算机将从您创建虚拟计算机之时起一直产生使用费，直到您将其删除。删除是本教程的最后一步。有关定价的更多信息，请参阅 Lightsail for Research 定价。

主题

步骤 1：完成先决条件

如果您是新 AWS 客户，请在开始使用 Amazon Lightsail for Research 之前完成设置先决条件。有关更多信息，请参阅 为研究设置亚马逊 Lightsail。

步骤 2：创建虚拟计算机

您可以根据以下过程所述使用 Lightsail for Research 控制台创建虚拟计算机。本教程旨在帮助您快速启动第一台虚拟计算机。我们还建议您探索可用的应用程序和硬件计划。有关更多信息，请参阅 应用程序和硬件套餐 和 创建虚拟计算机：

1. 登录 Lightsail for Research 控制台。
2. 在主页上，选择创建虚拟计算机。
3. 为您的虚拟计算机选择 AWS 区域。

   选择离您的实际位置最近的区域，以改善延迟。

4. 选择一个应用程序，也称为 Lightsail API 中的蓝图。

   创建虚拟计算机时，您选择的应用程序已安装并配置到您的虚拟计算机上。

5. 选择硬件计划，在 Lightsail API 中也称为捆绑包。

   硬件计划提供不同数量的处理能力，包括 vCPU 内核、内存、存储和每月数据传输。Lightsail for Research 为虚拟计算机提供标准计划和 GPU 计划。当您的工作计算要求较低时，请选择标准计划。当要求很高时，例如运行机器学习模型或其他计算密集型任务时，请选择 GPU 计划。

6. 输入虚拟计算机的名称。

7. 在摘要面板中选择创建虚拟计算机。

新的虚拟计算机启动并运行后，请继续执行本教程的下一步，了解如何启动计算机的应用程序。

步骤 3：启动虚拟计算机的应用程序

创建虚拟计算机且其处于正在运行状态后，即可在 Web 浏览器中启动虚拟会话。通过会话，您可以与虚拟计算机上安装的应用程序进行交互并对其进行管理。

1. 在 Lightsail for Research 控制台的导航窗格中选择虚拟计算机。

2. 找到您在步骤 1 中创建的虚拟计算机的名称，然后选择启动应用程序。例如，启动 JupyterLab。应用程序会话在一个新的 Web 浏览器窗口中打开。

   > **Important**
   >
   > 如果您的 Web 浏览器安装了弹出窗口阻止程序，则在打开会话之前，您可能需要允许来自 aws.amazon.com 域名的弹出窗口。

要了解如何连接到虚拟计算机，请继续执行本教程的下一步骤。

步骤 4：连接到您的虚拟计算机

您可以使用以下方法连接到虚拟计算机：

- 使用 Lightsail for Research 控制台中提供的基于浏览器的 NICE DCV 客户端。借助 NICE DCV，您可以使用图形用户界面（GUI）与您的研究应用程序和虚拟计算机的操作系统进行交互。

- 使用 Secure Shell（SSH）客户端，例如 OpenSSH、PuTTY 或 Windows Subsystem for Linux 访问虚拟计算机的命令行界面。使用 SSH 客户端，您可以编辑脚本和配置文件。
- 使用 Secure Copy（SCP）在您的本地计算机和虚拟计算机之间安全传输文件。使用 SCP，您可以在本地开始工作，然后在虚拟计算机上继续工作。您也可以从虚拟计算机下载文件，将工作复制到本地计算机。

> **Note**
>
> 您还可以使用基于浏览器的 NICE DCV 客户端访问虚拟计算机的命令行界面并传输文件。

要使用 SSH 连接虚拟计算机或使用 SCP 传输文件，必须提供虚拟计算机的密钥对。密钥对是您在连接到 Lightsail for Research 虚拟计算机时用于证明个人身份的一组安全凭证。密钥对包含公有密钥和私有密钥。

有关连接到虚拟计算机的更多信息，请参阅以下文档：

- 建立远程显示协议连接：
  - 启动虚拟计算机的应用程序
  - 访问虚拟计算机的操作系统
- 建立 SSH 连接或使用 SCP 传输文件：
  - 获取虚拟计算机的密钥对
  - 使用 Secure Shell 连接到虚拟计算机
  - 使用 Secure Copy 将文件传输到虚拟计算机

要了解虚拟计算机的存储，请继续执行本教程的下一步。

步骤 5：为虚拟计算机添加存储空间

Lightsail for Research 提供块级存储卷（磁盘），您可以将这些卷（磁盘）附加到虚拟计算机。即使您的虚拟计算机附带系统磁盘，您也可以根据存储需求的变化将其他磁盘附加到虚拟计算机。您也可以从一台虚拟计算机中分离一个磁盘，并把它附加到另一台虚拟计算机。

当您使用控制台将磁盘附加到虚拟计算机时，Lightsail for Research 会自动将其格式化并挂载该磁盘。此过程需要几分钟；因此在开始使用磁盘之前，您应该确认磁盘已进入已挂载状态。

有关创建、附加和管理磁盘的更多信息，请参阅以下文档：

- 创建磁盘
- 查看磁盘
- 将磁盘附加到虚拟计算机
- 将磁盘与虚拟计算机分离
- 删除磁盘

要了解备份虚拟计算机的信息，请继续执行本教程的下一步。

步骤 6：创建快照

快照是数据的时间点副本。您可以创建虚拟计算机的快照，并将其用作创建新计算机或备份数据的基准。快照包含还原您的计算机所需的所有数据（从拍摄快照的那一刻开始）。

有关创建和管理快照的更多信息，请参阅以下文档：

- 创建快照
- 查看快照
- 使用快照创建虚拟计算机或磁盘
- 删除快照

要了解清理虚拟计算机的信息，请继续执行本教程的下一步。

步骤 7：清除

在完成使用为本教程创建的虚拟计算机后，您可以将其删除。如果您不需要虚拟计算机，则无需支付虚拟计算机费用。

删除虚拟计算机并不会删除其关联的快照或附加磁盘。如果您创建了快照和磁盘，则应手动删除这些快照和磁盘，以免产生费用。

要保存虚拟计算机以备日后使用，但需要避免按标准小时价格收费，您可以停止虚拟计算机而不是将其删除。稍后您可以重新启动。有关更多信息，请参阅 查看虚拟计算机详细信息。有关定价的更多信息，请参阅 Lightsail for Research 定价。

> **Important**
>
> 删除 Lightsail for Research 资源是一项永久性操作。删除的数据无法恢复。如果以后可能需要这些数据，请先创建虚拟计算机的快照，然后再删除它。有关更多信息，请参阅创建快照。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择虚拟计算机。
3. 选择要删除的虚拟计算机。
4. 选择操作，然后选择删除虚拟计算机。
5. 在文本块中键入确认。然后，选择删除虚拟计算机。

亚马逊 Lightsail 研究版入门教程

以下教程提供了有关如何开始使用 Lightsail for Research 中提供的特定应用程序的更多信息。

主题

> **Note**
>
> AWS 公共部门博客上发布了入门 Lightsail for Research 和 rStudio 的深入教程。有关更多信息，请参阅 Amazon Lightsail for Research 入门：使用 RStudio 的教程。

开始使用 JupyterLab

在本教程中，我们将向您展示如何开始在 Amazon Lightsail for Research 中管理和使用您的 JupyterLab 虚拟计算机。

主题

步骤 1：完成先决条件

如果尚未使用该 JupyterLab 应用程序创建虚拟计算机，请使用该应用程序。有关更多信息，请参阅 创建虚拟计算机。

新的虚拟计算机启动并运行后，继续本教程的 “启动 JupyterLab 应用程序” 部分。

步骤 2：（可选）添加存储空间

您的虚拟计算机附带一个系统磁盘。但是，随着存储需求的变化，您可以将更多磁盘附加到虚拟计算机，以增加其存储空间。

您也可以将工作文件存储到附加的磁盘。然后，您可以分离磁盘并将其附加到另一台虚拟计算机，以便将文件从一台计算机快速移动到另一台计算机。

或者，您可以创建包含工作文件的附加磁盘的快照，然后根据该快照创建磁盘副本。然后，您可以将新的磁盘副本附加到另一台计算机，以便在不同的虚拟计算机上复制您的工作。有关更多信息，请参阅创建磁盘 和 将磁盘附加到虚拟计算机。

> **Note**
>
> 当你使用控制台将磁盘连接到虚拟计算机时，Lightsail for Research 会自动格式化并装载该磁盘。此过程需要几分钟；因此在开始使用磁盘之前，您应该确认磁盘已进入已挂载状态。默认情况下，Lightsail for Research 会将磁盘挂载到目录中。`/home/lightsail-user/<disk-name>` `<disk-name>`是你给磁盘起的名字。

步骤 3：上传和下载文件

您可以将文件上传到您的 JupyterLab 虚拟计算机，并从中下载文件。为此，您必须完成以下步骤：

1. 从亚马逊 Lightsail 获取密钥对。有关更多信息，请参阅 获取虚拟计算机的密钥对。
2. 获取密钥对后，您就可以通过 Secure Copy（SCP）实用程序，使用该密钥对来建立连接。SCP 允许您使用命令提示符或终端上传和下载文件。有关更多信息，请参阅 使用 Secure Copy 将文件传输到虚拟计算机。
3. （可选）您也可以使用密钥对并通过 SSH 连接到虚拟计算机。有关更多信息，请参阅 使用 Secure Shell 连接到虚拟计算机。

> **Note**
>
> 您还可以使用基于浏览器的 NICE DCV 客户端访问虚拟计算机的命令行界面并传输文件。NICE DCV 在 Lightsail for Research 主机中可用。有关更多信息，请参阅 启动虚拟计算机的应用程序 和 访问虚拟计算机的操作系统。

要管理附加存储磁盘中的项目文件，请确保将它们上传到附加磁盘的正确挂载目录。当你使用控制台将磁盘连接到虚拟计算机时，Lightsail for Research 会自动格式化磁盘并将其挂载到目录中。/home/lightsail-user/*<disk-name>* *<disk-name>*是你给磁盘起的名字。

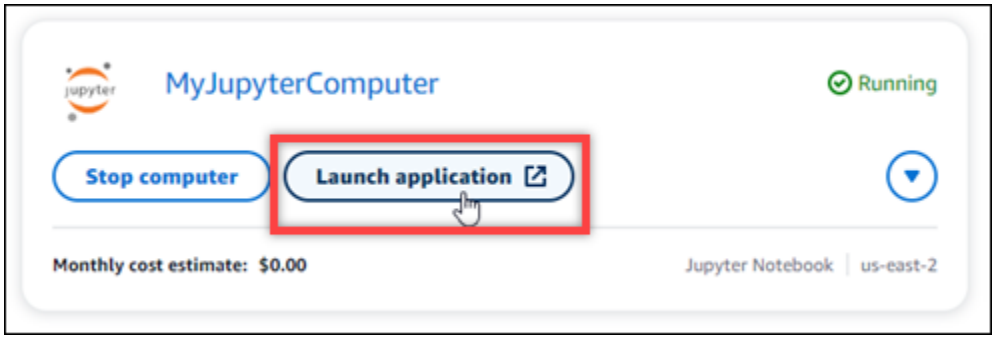
步骤 4：启动 JupyterLab应用程序

完成以下步骤，在新虚拟计算机上启动 JupyterLab 应用程序。

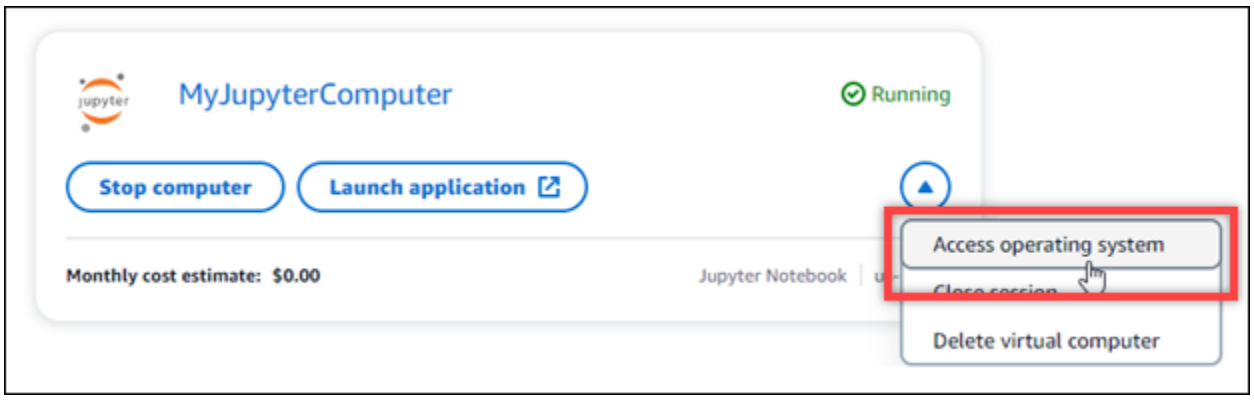
> **Important**
>
> 即使系统提示您更新操作系统或 JupyterLab 应用程序，也不要更新操作系统或应用程序。而是要选择关闭或忽略这些提示的选项。此外，不要修改 /home /lightsail-admin/ 目录中的任何文件。这些操作可能会使虚拟计算机无法使用。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中选择虚拟计算机，查看您的账户中可用的虚拟计算机。
3. 在虚拟计算机页面中，找到您的虚拟计算机，然后选择以下选项之一进行连接：

   a. （推荐）选择 “启动应用程序”，以聚焦模式启动 JupyterLab 应用程序。如果你最近没有连接到虚拟计算机，则可能需要等待几分钟，让 Lightsail for Research 准备会话。

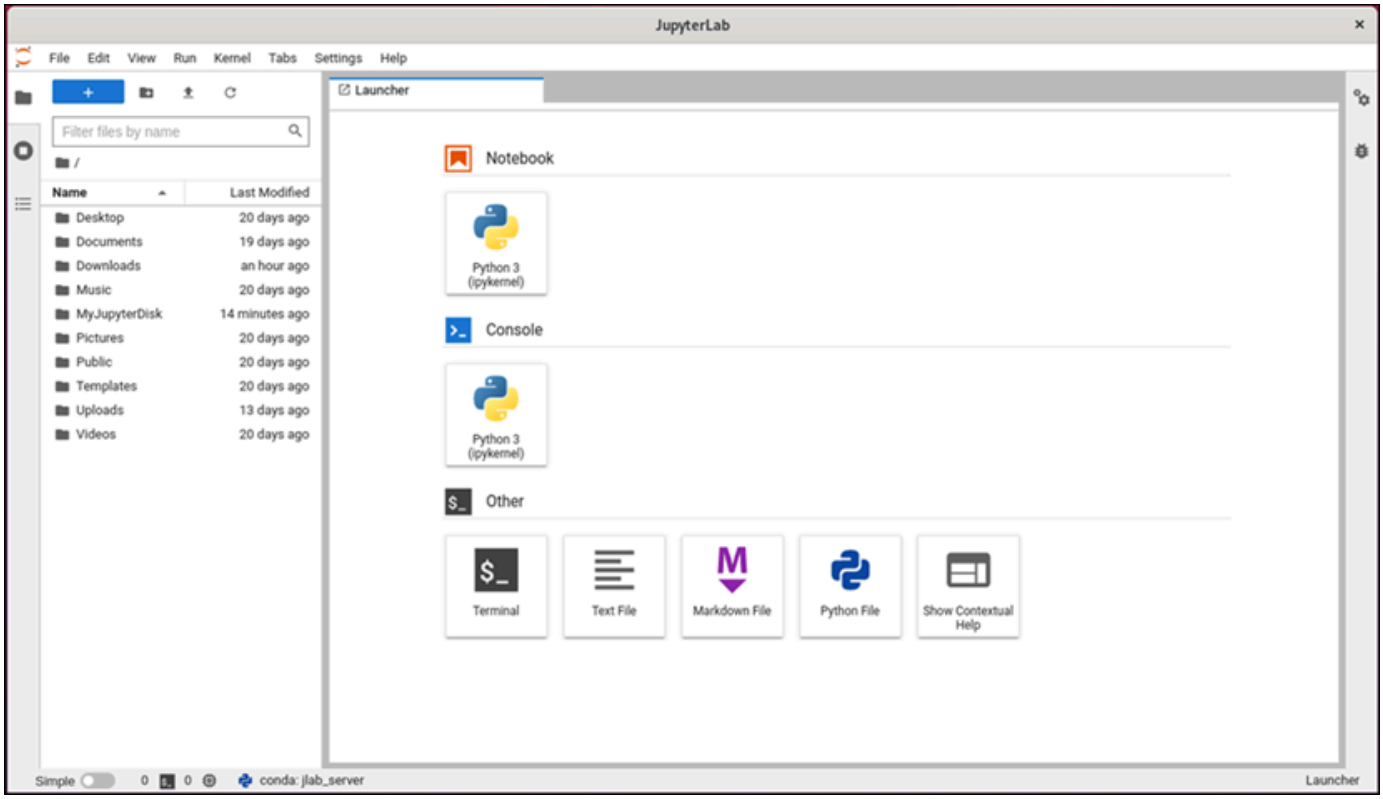
   b. 选择计算机的下拉菜单，然后选择访问操作系统，以访问虚拟计算机的桌面。



Lightsail for Research 运行几个命令来启动远程显示协议连接。片刻之后，系统将打开一个新的浏览器选项卡窗口，并与您的虚拟计算机建立虚拟桌面连接。如果您选择了 “启动应用程序” 选项，请继续执行此过程的下一步以在 JupyterLab 应用程序中打开文件。如果您选择了访问操作系统选项，则可以通过 Ubuntu 桌面打开其他应用程序。

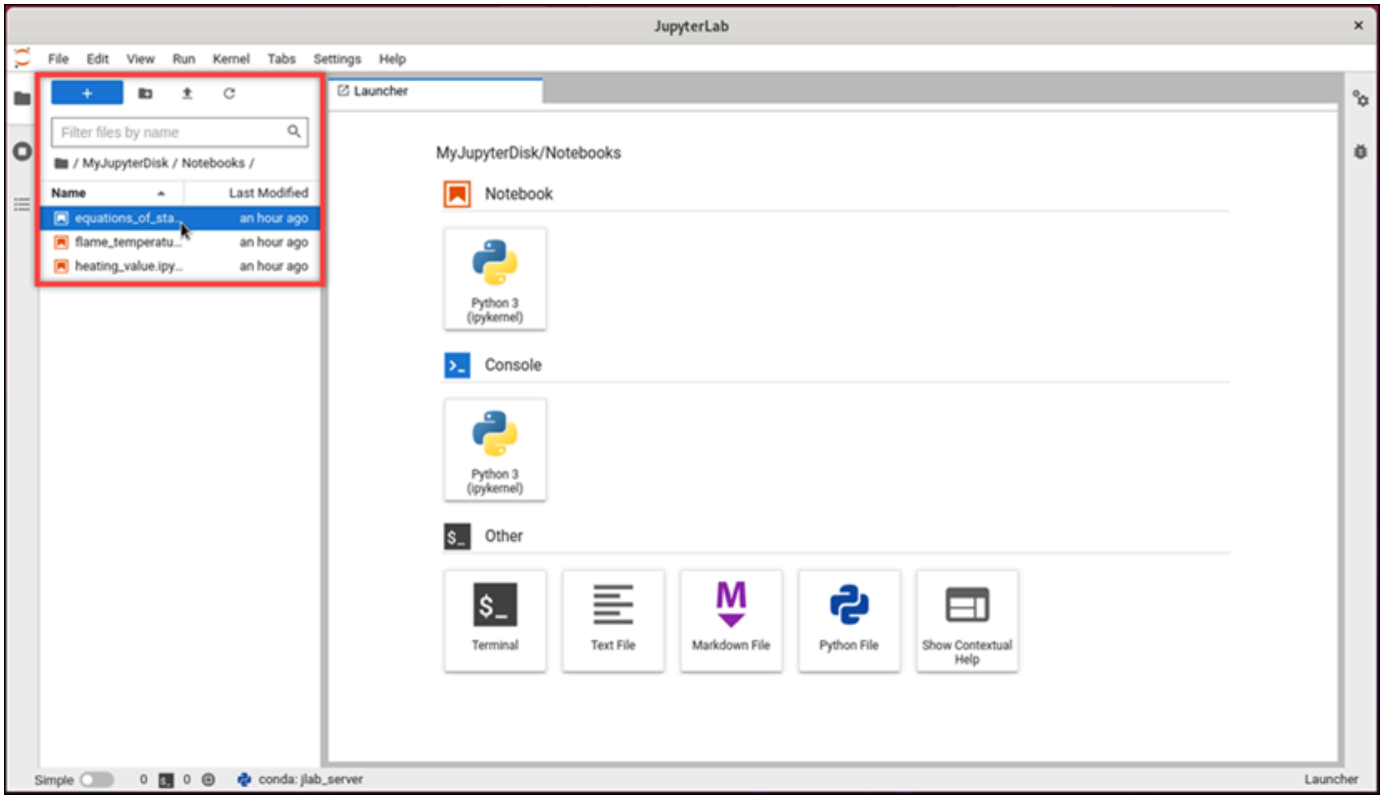
> **Note**
>
> 您的浏览器可能会提示您授权共享剪贴板。允许此操作可让您在本地计算机和虚拟计算机之间进行复制和粘贴。
>
> Ubuntu 可能还会提示您进行初始设置。按照提示进行操作，直到完成设置并可以使用操作系统。

4. JupyterLab 应用程序打开。在启动程序菜单中，您可以创建新的笔记本、启动控制台、启动终端以及创建各种文件。

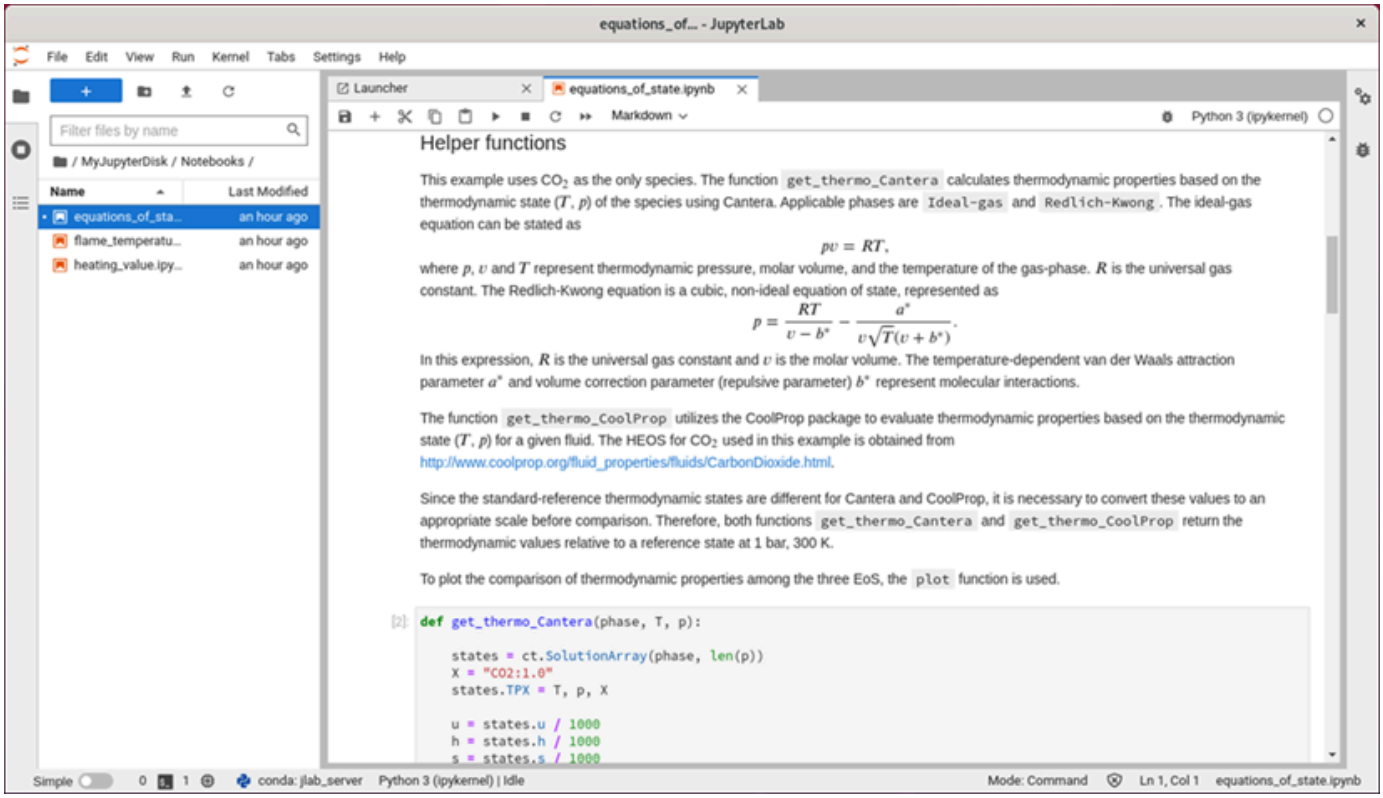


5. 要在中打开文件 JupyterLab，请在文件浏览器窗格中，选择存储项目文件的目录或文件夹。然后选择要打开的文件。

   如果您已将项目文件上传到附加磁盘，请查找挂载该磁盘的目录。默认情况下，Lightsail for Research 会将磁盘挂载到目录中。`/home/lightsail-user/<disk-name>` *<disk-name>*是你给磁盘起的名字。在以下示例中，`MyJupyterDisk` 目录代表已挂载的磁盘，`Notebooks` 子目录包含我们的 Jupyter notebook 文件。



在以下示例中，我们打开了 `equations_of_state.ipynb` Jupyter notebook 文件。



有关如何开始使用的信息，请继续阅读本教程的 第 5 步：阅读 JupyterLab文档 部分。

第 5 步：阅读 JupyterLab文档

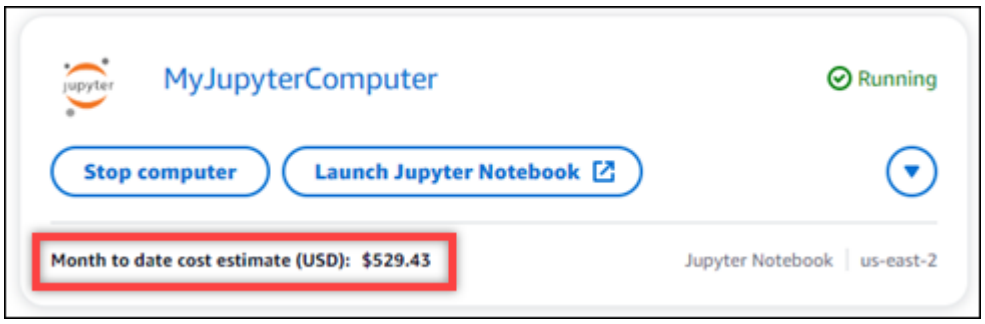
如果您不熟悉 JupyterLab，我们建议您阅读他们的官方文档。以下 JupyterLab 在线资源可用：

- JupyterLab文档
- Jupyter Discourse 论坛
- JupyterLab on StackOverflow
- JupyterLab on GitHub

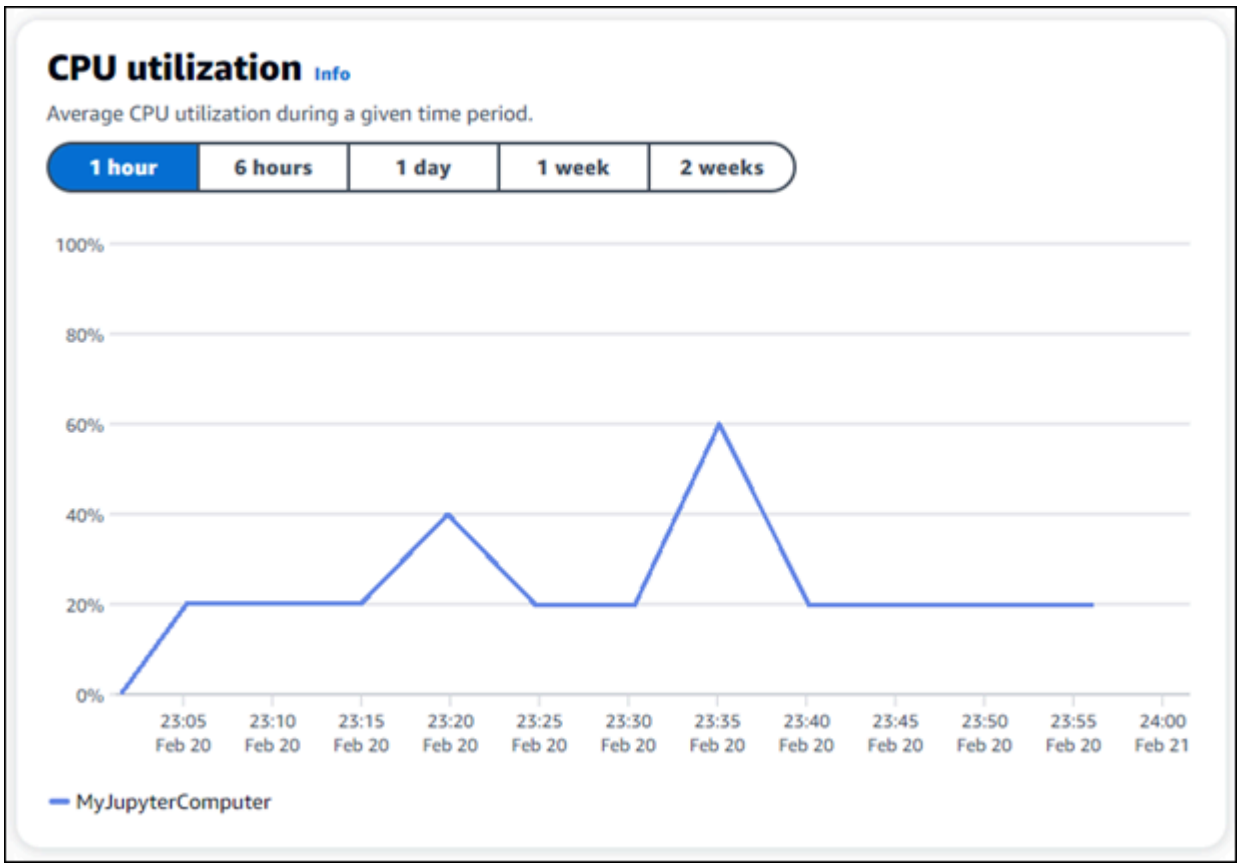
步骤 6：（可选）监控使用情况和成本

Lightsail for Research 资源迄今为止的费用和使用量估算值显示在 Lightsail for Research 控制台的以下区域中。

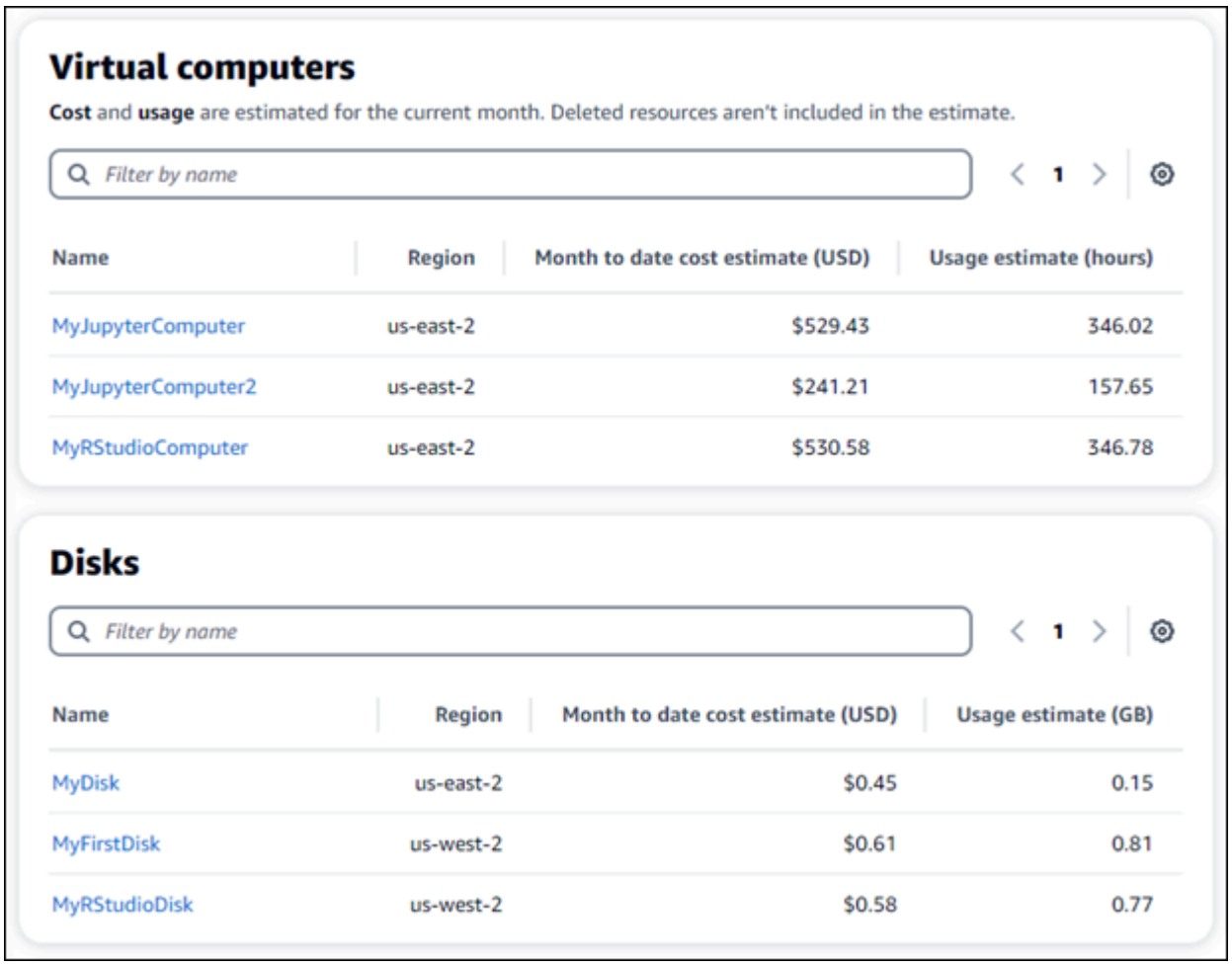
1. 在 Lightsail for Research 控制台的导航窗格中选择 “虚拟计算机”。虚拟计算机的本月至今成本估算列在每台正在运行的虚拟计算机下。



2. 要查看虚拟计算机的 CPU 使用率，请选择虚拟计算机的名称，然后选择控制面板选项卡。



3. 要查看所有 Lightsail for Research 资源的月初至今成本和使用量估算值，请在导航窗格中选择 “使用情况”。



步骤 7：（可选）创建成本控制规则

通过创建成本控制规则来管理虚拟计算机的使用情况和成本。您可以创建停止处于空闲状态的虚拟计算机规则，当计算机在给定时间段内达到指定的 CPU 使用率百分比时，该规则会停止正在运行的计算机。例如，当特定计算机的 CPU 使用率在 30 分钟内等于或低于 5% 时，规则就可以自动停止该计算机。这可能意味着计算机处于空闲状态，而 Lightsail for Research 会停止计算机，这样您就不会为闲置资源产生费用。

> **Important**
>
> 在创建停止处于空闲状态的虚拟计算机的规则之前，我们建议您监控 CPU 使用率几天。记下虚拟计算机处于不同负载下的 CPU 使用率。例如，当虚拟计算机编译代码、处理操作和处于空闲状态时的 CPU 使用率。这将帮助您确定规则的准确阈值。有关更多信息，请参阅本教程的 步骤 6：（可选）监控使用情况和成本 部分。

如果您创建的规则中 CPU 使用率阈值高于您的工作负载，则该规则可以连续停止您的虚拟计算机。例如，如果您在规则停止虚拟计算机后立即启动虚拟计算机，则该规则将重新激活，计算机将再次停止。

有关创建和管理成本控制规则的详细说明，请参阅以下指南：

- 成本控制
- 创建规则
- 删除规则

步骤 8：（可选）创建快照

快照是您的数据的 point-in-time 副本。您可以创建虚拟计算机的快照，并将其用作创建新计算机或备份数据的基准。快照包含还原您的计算机所需的所有数据（从拍摄快照的那一刻开始）。

有关创建和管理快照的详细说明，请参阅以下指南：

- 创建快照
- 查看快照
- 使用快照创建虚拟计算机或磁盘
- 删除快照

步骤 9：（可选）停止或删除虚拟计算机

在完成使用为本教程创建的虚拟计算机后，您可以将其删除。如果您不需要虚拟计算机，则无需支付虚拟计算机费用。

删除虚拟计算机并不会删除其关联的快照或附加磁盘。如果您创建了快照和磁盘，则应手动删除这些快照和磁盘，以免产生费用。

要保存虚拟计算机以备日后使用，但需要避免按标准小时价格收费，您可以停止虚拟计算机而不是将其删除。稍后您可以重新启动。有关更多信息，请参阅 查看虚拟计算机详细信息。有关定价的更多信息，请参阅 Lightsail for Research 定价。

> **Important**
>
> 删除 Lightsail for Research 资源是一项永久性操作。删除的数据无法恢复。如果以后可能需要这些数据，请先创建虚拟计算机的快照，然后再删除它。有关更多信息，请参阅创建快照。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择虚拟计算机。
3. 选择要删除的虚拟计算机。
4. 选择操作，然后选择删除虚拟计算机。
5. 在文本块中键入确认。然后，选择删除虚拟计算机。

RStudio 入门

在本教程中，我们将向你展示如何开始在 Amazon Lightsail for Research 中管理和使用你的 RStudio 虚拟计算机。

> **Note**
>
> AWS 公共部门博客上发布了入门 Lightsail for Research 和 rStudio 的深入教程。有关更多信息，请参阅 Amazon Lightsail for Research 入门：使用 RStudio 的教程。

主题

步骤 1：完成先决条件

如果尚未创建虚拟计算机，请使用 RStudio 应用程序创建一个虚拟计算机。有关更多信息，请参阅 创建虚拟计算机。

新的虚拟计算机启动并运行后，继续执行本教程的步骤 4。

步骤 2：（可选）添加存储空间

您的虚拟计算机附带一个系统磁盘。但是，随着存储需求的变化，您可以将更多磁盘附加到虚拟计算机，以增加其存储空间。

您也可以将工作文件存储到附加的磁盘。然后，您可以分离磁盘并将其附加到另一台虚拟计算机，以便将文件从一台计算机快速移动到另一台计算机。

或者，您可以创建包含工作文件的附加磁盘的快照，然后根据该快照创建磁盘副本。然后，您可以将新的磁盘副本附加到另一台计算机，以便在不同的虚拟计算机上复制您的工作。有关更多信息，请参阅 创建磁盘 和 将磁盘附加到虚拟计算机。

> **Note**
>
> 当你使用控制台将磁盘连接到虚拟计算机时，Lightsail for Research 会自动格式化并装载该磁盘。此过程需要几分钟；因此在开始使用磁盘之前，您应该确认磁盘已进入已挂载状态。默认情况下，Lightsail for Research 会将磁盘挂载到你*<disk-name>*为磁盘命名的/home/lightsail-user/*<disk-name>*目录中。

步骤 3：上传和下载文件

您可以将文件上传到 RStudio 虚拟计算机，以及从中下载文件。为此，您必须完成以下步骤：

1. 从亚马逊 Lightsail 获取密钥对。有关更多信息，请参阅 获取虚拟计算机的密钥对。
2. 获取密钥对后，您就可以通过 Secure Copy（SCP）实用程序，使用该密钥对来建立连接。SCP 允许您使用命令提示符或终端上传和下载文件。有关更多信息，请参阅 使用 Secure Copy 将文件传输到虚拟计算机。
3. （可选）您也可以使用密钥对并通过 SSH 连接到虚拟计算机。有关更多信息，请参阅 使用 Secure Shell 连接到虚拟计算机。

> **Note**
>
> 您还可以使用基于浏览器的 NICE DCV 客户端访问虚拟计算机的命令行界面并传输文件。NICE DCV 在 Lightsail for Research 主机中可用。有关更多信息，请参阅 启动虚拟计算机的应用程序 和 访问虚拟计算机的操作系统。

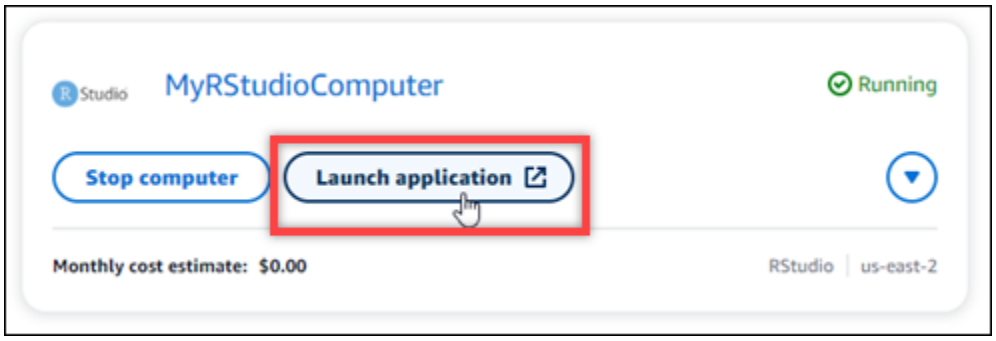
步骤 4：启动 RStudio 应用程序

完成以下过程，以在新的虚拟计算机上启动 RStudio 应用程序。

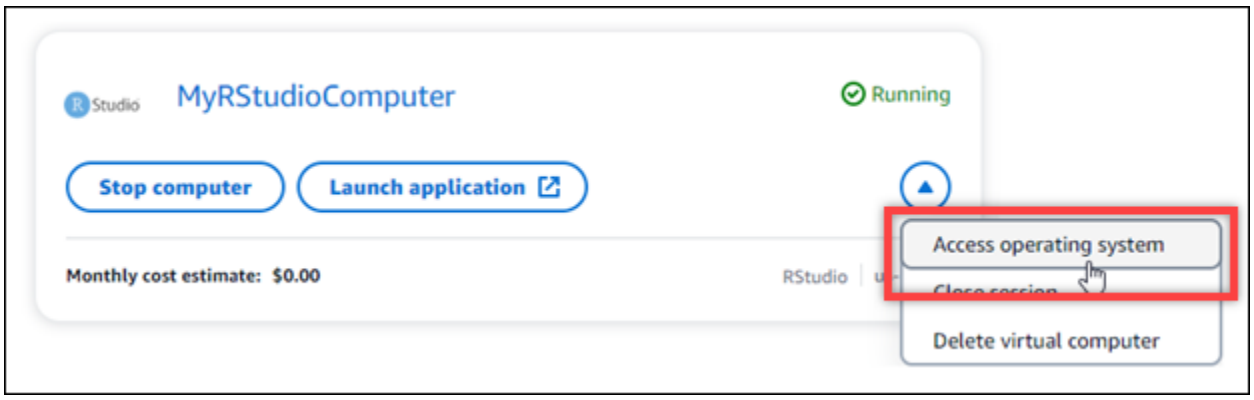
> **Important**
>
> 即使系统提示您更新操作系统或 RStudio 应用程序，也不要这样做。而是要选择关闭或忽略这些提示的选项。此外，不要修改 /home /lightsail-admin/ 目录中的任何文件。这些操作可能会使虚拟计算机无法使用。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中选择虚拟计算机，查看您的账户中可用的虚拟计算机。
3. 在虚拟计算机页面中，找到您的虚拟计算机，然后选择以下选项之一进行连接：

   a. （推荐）选择启动应用程序，以聚焦模式启动 RStudio 应用程序。如果你最近没有连接到虚拟计算机，则可能需要等待几分钟，让 Lightsail for Research 准备会话。

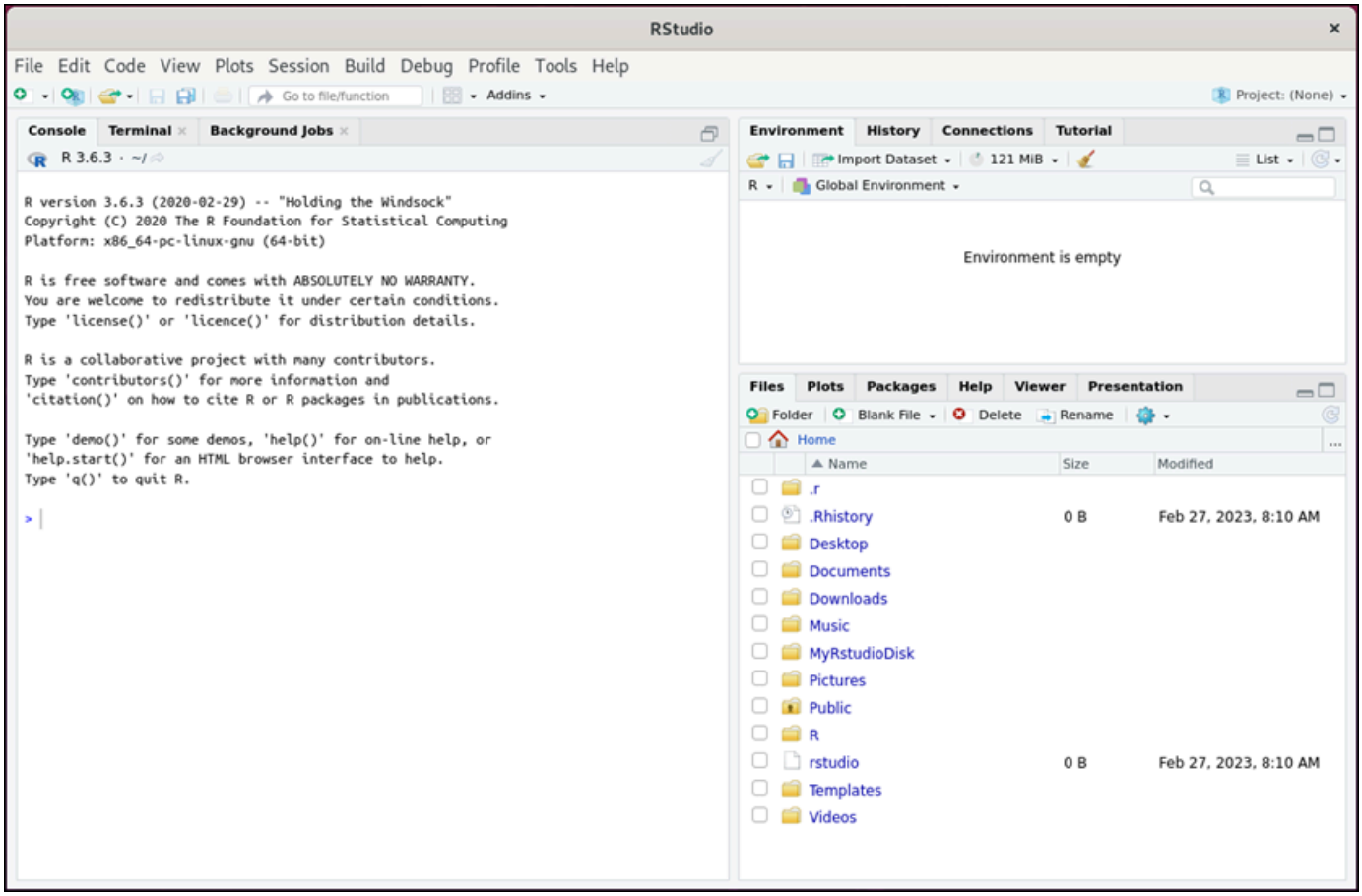
   b. 选择计算机的下拉菜单，然后选择访问操作系统，以访问虚拟计算机的桌面。如果您想在操作系统上安装其他应用程序，请执行此操作。



Lightsail for Research 运行几个命令来启动远程显示协议连接。片刻之后，系统将打开一个新的浏览器选项卡窗口，并与您的虚拟计算机建立虚拟桌面连接。如果您选择了启动应用程序选项，请继续执行此过程的下一步，以在 RStudio 应用程序中打开文件。如果您选择了访问操作系统选项，则可以通过 Ubuntu 桌面打开其他应用程序。

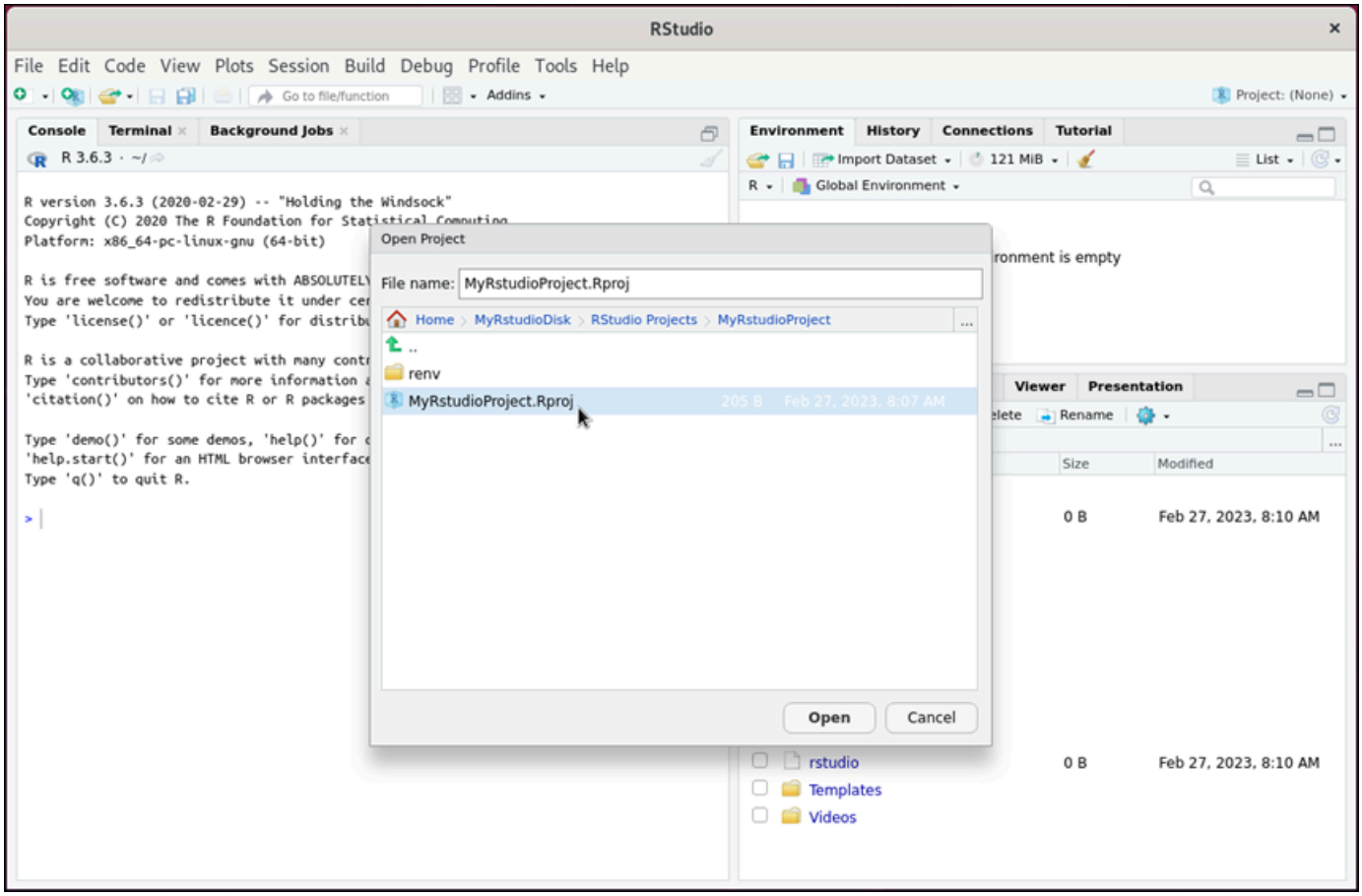
> **Note**
>
> 您的浏览器可能会提示您授权共享剪贴板。允许此操作可让您在本地计算机和虚拟计算机之间进行复制和粘贴。
>
> Ubuntu 可能还会提示您进行初始设置。按照提示进行操作，直到完成设置并可以使用操作系统。

4. RStudio 应用程序打开。

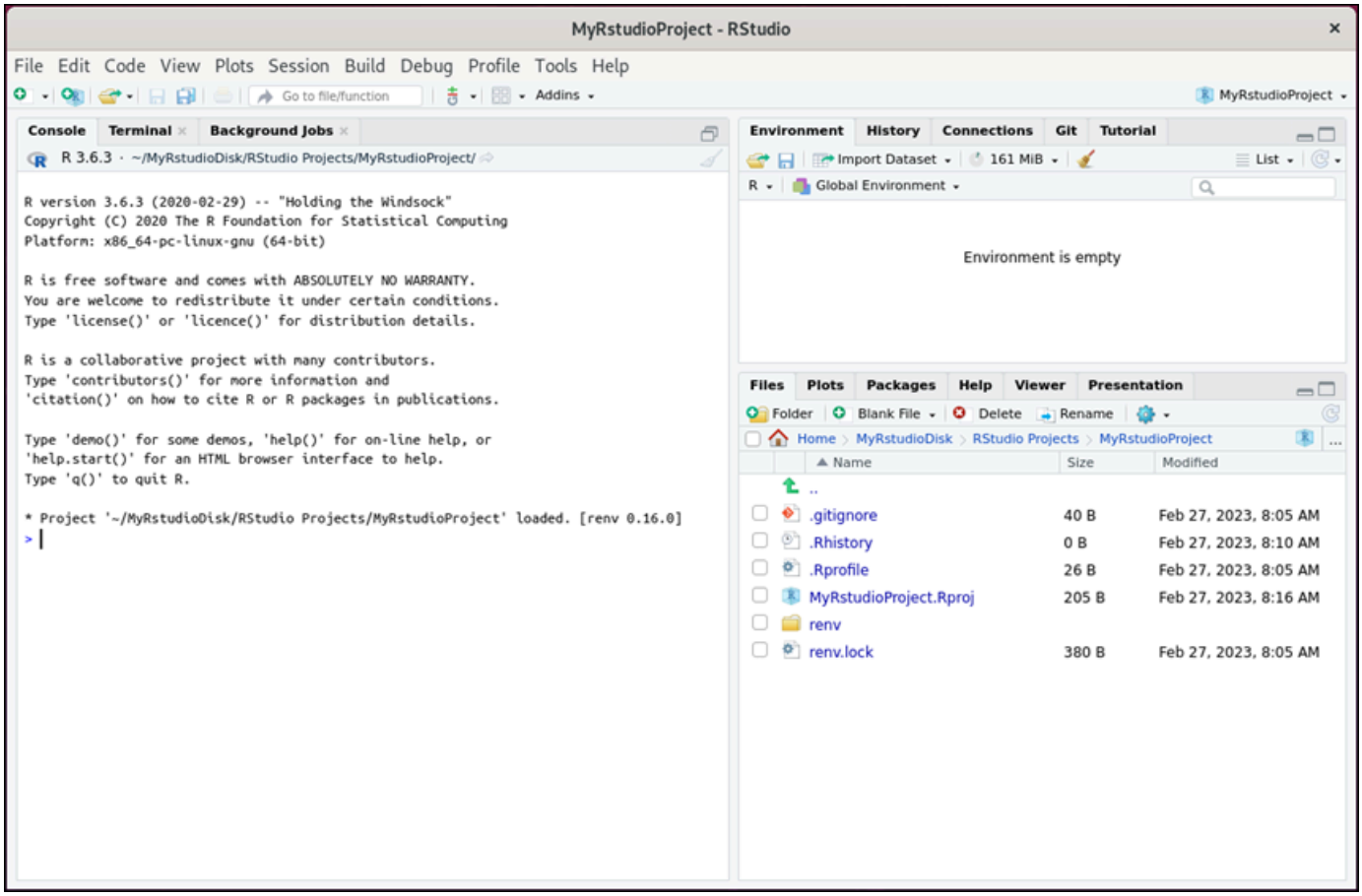


5. 要在 RStudio 中打开项目，请选择文件菜单，然后选择打开项目。浏览到存储项目文件的目录或文件夹。然后选择要打开的文件。

   如果您已将项目文件上传到附加磁盘，请查找挂载该磁盘的目录。默认情况下，Lightsail for Research 会将磁盘挂载到目录中。`/home/lightsail-user/<disk-name>` *<disk-name>*是你给磁盘起的名字。在以下示例中，`MyRstudioDisk` 目录代表已挂载的磁盘，`Projects` 子目录包含我们的 RStudio 项目文件。



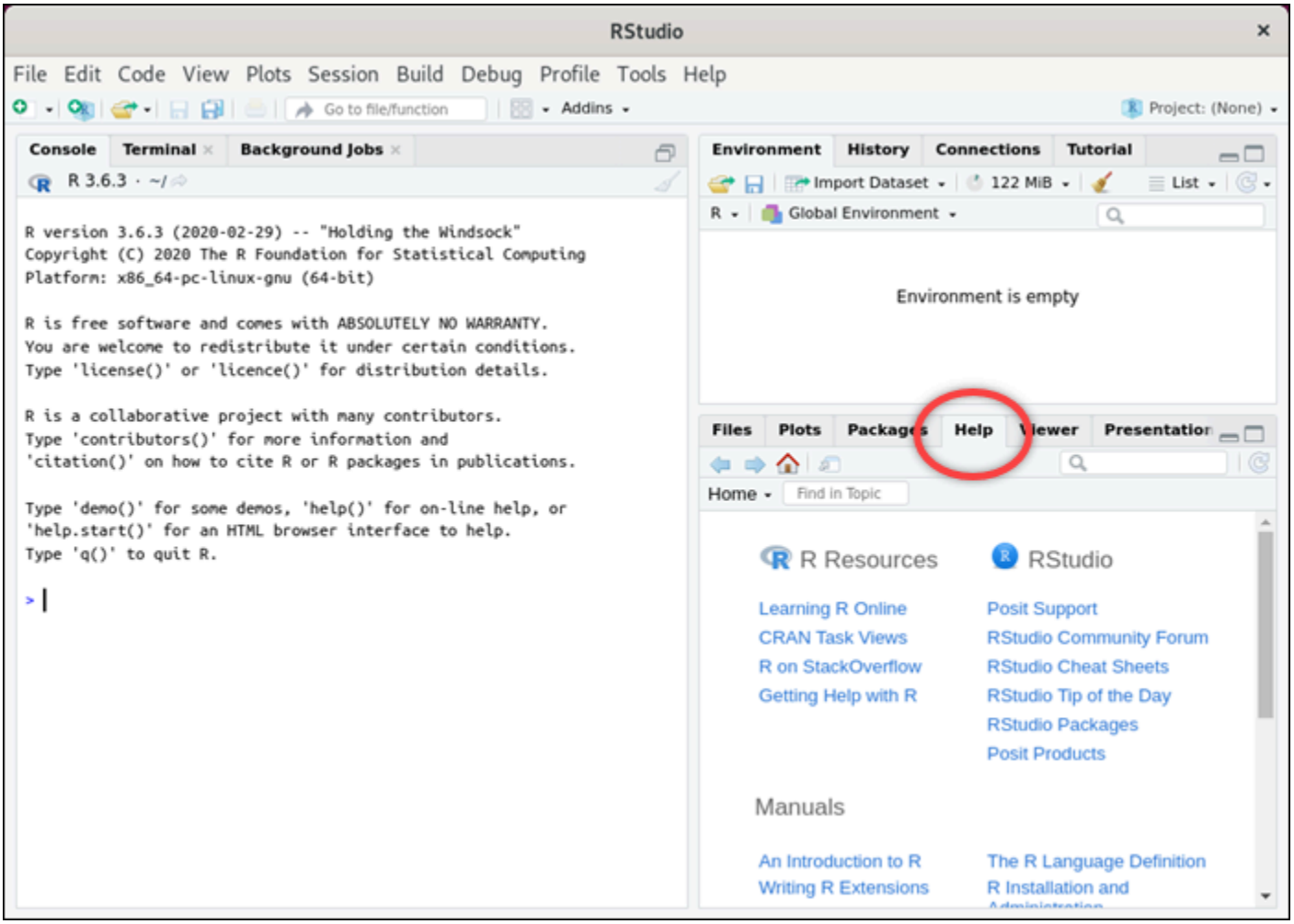
在以下示例中，我们打开了 MyRstudioProject.Rproj 项目文件。



有关如何开始使用 RStudio 的信息，请继续阅读本教程的 步骤 5：阅读 RStudio 文档 部分。

步骤 5：阅读 RStudio 文档

RStudio 应用程序与一个全面的文档包捆绑在一起。要开始学习 RStudio，我们建议您访问 RStudio 中的帮助选项卡，如以下示例所示。



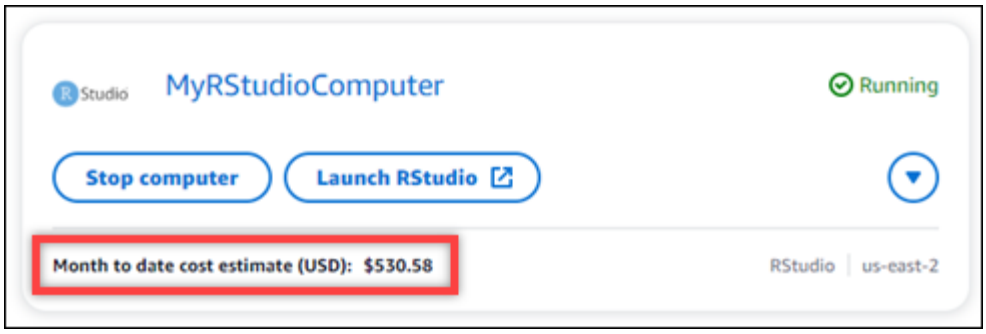
以下是可参阅的 RStudio 在线资源：

- 在线学习 R
- R on StackOverflow
- 获取关于 R 的帮助
- Posit 支持
- RStudio 社区论坛
- RStudio 备忘单
- RStudio 每日贴士（Twitter）
- RStudio 软件包

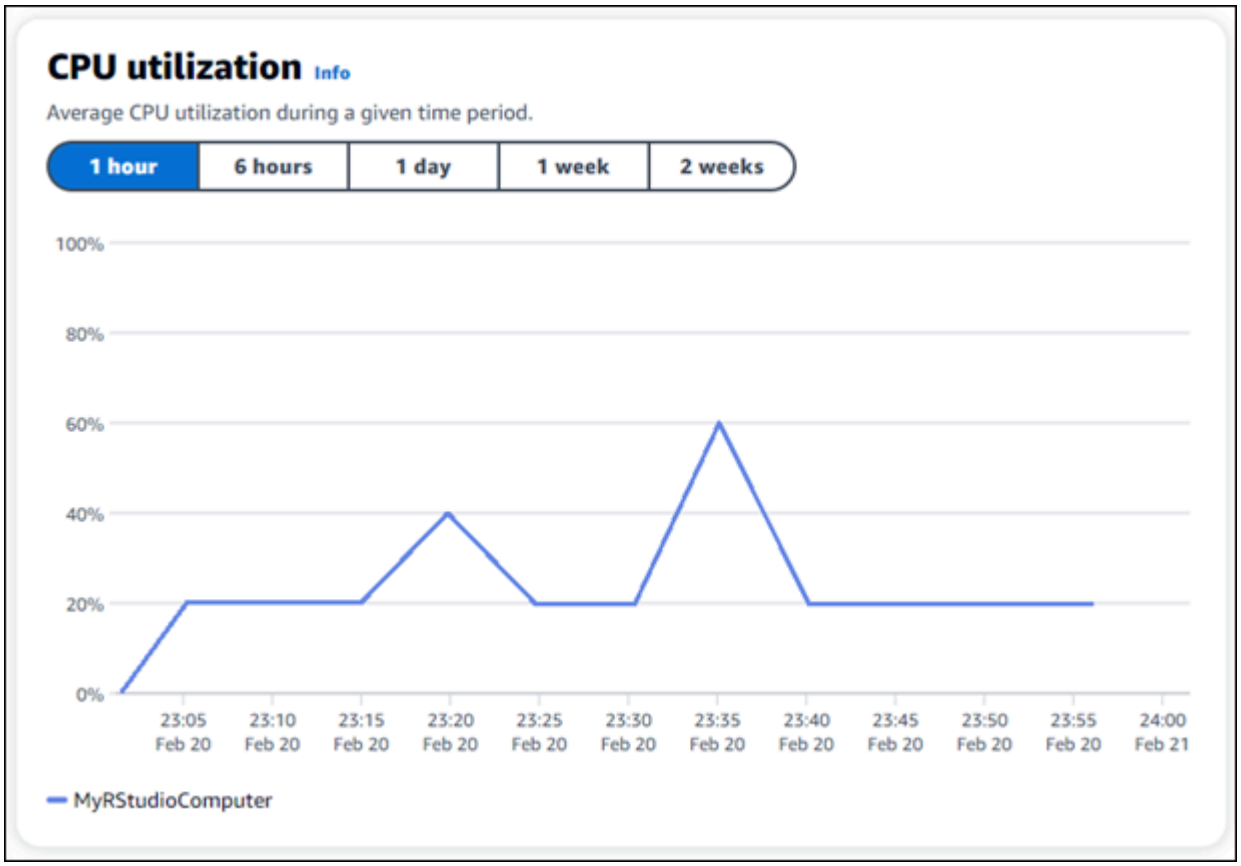
步骤 6：（可选）监控使用情况和成本

Lightsail for Research 资源迄今为止的费用和使用量估算值显示在 Lightsail for Research 控制台的以下区域中。

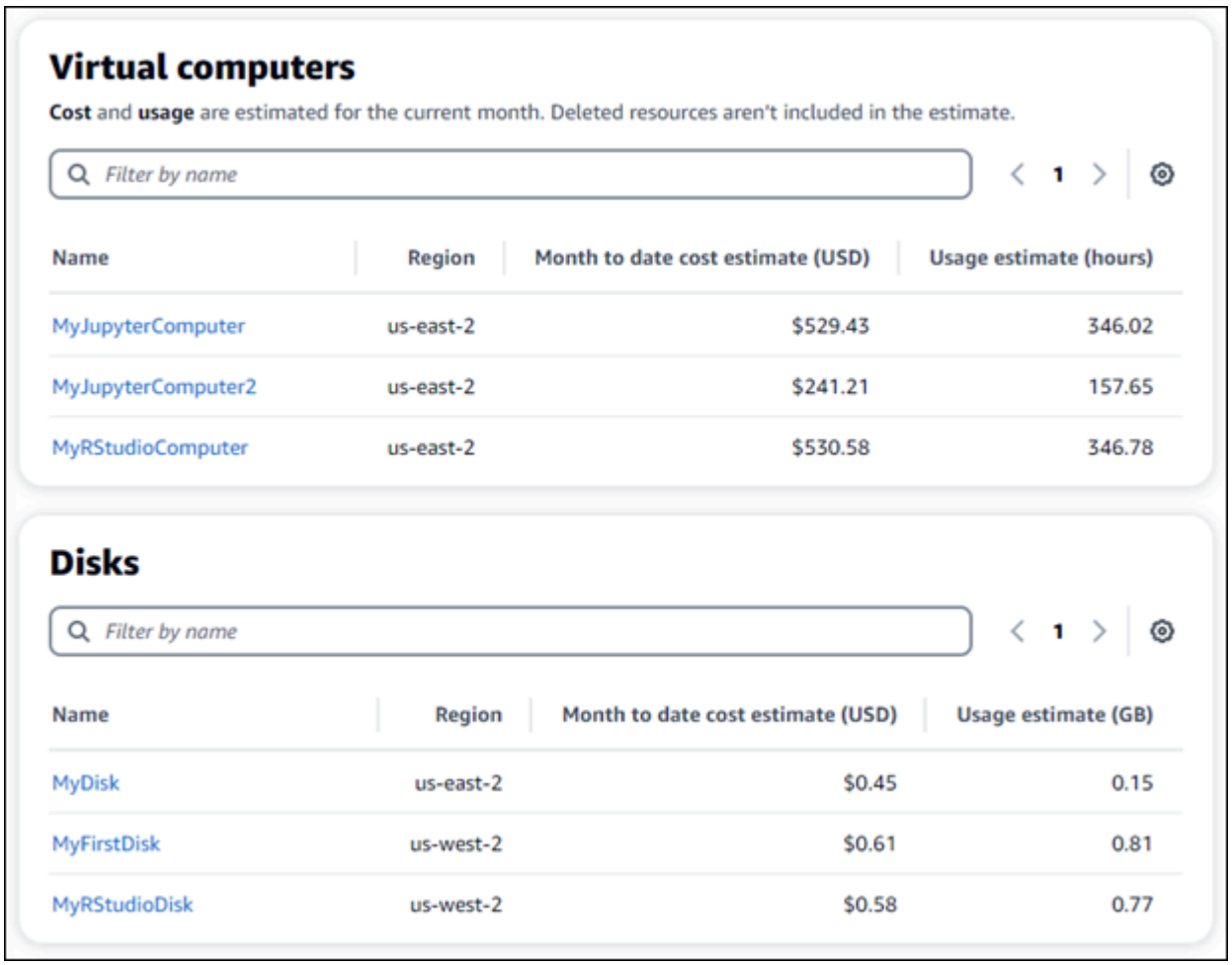
1. 在 Lightsail for Research 控制台的导航窗格中选择 “虚拟计算机”。虚拟计算机的本月至今成本估算列在每台正在运行的虚拟计算机下。



2. 要查看虚拟计算机的 CPU 使用率，请选择虚拟计算机的名称，然后选择控制面板选项卡。



3. 要查看所有 Lightsail for Research 资源的月初至今成本和使用量估算值，请在导航窗格中选择 “使用情况”。



步骤 7：（可选）创建成本控制规则

通过创建成本控制规则来管理虚拟计算机的使用情况和成本。您可以创建停止处于空闲状态的虚拟计算机规则，当计算机在给定时间段内达到指定的 CPU 使用率百分比时，该规则会停止正在运行的计算机。例如，当特定计算机的 CPU 使用率在 30 分钟内等于或低于 5% 时，规则就可以自动停止该计算机。这可能意味着计算机处于空闲状态，而 Lightsail for Research 会停止计算机，这样您就不会为闲置资源产生费用。

> **Important**
>
> 在创建停止处于空闲状态的虚拟计算机的规则之前，我们建议您监控 CPU 使用率几天。记下虚拟计算机处于不同负载下的 CPU 使用率。例如，当虚拟计算机编译代码、处理操作和处于空闲状态时的 CPU 使用率。这将帮助您确定规则的准确阈值。有关更多信息，请参阅本教程的 步骤 6：（可选）监控使用情况和成本 部分。

如果您创建的规则中 CPU 使用率阈值高于您的工作负载，则该规则可以连续停止您的虚拟计算机。例如，如果您在规则停止虚拟计算机后立即启动虚拟计算机，则该规则将重新激活，计算机将再次停止。

有关创建和管理成本控制规则的详细说明，请参阅以下指南：

- 成本控制
- 创建规则
- 删除规则

步骤 8：（可选）创建快照

快照是您的数据的 point-in-time 副本。您可以创建虚拟计算机的快照，并将其用作创建新计算机或备份数据的基准。快照包含还原您的计算机所需的所有数据（从拍摄快照的那一刻开始）。

有关创建和管理快照的详细说明，请参阅以下指南：

- 创建快照
- 查看快照
- 使用快照创建虚拟计算机或磁盘
- 删除快照

步骤 9：（可选）停止或删除虚拟计算机

在完成使用为本教程创建的虚拟计算机后，您可以将其删除。如果您不需要虚拟计算机，则无需支付虚拟计算机费用。

删除虚拟计算机并不会删除其关联的快照或附加磁盘。如果您创建了快照和磁盘，则应手动删除这些快照和磁盘，以免产生费用。

要保存虚拟计算机以备日后使用，但需要避免按标准小时价格收费，您可以停止虚拟计算机而不是将其删除。稍后您可以重新启动。有关更多信息，请参阅 查看虚拟计算机详细信息。有关定价的更多信息，请参阅 Lightsail for Research 定价。

> **Important**
>
> 删除 Lightsail for Research 资源是一项永久性操作。删除的数据无法恢复。如果以后可能需要这些数据，请先创建虚拟计算机的快照，然后再删除它。有关更多信息，请参阅创建快照。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择虚拟计算机。
3. 选择要删除的虚拟计算机。
4. 选择操作，然后选择删除虚拟计算机。
5. 在文本块中键入确认。然后，选择删除虚拟计算机。

虚拟计算机

有了 Amazon Lightsail for Research，你可以在中创建虚拟计算机。 AWS Cloud

创建虚拟计算机时，您需要选择要使用的应用程序和硬件套餐。您可以为虚拟计算机设置支出限额，并选择当虚拟计算机达到该限额时会发生什么。例如，您可以选择自动停止虚拟计算机，这样您的费用就不会超过配置的预算。

> **Important**
>
> 从 2024 年 3 月 22 日起，Lightsail for Research 虚拟计算机将默认启用 imdsv2。

主题

应用程序和硬件套餐

在创建 Amazon Lightsail for Research 虚拟计算机时，您需要为其选择应用程序和硬件计划（计划）。

应用程序提供软件配置（例如，应用程序和操作系统）。套餐提供虚拟计算机的硬件，例如 vCPU 数量、内存、存储空间和每月数据传输限额。应用程序和套餐共同构成了虚拟计算机的配置。

> **Note**
>
> 创建虚拟计算机后，则不能再更改其应用程序或套餐。但是，您可以创建虚拟计算机的快照，然后在使用快照创建新的虚拟计算机时选择新的套餐。有关快照的更多信息，请参阅 快照。

主题

应用程序

Amazon Lightsail for Research 提供并管理包含启动虚拟计算机所需的应用程序和操作系统的计算机映像。在 Lightsail for Research 中创建虚拟计算机时，您可以从应用程序列表中进行选择。所有 Lightsail for Research 应用程序映像都使用 Ubuntu (Linux) 操作系统。

Lightsail for Research 中提供了以下应用程序：

- JupyterLab— JupyterLab 是一个基于 Web 的集成开发环境 (IDE)，用于笔记本电脑、代码和数据。借助其灵活的界面，您可以配置和安排数据科学、科学计算、计算新闻和机器学习的工作流程。有关更多信息，请参阅 Jupyter 项目文档。
- RStudio – RStudio 是一个开源集成式开发环境（IDE），适用于 R 语言（一种用于统计计算和图形的编程语言）和 Python。它结合了源代码编辑器、构建自动化工具和调试程序，以及用于绘图和工作区管理的工具。有关更多信息，请参阅 RStudio IDE。
- VSCodium – VSCodium 是 Microsoft 编辑器 VS Code 的社区主导型二进制发行版。有关更多信息，请参阅 VSCodium。
- Scilab – Scilab 是一个开源数值计算软件包，也是一种面向数值的高级编程语言。有关更多信息，请参阅 Scilab。
- Ubuntu 20.04 LTS – Ubuntu 是一款基于 Debian 的开源 Linux 发行版。Ubuntu Server 精简、快速、功能强大，提供可靠、可预测、经济的服务。它是构建虚拟计算机的绝佳基础。有关更多信息，请参阅 Ubuntu 版本。

计划

计划提供硬件规格并确定您的 Lightsail for Research 虚拟计算机的定价。套餐包括固定数量的内存（RAM）、计算（vCPU）、基于 SSD 的存储卷（磁盘）空间和每月数据传输限额。套餐按小时按需收费，因此您只需为虚拟计算机的运行时间付费。

您选择的套餐可能取决于您的工作负载所需的资源。Lightsail for Research 提供以下计划类型：

- 标准 - 计算标准套餐是计算优化型套餐，是受益于高性能处理器的受计算限制的应用程序的理想选择。
- GPU - GPU 套餐为通用 GPU 计算提供经济高效的高性能平台。您可以使用这些套餐为科学、工程和渲染应用程序和工作负载加速。

标准套餐

以下是 Lightsail for Research 中提供的标准计划的硬件规格。

套餐名称	vCPU	内存	存储空间	每月数据传输限额
标准 XL	4	8 GB	50 GB	512 GB
标准 2XL	8	16 GB	50 GB	512 GB
标准 4XL	16	32 GB	50 GB	512 GB

GPU 套餐

以下是 Lightsail for Research 中可用的 GPU 计划的硬件规格。

套餐名称	vCPU	内存	存储空间	每月数据传输限额
GPU XL	4	16 GB	50 GB	1 TB
GPU 2XL	8	32 GB	50 GB	1 TB
GPU 4XL	16	64 GB	50 GB	1 TB

创建虚拟计算机

完成以下步骤，创建运行应用程序的 Lightsail for Research 虚拟计算机。

1. 登录 Lightsail for Research 控制台。
2. 在主页上，选择创建虚拟计算机。
3. AWS 区域 为您的虚拟计算机选择一台靠近您的实际位置的计算机。
4. 选择应用程序和硬件套餐。有关更多信息，请参阅 应用程序和硬件套餐。
5. 输入虚拟计算机的名称。有效字符包括字母数字字符、数字、句点、连字符和下划线。

   虚拟计算机名称还必须满足以下要求：

   - 在你的 Lightsail for Research 账户 AWS 区域 中，在每个账户中都要
   - 包含 2–255 个字符。
   - 以字母数字字符或数字作为开头和结尾。
6. 在摘要面板中选择创建虚拟计算机。

几分钟之内，您的 Lightsail for Research 虚拟计算机就准备就绪，您可以通过图形用户界面 (GUI) 会话与之连接。有关连接到 Lightsail for Research 虚拟计算机的更多信息，请参阅。启动虚拟计算机的应用程序

> **Important**
>
> 默认情况下，新创建的虚拟计算机会打开一组防火墙端口。有关这些端口的更多信息，请参阅管理虚拟计算机的防火墙端口。

查看虚拟计算机详细信息

完成以下步骤，即可在 Lightsail for Research 账户中查看虚拟计算机列表及其详细信息。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中选择虚拟计算机，查看您的账户中的虚拟计算机列表。

选择虚拟计算机的名称，以导航到其管理页面。以下是管理页面提供的信息：

- 虚拟计算机名称 - 您的虚拟计算机的名称。
- 状态 - 您的虚拟计算机可能具有以下状态代码之一：
  - Creating
  - Running
  - Stopping
  - Stopped
  - 未知
- AWS 区域— AWS 区域 您的虚拟计算机是在中创建的。
- 应用程序和硬件 - 虚拟计算机的应用程序和硬件套餐。
- 每月使用量估算 - 当前计费周期内此虚拟计算机的估计每小时使用量。
- 本月至今成本估算 - 此计费周期内虚拟计算机的估算成本（以美元计）。
- 控制面板 - 在控制面板选项卡中，您可以启动会话以访问虚拟计算机的应用程序。您还可以查看 CPU 使用率。CPU 使用率表明了虚拟计算机应用程序所使用的处理能力。图表中显示的每个数据点都表示一段时间内的平均 CPU 使用率。
- 成本控制规则 - 您定义的规则可帮助管理虚拟计算机的使用情况和成本。
- 虚拟计算机使用情况 - 给定计费周期的成本和使用情况估算。可按日期和时间对其进行筛选。
- 存储 - 在存储选项卡上创建、附加和分离虚拟计算机磁盘。磁盘是可以附加到虚拟计算机并作为硬盘挂载的存储卷。
- 标签 - 通过“标签”选项卡管理您的虚拟计算机标签。标签是您分配给 AWS 资源的标签。每个标签都由一个键和一个可选值组成。您可以使用标签来搜索和筛选资源，或者跟踪 AWS 成本。

启动虚拟计算机的应用程序

完成以下步骤，启动在 Lightsail for Research 虚拟计算机上运行的应用程序。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择虚拟计算机。
3. 找到您要启动应用程序的虚拟计算机的名称。

> **Note**
>
> 如果虚拟计算机已停止，请先选择启动计算机按钮将其打开。

4. 选择启动应用程序。例如，启动 JupyterLab。应用程序会话将在新的 Web 浏览器窗口中打开。

> **Important**
>
> 如果您的 Web 浏览器安装了弹出窗口阻止程序，则在打开会话之前，您可能需要允许来自 aws.amazon.com 域名的弹出窗口。

访问虚拟计算机的操作系统

完成以下步骤即可访问您的 Lightsail for Research 虚拟计算机的操作系统。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择虚拟计算机。
3. 找到您的虚拟计算机的名称，然后选择计算机状态下方的操作按钮下拉列表。

> **Note**
>
> 如果虚拟计算机已停止，请先选择启动按钮将其打开。

4. 选择访问操作系统。将在新的浏览器窗口中打开操作系统会话。

> **Important**
>
> 如果您的 Web 浏览器安装了弹出窗口阻止程序，则在打开会话之前，您可能需要允许来自 aws.amazon.com 域名的弹出窗口。

管理虚拟计算机的防火墙端口

Amazon Lightsail for Research 中的防火墙控制允许连接到您的虚拟计算机的流量。在虚拟计算机的防火墙中添加规则，指定允许连接到虚拟计算机的协议、端口和源 IPv4 或 IPv6 地址。防火墙规则始终是允许型的；您无法创建拒绝访问的规则。向虚拟计算机的防火墙添加规则，以允许流量到达虚拟计算机。每个虚拟计算机都具有两个防火墙；一个防火墙用于 IPv4 地址，另一个用于 IPv6 地址。这两个防火墙彼此独立，并且包含一组预配置规则，用于筛选进入实例的流量。

协议

协议是在两台计算机之间传输数据的格式。可以在防火墙规则中指定以下协议：

- 传输控制协议（TCP）主要用于建立和维持客户端与虚拟计算机上运行的应用程序之间的连接。它是一种广泛使用的协议，您可能经常在防火墙规则中指定该协议。
- 用户数据报协议（UDP）主要用于在客户端和虚拟计算机上运行的应用程序之间建立低延迟的容损连接。它最适用于所感知的延迟至关重要的网络应用程序，例如游戏、语音和视频通信。
- Internet 控制消息协议（ICMP）主要用于诊断网络通信问题，例如，确定数据是否及时到达预期目的地。它最适用于 Ping 实用程序，可以使用该实用程序来测试本地计算机和虚拟计算机之间的连接速度。它会报告数据到达虚拟计算机并返回到本地计算机所花费的时间。
- 所有用于允许所有协议流量流入虚拟计算机。当不确定要指定哪个协议时，请指定此协议。这包括所有互联网协议；而不仅仅是上面指定的协议。有关更多信息，请参阅互联网编号分配机构网站上的协议编号。

端口

与计算机上的物理端口（允许计算机与键盘和指针等外围设备进行通信）类似，防火墙端口将充当虚拟计算机的互联网通信端点。当客户端寻求与您的虚拟计算机连接时，它会公开一个端口来建立通信。

可在防火墙规则中指定的端口范围是 0 到 65535。在创建防火墙规则以允许客户端与虚拟计算机建立连接时，可以指定要使用的协议。您还可以指定用于建立连接的端口号和允许建立连接的 IP 地址。

默认情况下，对于新创建的虚拟计算机，以下端口处于打开状态。

- TCP
  - 22 - 用于 Secure Shell（SSH）。
  - 80 - 用于超文本传输协议（HTTP）。
  - 443 - 用于安全超文本传输协议（HTTPS）。

- 8443 - 用于安全超文本传输协议（HTTPS）。

为什么要打开和关闭端口

打开端口时，即允许客户端与虚拟计算机建立连接。关闭端口时，会阻止与虚拟计算机建立连接。例如，要允许 SSH 客户端连接到虚拟计算机，您需要配置一条防火墙规则，只允许来自需要建立连接的计算机的 IP 地址通过端口 22 进行 TCP 连接。在这种情况下，您不想允许任何 IP 地址与您的虚拟计算机建立 SSH 连接。这样做可能会导致安全风险。如果您的实例的防火墙上已经配置了此规则，则可以将其删除以阻止 SSH 客户端连接到您的虚拟计算机。

以下过程向您展示如何获取虚拟计算机上当前打开的端口、如何打开新端口和关闭端口。

主题

完成先决条件

在开始之前，请满足以下先决条件。

- 在 Lightsail 中创建一台用于研究的虚拟计算机。有关更多信息，请参阅 创建虚拟计算机。
- 下载并安装 AWS Command Line Interface (AWS CLI)。有关更多信息，请参阅《AWS Command Line Interface 用户指南版本 2》中的安装或更新最新版本的 AWS CLI。
- 配置 AWS CLI 以访问您的 AWS 账户。有关更多信息，请参阅《AWS Command Line Interface 用户指南版本 2》中的配置基础知识。

获取虚拟计算机的端口状态

完成以下过程以获取虚拟计算机的端口状态。此过程使用`get-instance-port-states` AWS CLI 命令获取特定 Lightsail for Research 虚拟计算机的防火墙端口状态、允许通过端口连接到虚拟计算机的 IP 地址以及协议。有关更多信息，请参阅 AWS CLI 命令参考 中的 get-instance-port-states。

1. 此步骤取决于您本地计算机的操作系统。

- 如果您的本地计算机使用 Windows 操作系统，请打开命令提示符窗口。
- 如果您的本地计算机使用基于 Linux 或 Unix 的操作系统（包括 macOS），请打开终端窗口。

2. 输入以下命令，获取防火墙端口状态和允许的 IP 地址和协议。在命令中，将 *REGION* 替换为创建虚拟计算机所在的 AWS 区域的代码，例如 us-east-2。将 *NAME* 替换为您的虚拟计算机的名称。

```
aws lightsail get-instance-port-states --region REGION --instance-name NAME
```

示例

```
aws lightsail get-instance-port-states --region us-east-2 --instance-name MyUbuntu
```

响应将显示开放的端口和协议，以及允许连接到您的虚拟计算机的 IP CIDR 范围。

```
[redacted] % aws lightsail get-instance-port-states --region us-east-2 --instance
-name MyUbuntu
PORTSTATES      80      tcp     open    80
CIDRS   0.0.0.0/0
IPV6CIDRS       ::/0
PORTSTATES      22      tcp     open    22
CIDRS   0.0.0.0/0
IPV6CIDRS       ::/0
PORTSTATES      8443    tcp     open    8443
CIDRS   0.0.0.0/0
IPV6CIDRS       ::/0
PORTSTATES      443     tcp     open    443
CIDRS   0.0.0.0/0
IPV6CIDRS       ::/0
```

有关如何打开端口的信息，请继续阅读下一节。

打开虚拟计算机的端口

完成以下过程，以为虚拟计算机打开端口。此过程使用open-instance-public-ports AWS CLI 命令。打开防火墙端口，以允许从可信的 IP 地址或 IP 地址范围建立连接。例如，要允许 IP 地址 192.0.2.44，请指定 192.0.2.44 或 192.0.2.44/32。要允许 IP 地址 192.0.2.0 至 192.0.2.255，请指定 192.0.2.0/24。有关更多信息，请参阅 AWS CLI 命令参考 中的 open-instance-public-ports。

1. 此步骤取决于您本地计算机的操作系统。

- 如果您的本地计算机使用 Windows 操作系统，请打开命令提示符窗口。
- 如果您的本地计算机使用基于 Linux 或 Unix 的操作系统（包括 macOS），请打开终端窗口。

2. 输入以下命令以打开端口。

   在以下命令中，替换以下项目：

   - *REGION*替换为创建虚拟计算机的 AWS 区域的代码，例如us-east-2。
   - 将 *NAME* 替换为您的虚拟计算机的名称。
   - 将 *FROM-PORT* 替换为要打开的一系列端口中的第一个端口。
   - 将 *PROTOCOL* 替换为 IP 协议名称。例如，TCP。
   - 将 *TO-PORT* 替换为要打开的一系列端口中的最后一个端口。
   - 将 *IP* 替换为您想要允许连接到虚拟计算机的 IP 地址或 IP 地址范围。

```
aws lightsail open-instance-public-ports --region REGION --instance-name NAME --
port-info fromPort=FROM-PORT, protocol=PROTOCOL, toPort=TO-PORT,cidrs=IP
```

   示例

```
aws lightsail open-instance-public-ports --region us-east-2 --instance-
name MyUbuntu --port-info fromPort=22, protocol=TCP, toPort=22,cidrs=192.0.2.0/24
```

   响应将显示新添加的端口、协议，以及允许连接到您的虚拟计算机的 IP CIDR 范围。

```
[redacted] % aws lightsail open-instance-public-ports --instance-name MyUbuntu -
-port-info fromPort=22,protocol=TCP,toPort=22,cidrs=192.0.2.0/24
{
    "operation": {
        "id": "0789ead5-6996-4277-97b6-0cc7fad55daf",
        "resourceName": "MyUbuntu",
        "resourceType": "Instance",
        "createdAt": "2023-02-15T16:41:50.048000-08:00",
        "location": {
            "availabilityZone": "us-east-2a",
            "regionName": "us-east-2"
        },
        "isTerminal": true,
        "operationDetails": "22/tcp(192.0.2.0/24)",
        "operationType": "OpenInstancePublicPorts",
        "status": "Succeeded",
        "statusChangedAt": "2023-02-15T16:41:50.048000-08:00"
    }
}
```

   有关如何关闭端口的信息，请继续阅读下一节。

虚拟计算机的关闭端口

完成以下过程，以为虚拟计算机关闭端口。此过程使用`close-instance-public-ports` AWS CLI 命令。有关更多信息，请参阅 AWS CLI 命令参考 中的 close-instance-public-ports。

1. 此步骤取决于您本地计算机的操作系统。
   - 如果您的本地计算机使用 Windows 操作系统，请打开命令提示符窗口。
   - 如果您的本地计算机使用基于 Linux 或 Unix 的操作系统（包括 macOS），请打开终端窗口。
2. 输入以下命令以关闭端口。

   在以下命令中，替换以下项目：

   - *REGION*替换为创建虚拟计算机的 AWS 区域的代码，例如`us-east-2`。
   - 将 *NAME* 替换为您的虚拟计算机的名称。
   - 将 *FROM-PORT* 替换为要关闭的一系列端口中的第一个端口。
   - 将 *PROTOCOL* 替换为 IP 协议名称。例如，TCP。
   - 将 *TO-PORT* 替换为要关闭的一系列端口中的最后一个端口。
   - 将 *IP* 替换为要删除的 IP 地址或 IP 地址范围。

   ```
   aws lightsail close-instance-public-ports --region REGION --instance-name NAME --
   port-info fromPort=FROM-PORT, protocol=PROTOCOL, toPort=TO-PORT,cidrs=IP
   ```

   示例

   ```
   aws lightsail close-instance-public-ports --region us-east-2 --instance-
   name MyUbuntu --port-info fromPort=22, protocol=TCP, toPort=22,cidrs=192.0.2.0/24
   ```

   响应将显示端口和协议，以及已关闭且不再允许连接到虚拟计算机的 IP CIDR 范围。

继续执行后续步骤

成功管理虚拟计算机的防火墙端口后，您可以完成以下其他后续步骤：

- 获取虚拟计算机的密钥对。使用密钥对，您可以使用许多 SSH 客户端（例如 OpenSSH、PuTTY 和 Windows Subsystem for Linux）建立连接。有关更多信息，请参阅 获取虚拟计算机的密钥对。
- 使用 SSH 连接到您的虚拟计算机，以使用命令行对其进行管理。有关更多信息，请参阅 使用 Secure Copy 将文件传输到虚拟计算机。
- 使用 SCP 连接到您的虚拟计算机，以安全地传输文件。有关更多信息，请参阅 使用 Secure Copy 将文件传输到虚拟计算机。

获取虚拟计算机的密钥对

密钥对由公钥和私钥组成，是您在连接到 Amazon Lightsail for Research 虚拟计算机时用来证明自己身份的一组安全证书。公钥存储在 Lightsail for Research 中的每台虚拟计算机上，私钥保存在本地计算机上。使用私有密钥可在虚拟计算机上安全地建立安全外壳协议（SSH）。拥有私有密钥的任何人都可以连接到您的虚拟计算机，因此请务必将您的私有密钥存储在一个安全的位置。

首次创建 Lightsail 实例或 Lightsail for Research 虚拟计算机时，会自动创建亚马逊 Lightsail 默认密钥对 (DKP)。DKP 特定于您在其中创建实例或虚拟计算机的每个 AWS 区域。例如，美国东部（俄亥俄州）区域的 Lightsail DKP（us-east-2）适用于您在美国东部（俄亥俄州）在 Lightsail 和 Lightsail for Research 中创建的所有计算机，这些计算机在创建时配置为使用 DKP。Lightsail for Research 会自动将 DKP 的公钥存储在你创建的虚拟计算机上。你可以随时通过对 Lightsail 服务进行 API 调用来下载 DKP 的私钥。

在本文档中，我们将介绍如何获取虚拟计算机的 DKP。获取 DKP 后，您可以使用许多 SSH 客户端（例如 OpenSSH、PuTTY 和 Windows Subsystem for Linux）建立连接。您还可以使用 Secure Copy（SCP）将文件从您的本地计算机安全传输到您的虚拟计算机。

> **Note**
>
> 您还可以使用基于浏览器的 NICE DCV 客户端与虚拟计算机建立远程显示协议连接。NICE DCV 在 Lightsail for Research 主机中可用。该 RDP 客户端不需要您为计算机获取密钥对。有关更多信息，请参阅 启动虚拟计算机的应用程序 和 访问虚拟计算机的操作系统。

主题

完成先决条件

在开始之前，请满足以下先决条件。

- 在 Lightsail 中创建一台用于研究的虚拟计算机。有关更多信息，请参阅 创建虚拟计算机。
- 下载并安装 AWS Command Line Interface (AWS CLI)。有关更多信息，请参阅《AWS Command Line Interface 用户指南版本 2》中的安装或更新最新版本的 AWS CLI。
- 配置 AWS CLI 以访问您的 AWS 账户。有关更多信息，请参阅《AWS Command Line Interface 用户指南版本 2》中的配置基础知识。
- 下载并安装 jq。它是一个轻型且灵活的命令行 JSON 处理器，用于在以下过程中从 AWS CLI的 JSON 输出中提取密钥对详细信息。有关下载和安装 jq 的更多信息，请参阅 jq 网站上的下载 jq。

获取虚拟计算机的密钥对

完成以下过程之一，即可在 Lightsail for Research 中获取虚拟计算机的 Lightsail DKP。

使用 Windows 本地计算机获取虚拟计算机的密钥对

如果您的本地计算机使用 Windows 操作系统，则适用此过程。此过程使用`download-default-key-pair` AWS CLI 命令获取某个区域的 Lightsail DKP。 AWS 有关更多信息，请参阅 AWS CLI 命令参考 中的 download-default-key-pair。

1. 打开 Command Prompt (命令提示符窗口)。
2. 输入以下命令以获取特定区域的 Lightsail DKP。 AWS 此命令将信息保存到 dkp-details.json 文件中。在命令中，*region-code*替换为创建虚拟计算机的 AWS 区域的代码，例如us-east-2。

```
aws lightsail download-default-key-pair --region region-code > dkp-details.json
```

示例

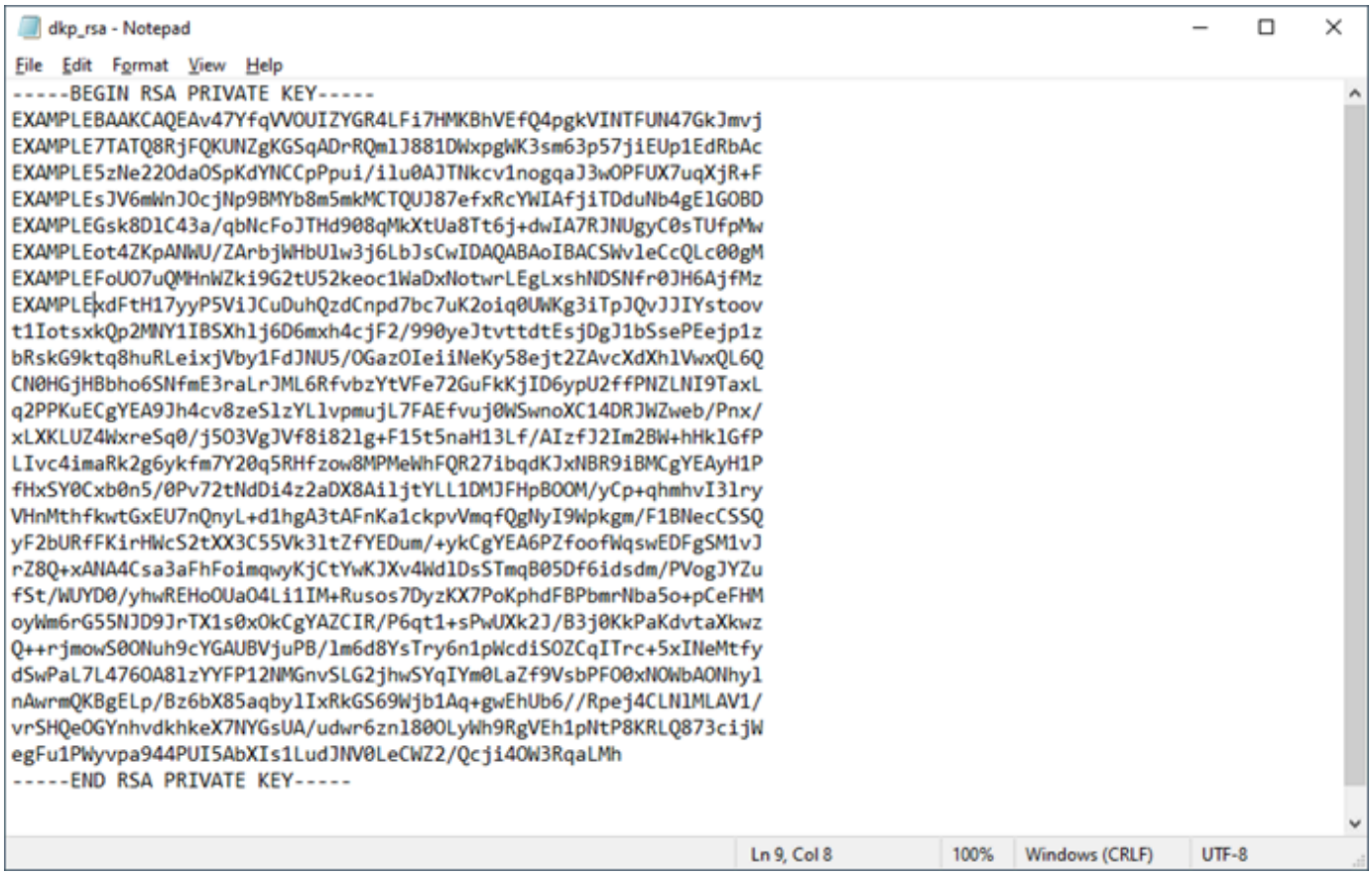
```
aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
```

该命令没有响应。您可以通过打开dkp-details.json文件并查看 Lightsail DKP 信息是否已保存来确认命令是否成功。dkp-details.json 文件的内容应与以下示例类似。如果文件为空，则命令失败。

3. 输入以下命令从 dkp-details.json 文件中提取私有密钥信息并将其添加到新的 dkp_rsa 私有密钥文件中。

```
type dkp-details.json | jq -r ".privateKeyBase64" > dkp_rsa
```

该命令没有响应。您可以通过打开 dkp_rsa 文件并查看其中是否包含信息来确认命令是否成功。dkp_rsa 文件的内容应与以下示例类似。如果文件为空，则命令失败。



现在，您拥有与虚拟计算机建立 SSH 或 SCP 连接所需的私有密钥。继续阅读下一节，了解后续步骤。

为使用 Linux、Unix 或 macOS 本地计算机的虚拟计算机获取密钥对

如果您的本地计算机使用 Linux、Unix 或 macOS 操作系统，则适用此过程。此过程使用download-default-key-pair AWS CLI 命令获取某个区域的 Lightsail DKP。 AWS 有关更多信息，请参阅 AWS CLI 命令参考 中的 download-default-key-pair。

1. 打开终端窗口。

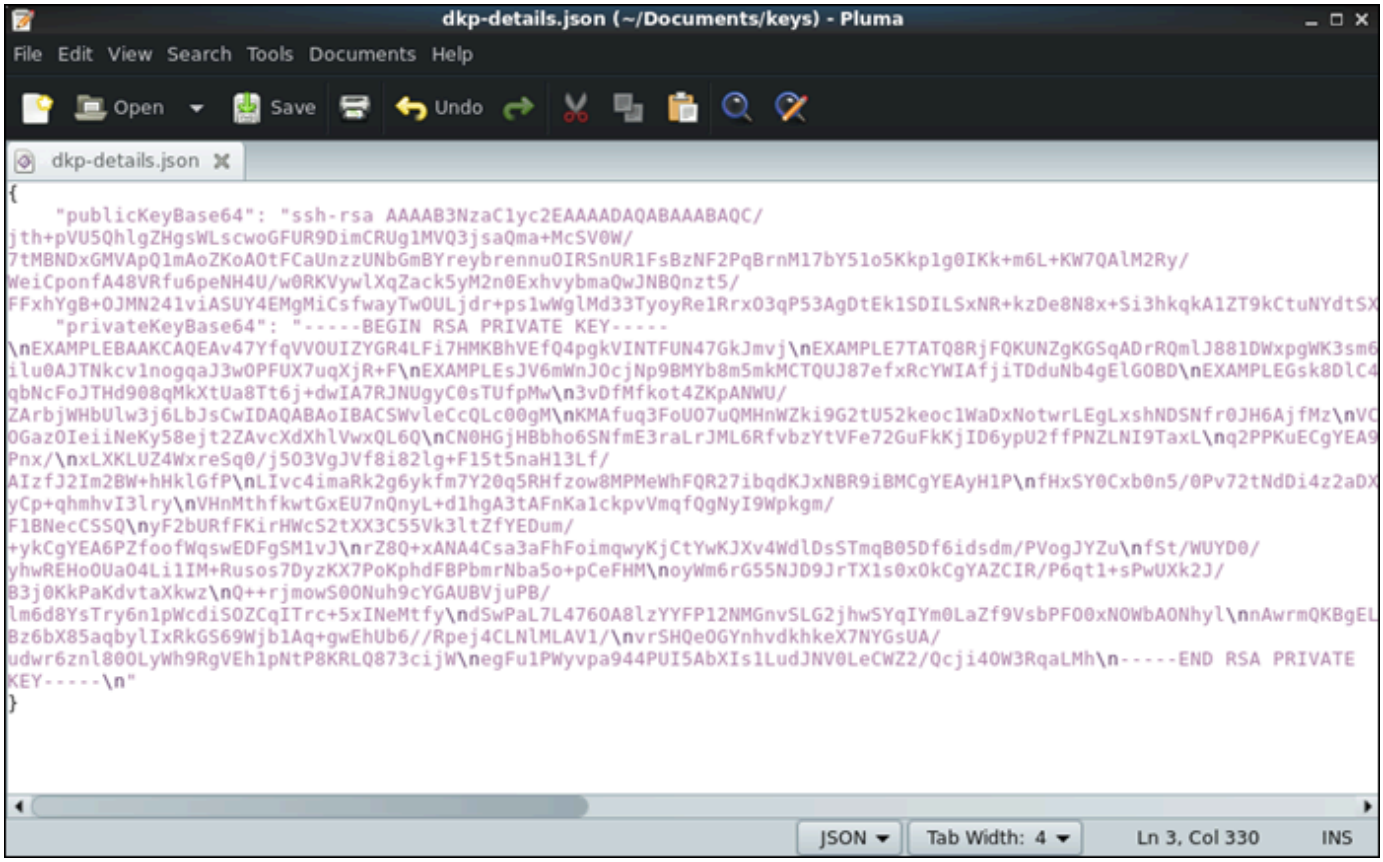
2. 输入以下命令以获取特定区域的 Lightsail DKP。 AWS 此命令将信息保存到 dkp-details.json 文件中。在命令中，*region-code*替换为创建虚拟计算机的 AWS 区域的代码，例如us-east-2。

```
aws lightsail download-default-key-pair --region region-code > dkp-details.json
```

示例

```
aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
```

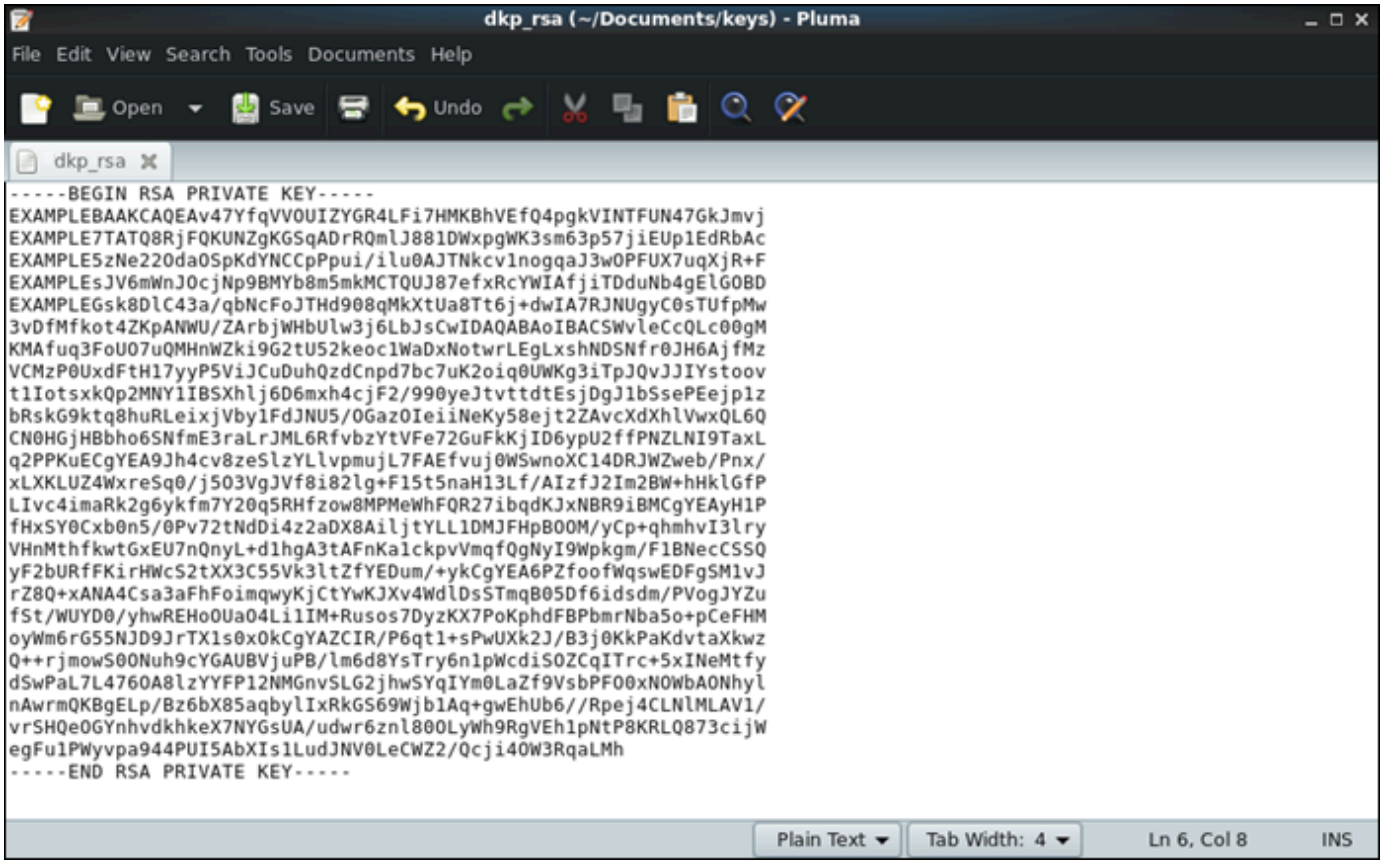
该命令没有响应。您可以通过打开dkp-details.json文件并查看 Lightsail DKP 信息是否已保存来确认命令是否成功。dkp-details.json 文件的内容应与以下示例类似。如果文件为空，则命令失败。



3. 输入以下命令从 dkp-details.json 文件中提取私有密钥信息并将其添加到新的 dkp_rsa 私有密钥文件中。

```
cat dkp-details.json | jq -r '.privateKeyBase64' > dkp_rsa
```

该命令没有响应。您可以通过打开 dkp_rsa 文件并查看其中是否包含信息来确认命令是否成功。dkp_rsa 文件的内容应与以下示例类似。如果文件为空，则命令失败。



4. 输入以下命令，为 dkp_rsa 文件设置权限。

```
chmod 600 dkp_rsa
```

现在，您拥有与虚拟计算机建立 SSH 或 SCP 连接所需的私有密钥。继续阅读下一节，了解后续步骤。

继续执行后续步骤

成功获取虚拟计算机的密钥对后，您可以完成以下其他后续步骤：

- 使用 SSH 连接到您的虚拟计算机，以使用命令行对其进行管理。有关更多信息，请参阅 使用 Secure Shell 连接到虚拟计算机。
- 使用 SCP 连接到您的虚拟计算机，以安全地传输文件。有关更多信息，请参阅 使用 Secure Copy 将文件传输到虚拟计算机。

使用 Secure Shell 连接到虚拟计算机

您可以使用安全外壳协议 (SSH) 连接到 Amazon Lightsail for Research 中的虚拟计算机。您可以使用 SSH 远程管理虚拟计算机，这样您就可以通过互联网登录计算机并运行命令。

> **Note**
>
> 您还可以使用基于浏览器的 NICE DCV 客户端与虚拟计算机建立远程显示协议连接。NICE DCV 在 Lightsail for Research 主机中可用。有关更多信息，请参阅 访问虚拟计算机的操作系统。

主题

完成先决条件

在开始之前，请满足以下先决条件。

- 在 Lightsail 中创建一台用于研究的虚拟计算机。有关更多信息，请参阅 创建虚拟计算机。
- 确保您要连接的虚拟计算机处于运行状态。另外，请记下虚拟计算机的名称和创建虚拟计算机的 AWS 区域。在此流程的稍后阶段，您将需要这些信息。有关更多信息，请参阅 查看虚拟计算机详细信息。
- 确保您要连接的虚拟计算机上的端口 22 已打开。这是 SSH 使用的默认端口。该端口预设情况下打开。但是，如果您将其关闭，则必须先将其重新打开，然后才能继续使用。有关更多信息，请参阅 管理虚拟计算机的防火墙端口。
- 为您的虚拟计算机获取 Lightsail 默认密钥对 (DKP)。有关更多信息，请参阅 获取虚拟计算机的密钥对。

> **Tip**
>
> 如果您打算使用 AWS CloudShell 连接到您的虚拟计算机，请参阅使用 Connect 连接到虚拟计算机 AWS CloudShell下一节中的。有关更多信息，请参阅什么是 AWS CloudShell。否则，请继续执行下一个先决条件。

- 下载并安装 AWS Command Line Interface (AWS CLI)。有关更多信息，请参阅《AWS Command Line Interface 用户指南版本 2》中的安装或更新最新版本的 AWS CLI。
- 配置 AWS CLI 以访问您的 AWS 账户。有关更多信息，请参阅《AWS Command Line Interface 用户指南版本 2》中的配置基础知识。
- 下载并安装 jq。它是一个轻型且灵活的命令行 JSON 处理器，用于在以下过程中提取密钥对详细信息。有关下载和安装 jq 的更多信息，请参阅 jq 网站上的下载 jq。

使用 SSH 连接到虚拟计算机

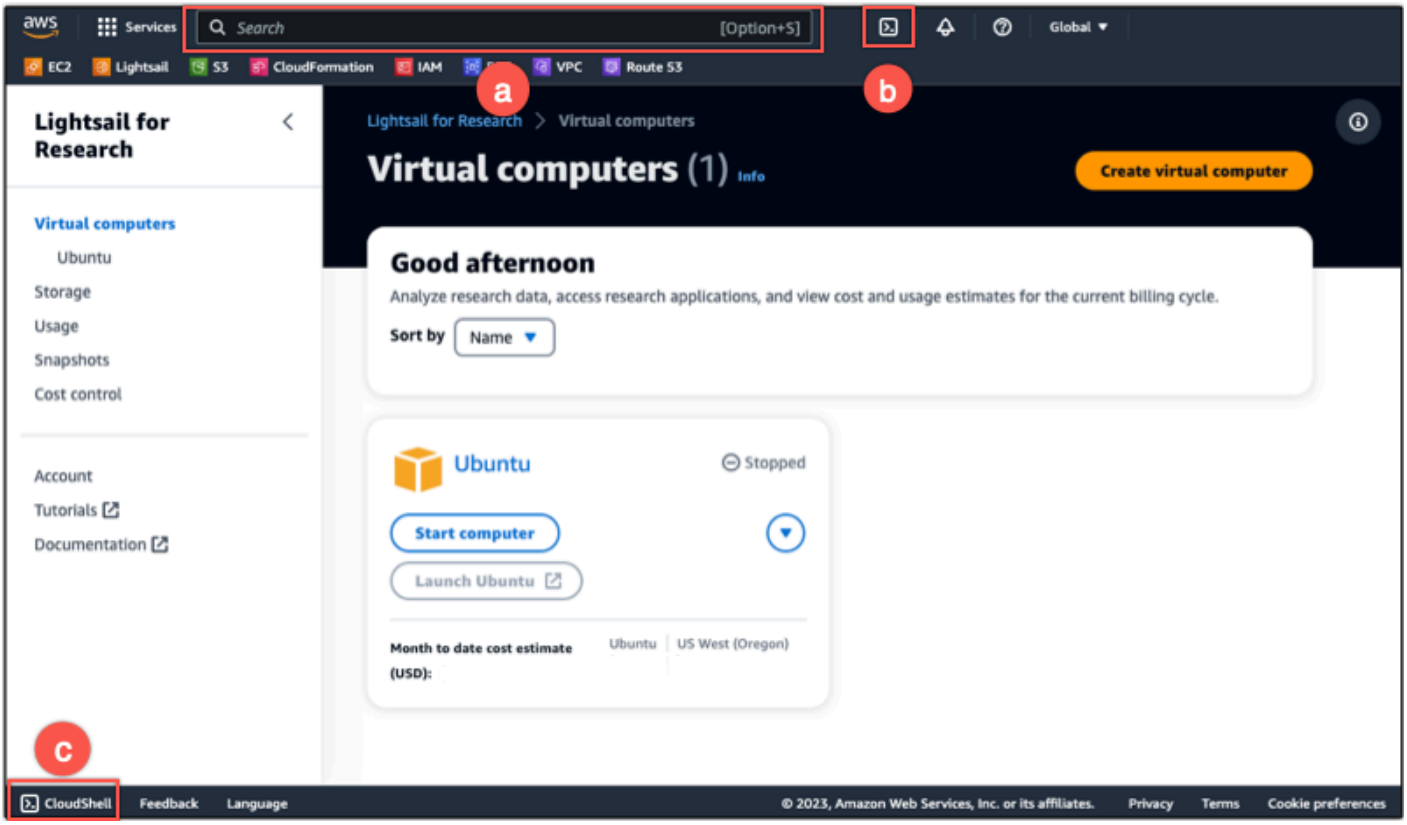
完成以下过程之一，在 Lightsail for Research 中建立与虚拟计算机的 SSH 连接。

使用 Connect 连接到虚拟计算机 AWS CloudShell

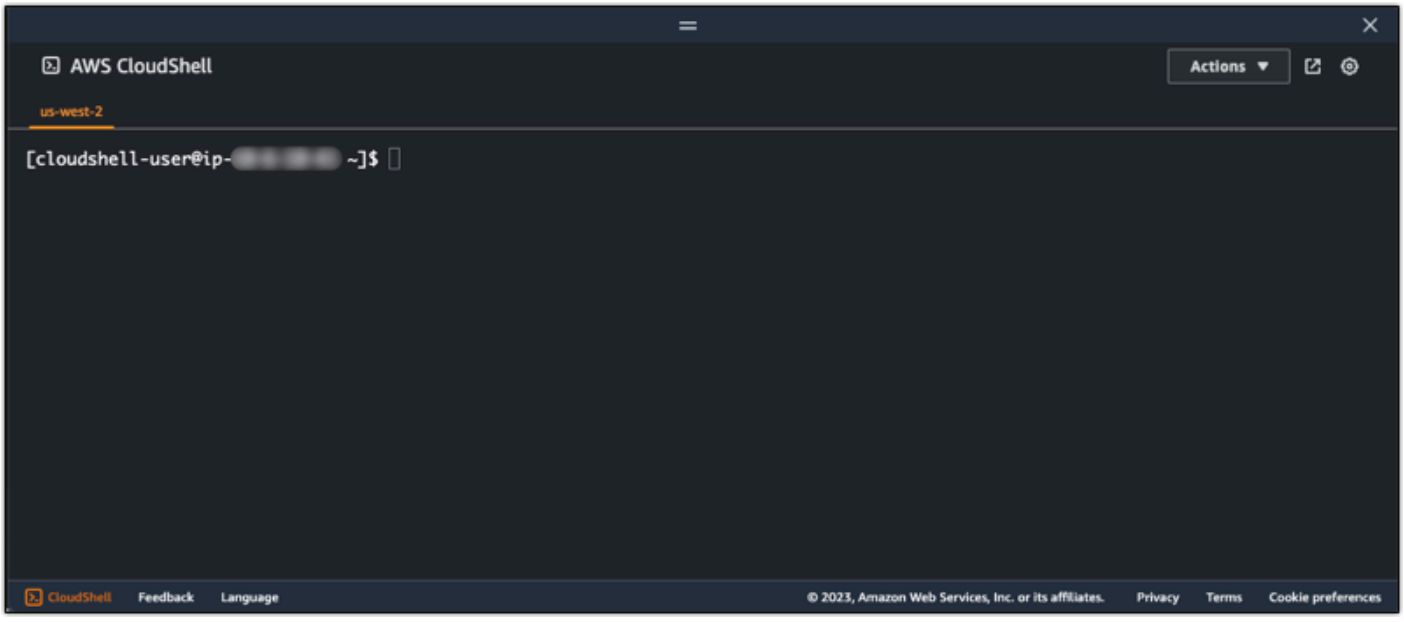
如果您希望以最少的设置连接到虚拟计算机，则此过程适用。 AWS CloudShell 使用基于浏览器、经过预先验证的 shell，您可以直接从中启动该外壳。 AWS Management Console您可以使用首选外壳运行 AWS CLI 命令，例如 Bash PowerShell、或 Z shell。您无需下载或安装命令行工具，即可完成此操作。有关更多信息，请参阅《AWS CloudShell 用户指南》中的开始使用 AWS CloudShell。

> **Important**
>
> 在开始之前，请确保获取要连接的虚拟计算机的 Lightsail 默认密钥对 (DKP)。有关更多信息，请参阅 获取虚拟计算机的密钥对。

1. 在 Lightsail for Research 控制台中，选择以下选项之一启动 CloudShell ：
   a. 在 “搜索” 框中，键入 CloudShell “”，然后选择CloudShell。
   b. 在导航栏上，选择图CloudShell标。
   c. CloudShell在控制台左下角的控制台工具栏上选择。



当系统显示命令提示符时，表示 shell 已经准备就绪，可以进行交互。



2. 选择要使用的预装外壳。要更改默认 shell，请在命令行提示符下输入以下程序名称之一。 Bash是启动时正在运行的默认 shell AWS CloudShell。

Bash

```
bash
```

如果切换到 Bash，则命令提示符处的符号将更新为 $。

PowerShell

```
pwsh
```

如果切换到 PowerShell，则命令提示符处的符号将更新为PS>。

Z shell

```
zsh
```

如果切换到 Z shell，则命令提示符处的符号将更新为 %。

3. 要从 CloudShell 终端窗口连接到虚拟计算机，请参阅在 Linux、Unix 或 macOS 本地计算机上使用 SSH 连接到虚拟计算机。

有关 CloudShell环境中预安装软件的信息，请参阅《AWS CloudShell 用户指南》中的AWS CloudShell 计算环境。

在 Windows 本地计算机上使用 SSH 连接到虚拟计算机

如果您的本地计算机使用 Windows 操作系统，则此过程适用。此过程使用`get-instance` AWS CLI 命令获取您要连接的实例的用户名和公有 IP 地址。有关更多信息，请参阅《AWS CLI 命令参考》中的 get-instance。

> **Important**
>
> 在开始此过程之前，请确保获得要连接的虚拟计算机的 Lightsail 默认密钥对 (DKP)。有关更多信息，请参阅 获取虚拟计算机的密钥对。该过程将 Lightsail DKP 的私钥输出到一个`dkp_rsa`文件中，该文件用于以下命令之一。

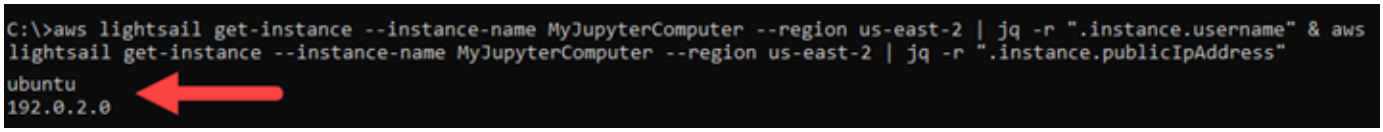
1. 打开 Command Prompt (命令提示符窗口)。
2. 输入以下命令，以显示虚拟计算机的公有 IP 地址和用户名。在命令中，*`region-code`*替换为 AWS 区域 创建虚拟计算机时使用的代码，例如`us-east-2`。将 *`computer-name`* 替换为要连接的虚拟计算机的名称。

```
aws lightsail get-instance --region region-code --instance-name computer-name |
 jq -r ".instance.username" & aws lightsail get-instance --region region-code --
instance-name computer-name | jq -r ".instance.publicIpAddress"
```

示例

```
aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
 | jq -r ".instance.username" & aws lightsail get-instance --region us-east-2 --
instance-name MyJupyterComputer | jq -r ".instance.publicIpAddress"
```

响应将显示虚拟计算机的用户名和公有 IP 地址，如以下示例所示。请记下这些值，因为在此过程的后续步骤中需要这些值。



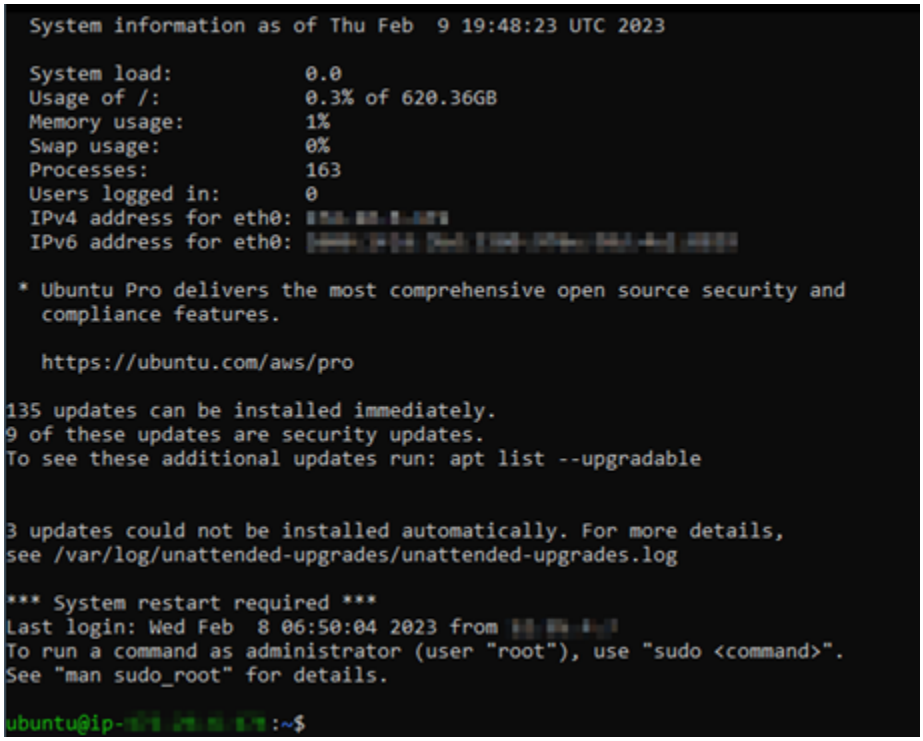
3. 输入以下命令，与您的虚拟计算机建立 SSH 连接。在命令中，将 *user-name* 替换为登录用户名，将 *public-ip-address* 替换为虚拟计算机的公有 IP 地址。

```
ssh -i dkp_rsa user-name@public-ip-address
```

示例

```
ssh -i dkp_rsa ubuntu@192.0.2.0
```

您应该会看到与以下示例类似的响应，该示例显示了在 Lightsail for Research 中与 Ubuntu 虚拟计算机建立的 SSH 连接。



现在，您已成功建立与虚拟计算机的 SSH 连接，请继续阅读下一节以了解其他后续步骤。

在 Linux、Unix 或 macOS 本地计算机上使用 SSH 连接到虚拟计算机

如果您的本地计算机使用的是 Linux、Unix 或 macOS 操作系统，则此过程适用。此过程使用`get-instance` AWS CLI 命令获取您要连接的实例的用户名和公有 IP 地址。有关更多信息，请参阅《AWS CLI 命令参考》中的 get-instance。

> **Important**
>
> 在开始此过程之前，请确保获得要连接的虚拟计算机的 Lightsail 默认密钥对 (DKP)。有关更多信息，请参阅 获取虚拟计算机的密钥对。该过程将 Lightsail DKP 的私钥输出到一个`dkp_rsa`文件中，该文件用于以下命令之一。

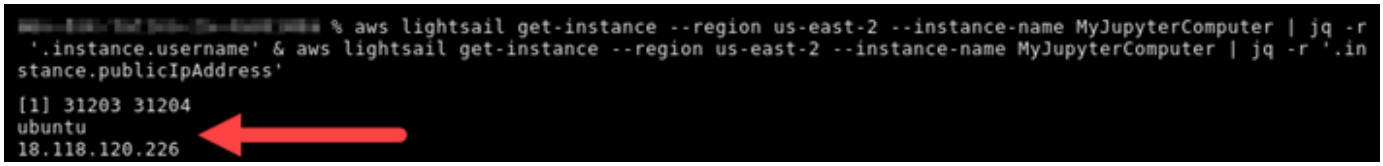
1. 打开终端窗口。
2. 输入以下命令，以显示虚拟计算机的公有 IP 地址和用户名。在命令中，*`region-code`*替换为创建虚拟计算机的 AWS 区域的代码，例如`us-east-2`。将 *`computer-name`* 替换为要连接的虚拟计算机的名称。

```
aws lightsail get-instance --region region-code --instance-name computer-name |
 jq -r '.instance.username' && aws lightsail get-instance --region region-code --
instance-name computer-name | jq -r '.instance.publicIpAddress'
```

示例

```
aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
 | jq -r '.instance.username' && aws lightsail get-instance --region us-east-2 --
instance-name MyJupyterComputer | jq -r '.instance.publicIpAddress'
```

响应将显示虚拟计算机的用户名和公有 IP 地址，如以下示例所示。请记下这些值，因为在此过程的后续步骤中需要这些值。



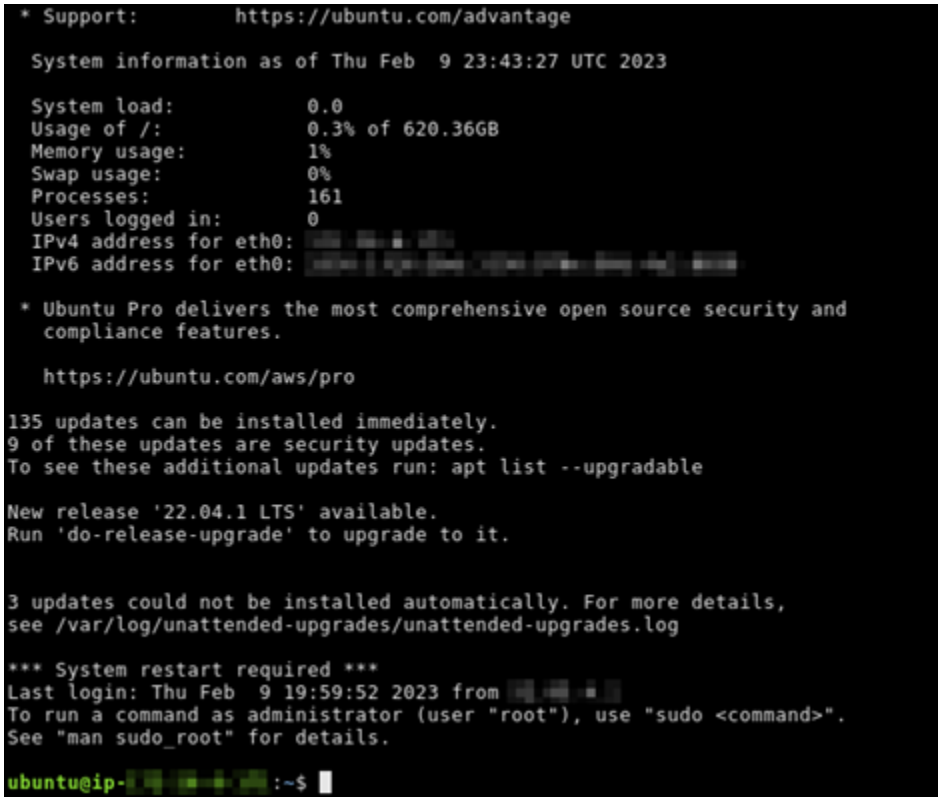
3. 输入以下命令，与您的虚拟计算机建立 SSH 连接。在命令中，将 *user-name* 替换为登录用户名，将 *public-ip-address* 替换为虚拟计算机的公有 IP 地址。

```
ssh -i dkp_rsa user-name@public-ip-address
```

示例

```
ssh -i dkp_rsa ubuntu@192.0.2.0
```

您应该会看到与以下示例类似的响应，该示例显示了在 Lightsail for Research 中与 Ubuntu 虚拟计算机建立的 SSH 连接。



现在，您已成功建立与虚拟计算机的 SSH 连接，请继续阅读下一节以了解其他后续步骤。

继续执行后续步骤

成功与虚拟计算机建立 SSH 连接后，您可以完成以下其他后续步骤：

- 使用 SCP 连接到您的虚拟计算机，以安全地传输文件。有关更多信息，请参阅 使用 Secure Copy 将文件传输到虚拟计算机。

使用 Secure Copy 将文件传输到虚拟计算机

您可以使用安全复制 (SCP) 将文件从本地计算机传输到 Amazon Lightsail for Research 中的虚拟计算机。通过此过程，您可以一次传输多个文件或整个目录。

> **Note**
>
> 您还可以使用 Lightsail for Research 控制台中提供的基于浏览器的 NICE DCV 客户端，与虚拟计算机建立远程显示协议连接。使用 NICE DCV 客户端，您可以快速传输单个文件。有关更多信息，请参阅 访问虚拟计算机的操作系统。

主题

完成先决条件

在开始之前，请满足以下先决条件。

- 在 Lightsail 中创建一台用于研究的虚拟计算机。有关更多信息，请参阅 创建虚拟计算机。
- 确保您要连接的虚拟计算机处于运行状态。另外，记下虚拟计算机的名称和创建虚拟计算机所在的 AWS 区域。您在此过程的稍后部分将会需要此信息。有关更多信息，请参阅 查看虚拟计算机详细信息。
- 下载并安装 AWS Command Line Interface (AWS CLI)。有关更多信息，请参阅《AWS Command Line Interface 用户指南版本 2》中的安装或更新最新版本的 AWS CLI。
- 配置 AWS CLI 以访问您的 AWS 账户。有关更多信息，请参阅《AWS Command Line Interface 用户指南版本 2》中的配置基础知识。
- 下载并安装 jq。它是一个轻型且灵活的命令行 JSON 处理器，用于在以下过程中提取密钥对详细信息。有关下载和安装 jq 的更多信息，请参阅 jq 网站上的下载 jq。
- 确保您要连接的虚拟计算机上的端口 22 已打开。这是 SSH 使用的默认端口。该端口预设情况下打开。但是，如果您将其关闭，则必须先将其重新打开，然后才能继续使用。有关更多信息，请参阅管理虚拟计算机的防火墙端口。
- 为您的虚拟计算机获取 Lightsail 默认密钥对 (DKP)。有关更多信息，请参阅 创建虚拟计算机。

使用 SCP 连接到虚拟计算机

完成以下过程之一，使用 SCP 连接到 Lightsail for Research 中的虚拟计算机。

在 Windows 本地计算机上使用 SCP 连接到虚拟计算机

如果您的本地计算机使用 Windows 操作系统，则适用此过程。此过程使用`get-instance` AWS CLI 命令获取您要连接的实例的用户名和公有 IP 地址。有关更多信息，请参阅《AWS CLI 命令参考》中的 get-instance。

> **Important**
>
> 在开始此过程之前，请确保获得要连接的虚拟计算机的 Lightsail 默认密钥对 (DKP)。有关更多信息，请参阅 获取虚拟计算机的密钥对。该过程将 Lightsail DKP 的私钥输出到一个`dkp_rsa`文件中，该文件用于以下命令之一。

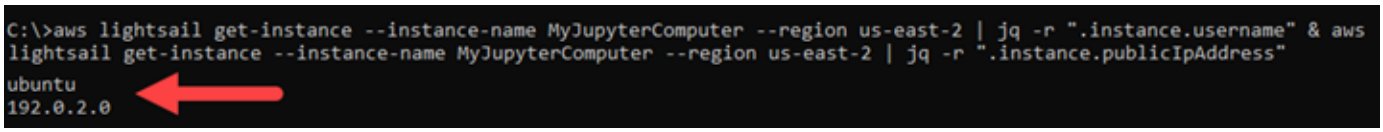
1. 打开 Command Prompt (命令提示符窗口)。
2. 输入以下命令，以显示虚拟计算机的公有 IP 地址和用户名。在命令中，*`region-code`*替换为创建虚拟计算机的 AWS 区域的代码，例如`us-east-2`。将 *`computer-name`* 替换为要连接的虚拟计算机的名称。

   ```
   aws lightsail get-instance --region region-code --instance-name computer-name |
    jq -r ".instance.username" & aws lightsail get-instance --region region-code --
   instance-name computer-name | jq -r ".instance.publicIpAddress"
   ```

   示例

   ```
   aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
    | jq -r ".instance.username" & aws lightsail get-instance --region us-east-2 --
   instance-name MyJupyterComputer | jq -r ".instance.publicIpAddress"
   ```

   响应将显示虚拟计算机的用户名和公有 IP 地址，如以下示例所示。请记下这些值，因为在此过程的后续步骤中需要这些值。

3. 输入以下命令，与您的虚拟计算机建立 SCP 连接，并将文件传输到该虚拟计算机。

   ```
   scp -i dkp_rsa -r "source-folder" user-name@public-ip-address:destination-directory
   ```

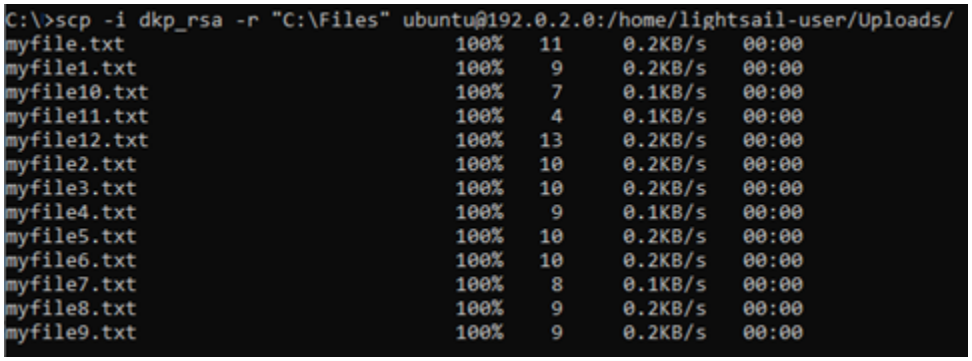
   在该命令中，将：

- *source-folder* 替换为本地计算机上包含要传输的文件的文件夹。
- *user-name* 替换为来自此过程上一步的用户名（例如 ubuntu）。
- *public-ip-address* 替换为来自此过程上一步的虚拟计算机的公有 IP 地址。
- *destination-directory* 替换为您希望从其中复制文件的虚拟计算机上的目录路径。

以下示例将所有文件从本地计算机上的 C:\Files 文件夹复制到远程虚拟计算机上的 /home/lightsail-user/Uploads/ 目录中。

```
scp -i dkp_rsa -r "C:\Files" ubuntu@192.0.2.0:/home/lightsail-user/Uploads/
```

您应看到类似于以下示例的响应。它显示了从源文件夹传输到目标目录的每个文件。现在，您应能够访问虚拟计算机上的这些文件。



在 Linux、Unix 或 macOS 本地计算机上使用 SCP 连接到虚拟计算机

如果您的本地计算机使用 Linux、Unix 或 macOS 操作系统，则适用此过程。此过程使用get-instance AWS CLI 命令获取您要连接的实例的用户名和公有 IP 地址。有关更多信息，请参阅《AWS CLI 命令参考》中的 get-instance。

> **Important**
>
> 在开始此过程之前，请确保获得要连接的虚拟计算机的 Lightsail 默认密钥对 (DKP)。有关更多信息，请参阅 获取虚拟计算机的密钥对。该过程将 Lightsail DKP 的私钥输出到一个dkp_rsa文件中，该文件用于以下命令之一。

1. 打开终端窗口。

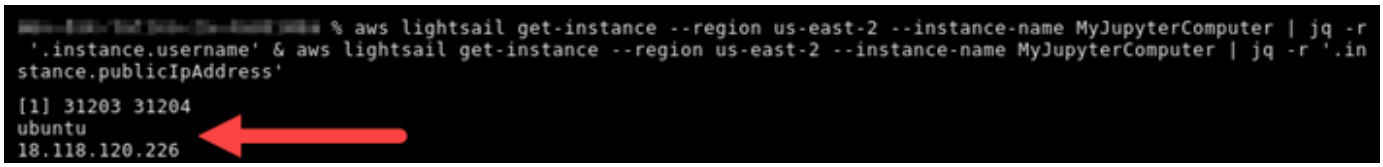
2. 输入以下命令，以显示虚拟计算机的公有 IP 地址和用户名。在命令中，*region-code*替换为创建虚拟计算机的 AWS 区域的代码，例如us-east-2。将 *computer-name* 替换为要连接的虚拟计算机的名称。

```
aws lightsail get-instance --region region-code --instance-name computer-name |
 jq -r '.instance.username' & aws lightsail get-instance --region region-code --
instance-name computer-name | jq -r '.instance.publicIpAddress'
```

示例

```
aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
 | jq -r '.instance.username' & aws lightsail get-instance --region us-east-2 --
instance-name MyJupyterComputer | jq -r '.instance.publicIpAddress'
```

响应将显示虚拟计算机的用户名和公有 IP 地址，如以下示例所示。请记下这些值，因为在此过程的后续步骤中需要这些值。



3. 输入以下命令，与您的虚拟计算机建立 SCP 连接，并将文件传输到该虚拟计算机。

```
scp -i dkp_rsa -r 'source-folder' user-name@public-ip-address:destination-directory
```

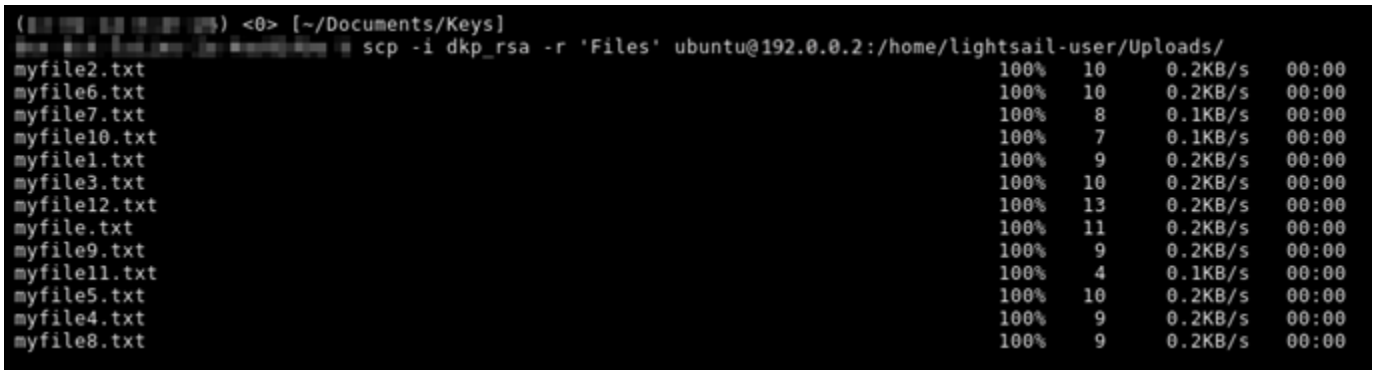
在该命令中，将：

- *source-folder* 替换为本地计算机上包含要传输的文件的文件夹。
- *user-name* 替换为来自此过程上一步的用户名（例如 ubuntu）。
- *public-ip-address* 替换为来自此过程上一步的虚拟计算机的公有 IP 地址。
- *destination-directory* 替换为您希望从其中复制文件的虚拟计算机上的目录路径。

以下示例将所有文件从本地计算机上的 C:\Files 文件夹复制到远程虚拟计算机上的 /home/lightsail-user/Uploads/ 目录中。

```
scp -i dkp_rsa -r 'Files' ubuntu@192.0.2.0:/home/lightsail-user/Uploads/
```

您应看到类似于以下示例的响应。它显示了从源文件夹传输到目标目录的每个文件。现在，您应能够访问虚拟计算机上的这些文件。



删除虚拟计算机

完成以下步骤，在不再需要您的 Lightsail for Research 虚拟计算机时将其删除。一旦删除该虚拟计算机，它将不再产生费用。附加到已删除计算机的资源（例如快照）会继续产生费用，直至您将其删除。

> **Important**
>
> 删除虚拟计算机是一项永久性操作，计算机无法还原。如果以后可能需要数据，请先创建虚拟计算机的快照，然后再删除它。有关更多信息，请参阅创建快照。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择虚拟计算机。
3. 选择要删除的虚拟计算机。
4. 选择操作，然后选择删除虚拟计算机。
5. 在文本块中键入确认。然后，选择删除虚拟计算机。

存储

Amazon Lightsail for Research 提供块级存储卷（磁盘），您可以将这些卷（磁盘）附加到正在运行 Lightsail for Research 的虚拟计算机。可以使用磁盘作为主要存储设备，以获取需要频繁更新和精细更新的数据。例如，如果在 Lightsail for Research 虚拟计算机上运行数据库，则建议选用磁盘作为存储选项。

磁盘就像未格式化的外部块设备，可附加到单个虚拟计算机。卷始终不受计算机运行生命周期的影响。将磁盘附加到计算机后，您可以像使用其他物理硬盘一样使用它。

您可以将多个磁盘附加到一台计算机。您也可以从一台计算机中分离一个磁盘，并把它附加到另一台计算机。

为保留您的数据的备份副本，请创建磁盘的快照。您可以利用该快照创建一个新磁盘，并将其附加到另一台计算机。

主题

创建磁盘

完成以下步骤以为 Lightsail for Research 虚拟计算机创建磁盘。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，请选择存储。
3. 选择创建磁盘。
4. 输入磁盘的名称。有效字符包括字母数字字符、数字、句点、连字符和下划线。

   磁盘名称还必须满足以下要求：

   - 在各个 AWS 区域 内您的 Lightsail for Research 账户中必须唯一。
   - 包含 2–255 个字符。

- 以字母数字字符或数字作为开头和结尾。

5. 为您的磁盘选择一个 AWS 区域。

   该磁盘必须与要附加到的虚拟计算机位于同一区域内。

6. 选择您的磁盘大小（以 GB 为单位）。

7. 有关将磁盘附加到虚拟计算机的信息，请继续阅读附加磁盘部分。

查看磁盘

完成以下步骤，以查看您的 Lightsail for Research 账户中的磁盘及其详细信息。

1. 登录 Lightsail for Research 控制台。

2. 在导航窗格中，请选择存储。

   存储页面提供了您的 Lightsail for Research 账户中磁盘的全面视图。

   页面上会显示以下信息：

   - 名称 - 存储磁盘的名称。
   - 大小 - 磁盘的大小（以 GB 为单位）。
   - AWS 区域 - 您创建的磁盘所在的 AWS 区域。
   - 附加到 - 磁盘所附加到的 Lightsail 计算机。
   - 创建日期 - 磁盘的创建日期。

将磁盘附加到虚拟计算机

完成以下步骤，以在 Lightsail for Research 中将磁盘附加到虚拟计算机。最多可以将 15 个磁盘附加到虚拟计算机。当您使用 Lightsail for Research 控制台将磁盘附加到虚拟计算机时，服务会自动将其格式化并挂载该磁盘。此过程需要几分钟；因此在开始使用磁盘之前，您应该确认磁盘已进入已挂载状态。默认情况下，Lightsail for Research 会将磁盘挂载到 `/home/lightsail-user/<disk-name>` 目录。*<disk-name>* 是您给磁盘的命名。

> **Important**
>
> 在将磁盘附加到虚拟计算机之前，虚拟计算机必须处于正在运行状态。如果在虚拟计算机处于已停止状态时将磁盘附加到该虚拟计算机，则磁盘将被附加但无法挂载。如果磁盘的挂载状态为失败，则必须先分离该磁盘，然后在虚拟计算机处于正在运行状态时重新附加该磁盘。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择虚拟计算机。
3. 选择要附加磁盘的计算机。
4. 选择存储选项卡。
5. 选择挂载磁盘。
6. 选择要附加到计算机的磁盘的名称。
7. 选择附加。

将磁盘与虚拟计算机分离

完成以下步骤，将磁盘与计算器分离。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，请选择存储。
3. 找到要分离的磁盘。在已附加到列下，选择磁盘所附加的计算机名称。
4. 选择停止以停止计算机。必须先停止计算机，然后才能分离磁盘。
5. 确认要停止计算机，然后选择停止计算机。
6. 选择存储选项卡。
7. 选择要分离的磁盘，然后选择分离。
8. 确认要将磁盘与计算机分离，然后选择分离。

删除磁盘

当您不再需要存储磁盘时，可完成以下步骤以将其删除。当磁盘被删除之后，您便不再需要支付其费用。

如果磁盘附加到了计算机，则必须首先将其分离，然后才能删除。有关更多信息，请参阅 将磁盘与虚拟计算机分离。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，请选择存储。
3. 查找并选择要删除的磁盘。
4. 选择删除磁盘。
5. 确认您要删除磁盘。然后选择删除。

快照

快照是数据的时间点副本。您可以创建 Amazon Lightsail for Research 虚拟计算机和存储磁盘的快照，并将其用作创建新计算机或备份数据的基准。

快照包含还原您的计算机所需的所有数据（从拍摄快照的那一刻开始）。在使用快照创建新虚拟计算机时，它首先是作为用于创建快照的原始计算机的精确副本。

由于您的资源可能随时出现故障，因此我们建议您经常创建快照以避免数据永久丢失。

主题

创建快照

完成以下步骤以为 Lightsail for Research 虚拟计算机或磁盘创建快照。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择快照。
3. 完成以下步骤：
   - 在虚拟计算机快照下，找到要创建快照的计算机的名称，然后选择创建快照。
   - 在磁盘快照下，找到要创建快照的磁盘的名称，然后选择创建快照。
4. 输入快照的名称。有效字符包括字母数字字符、数字、句点、连字符和下划线。

   快照名称还必须满足以下要求：

   - 在各个 AWS 区域 内您的 Lightsail for Research 账户中必须唯一。
   - 包含 2–255 个字符。
   - 以字母数字字符或数字作为开头和结尾。
5. 选择创建快照。

查看快照

完成以下步骤，以查看虚拟计算机和磁盘的快照。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择快照。

   快照页面显示您创建的虚拟计算机和磁盘快照。

   存档的快照也位于此页面上。存档的快照是已从您的账户中删除的资源的快照。

使用快照创建虚拟计算机或磁盘

完成以下步骤，以使用快照创建一个新的 Lightsail for Research 虚拟计算机或磁盘。

使用快照创建虚拟计算机时，请使用与原始计算机大小相同或更大的计划。不能使用比原始虚拟计算机更小的计划。

使用快照创建磁盘时，请选择比原始磁盘更大的磁盘大小。不能使用比原始磁盘更小的磁盘。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择快照。
3. 在快照页面上，找到要用于创建新计算机或磁盘的计算机或磁盘快照的名称。选择快照下拉菜单，以查看该资源的可用快照列表。
4. 选择要用于创建虚拟计算机的快照。
5. 选择操作下拉菜单。然后，选择创建虚拟计算机或创建磁盘。

删除快照

完成以下步骤以删除快照。

1. 登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择快照。
3. 在快照页面上，找到要删除的计算机或磁盘快照的名称。选择快照下拉菜单，以查看该资源的可用快照列表。
4. 选择要删除的快照。

5. 选择操作下拉菜单。然后，选择删除快照。
6. 确认快照名称是否正确。然后，选择删除快照。

亚马逊 Lightsail 研究版中的成本和使用量估算

Amazon Lightsail for Research 会为您的 AWS 资源提供成本和使用量估算。在使用 Lightsail 进行研究时，您可以使用这些估算值来计划支出方式、寻找节省成本的机会，并做出明智的决策。

创建虚拟计算机或磁盘时，会显示该资源的成本和使用情况估算。资源创建完毕，并且处于可用或正在运行状态，就会开始跟踪成本和使用情况估算。资源创建后，估算将在 15 分钟内显示在 AWS 管理控制台中。估算中未包括已删除的资源。

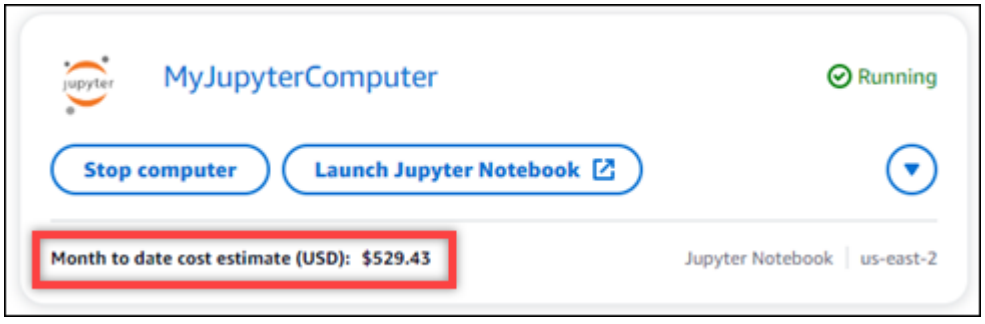
> **Important**
>
> 估算是基于资源使用情况的估算成本。您的实际费用将基于资源的实际使用情况，而不是 Lightsail for Research 控制台中显示的估算值。实际费用显示在您的 AWS Billing 账户对账单上。
>
> 登录 AWS Management Console 并打开 AWS Billing 控制台，网址为 https://console.aws.amazon.com/billing/。

主题

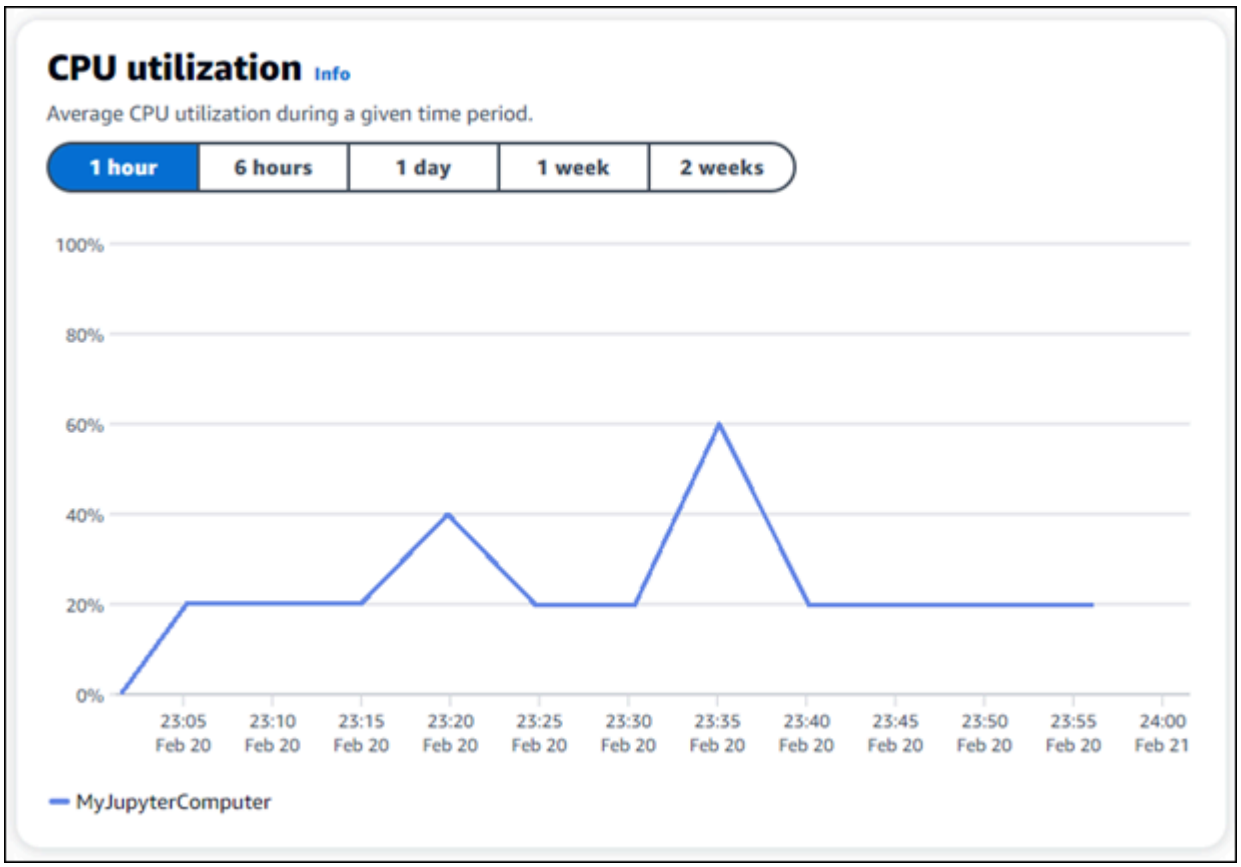
监控成本和使用情况估算。

Lightsail for Research 资源迄今为止的费用和使用量估算值显示在 Lightsail for Research 控制台的以下区域中。

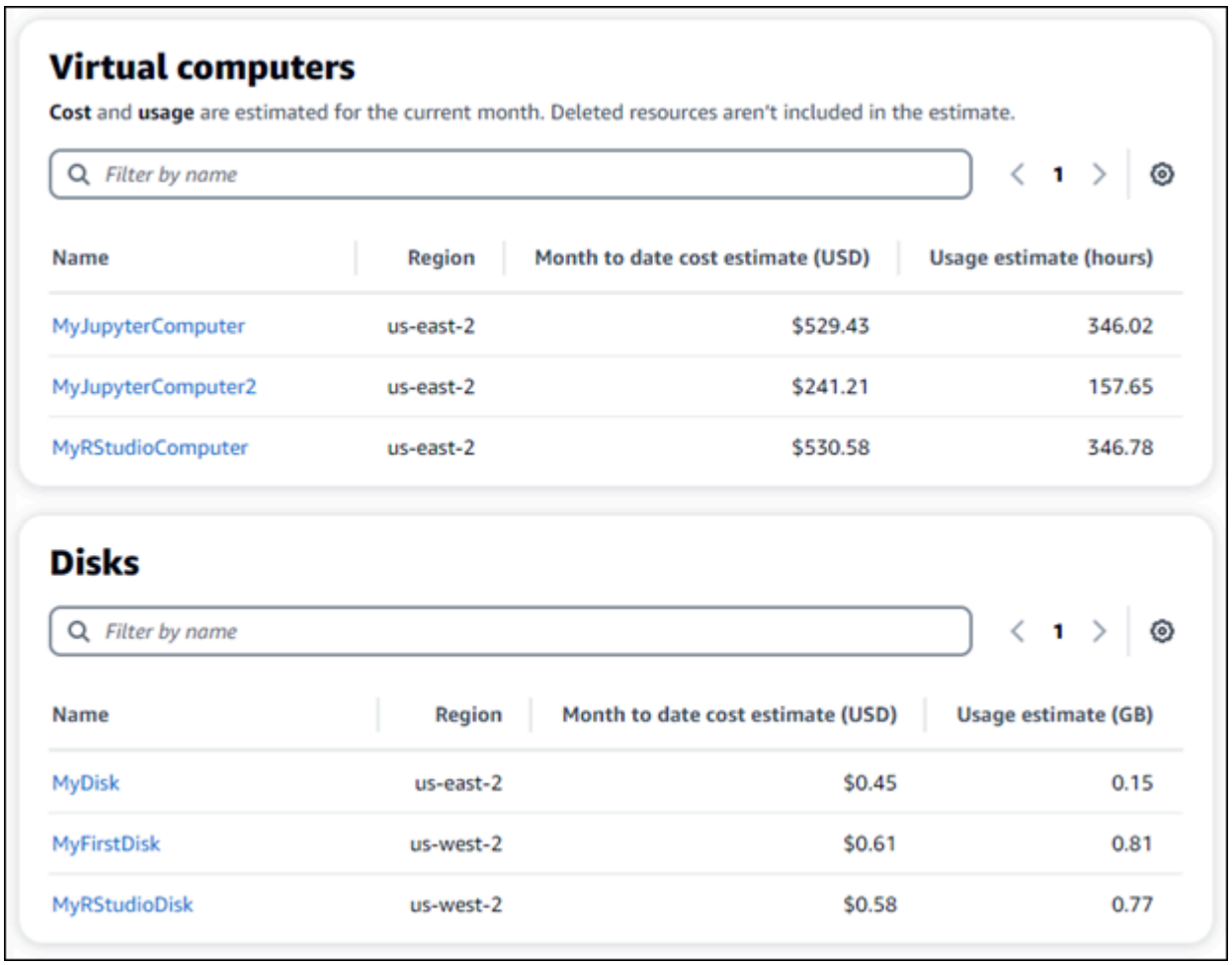
1. 在 Lightsail for Research 控制台的导航窗格中选择 “虚拟计算机”。虚拟计算机的本月至今成本估算列在每台正在运行的虚拟计算机下。



2. 要查看虚拟计算机的 CPU 使用率，请选择虚拟计算机的名称，然后选择控制面板选项卡。



3. 要查看所有 Lightsail for Research 资源的月初至今成本和使用量估算值，请在导航窗格中选择 “使用情况”。


Virtual computers
Cost and usage are estimated for the current month. Deleted resources aren't included in the estimate.
Filter by name
1
Name
Region
Month to date cost estimate (USD)
Usage estimate (hours)
MyJupyterComputer
us-east-2
$529.43
346.02
MyJupyterComputer2
us-east-2
$241.21
157.65
MyRStudioComputer
us-east-2
$530.58
346.78
Disks
Filter by name
1
Name
Region
Month to date cost estimate (USD)
Usage estimate (GB)
MyDisk
us-east-2
$0.45
0.15
MyFirstDisk
us-west-2
$0.61
0.81
MyRStudioDisk
us-west-2
$0.58
0.77

成本控制

成本控制使用您定义的规则来帮助管理 Lightsail for Research 虚拟计算机的使用情况和成本。

您可以创建停止处于空闲状态的虚拟计算机规则，当计算机在给定时间段内达到指定的 CPU 使用率百分比时，该规则会停止正在运行的计算机。例如，当特定计算机的 CPU 使用率在 30 分钟内等于或低于 5% 时，规则就可以自动停止该计算机。这表示计算机处于空闲状态，Lightsail for Research 会停止计算机。虚拟计算机停止运行后，您不再需要支付标准的小时费用。

主题

创建规则

完成以下步骤以为 Lightsail for Research 虚拟计算机创建规则。

> **Note**
>
> 目前唯一支持的规则操作是停止虚拟计算机。CPU 使用率是当前受规则监控的唯一指标，唯一支持的操作是小于或等于。

1. 登录 Lightsail for Research 控制台。
2. 在控制台导航窗格中，选择成本控制。
3. 选择创建规则。
4. 选择要应用规则的资源。
5. 指定规则应运行的 CPU 使用率百分比和时间段。

   例如，您可以指定 5% 和 30 分钟。当计算机的 CPU 使用率在 30 分钟内小于或等于 5% 时，Lightsail for Research 会自动停止该计算机。
6. 选择创建规则。
7. 确认新规则的信息正确无误，然后选择确认。

删除规则

完成以下步骤以为 Lightsail for Research 虚拟计算机删除规则。

1. 登录 Lightsail for Research 控制台。
2. 在控制台导航窗格中，选择成本控制。
3. 选择要删除的规则。
4. 选择删除。
5. 确认您希望删除规则，并选择删除。

标签

借助 Amazon Lightsail for Research，您可以为资源分配标签。每个标签都是一个标记，包含一个密钥和一个可选值，让您能够有效地管理资源。没有值的键被称为“仅包含键的标签”，而带有值的键称为“键值标签”。尽管没有固有类型的标签，但利用标签，您可以根据用途、所有者、环境或其他标准来将资源分类。这在您有许多相同类型的资源时会非常有用。您可以根据分配到特定资源的标签来快速识别该资源。例如，您可以定义一组标签，以帮助跟踪每个资源的项目或优先级。

您可以在 Amazon Lightsail for Research 控制台中标记以下资源：

- 虚拟计算机
- 存储磁盘
- 快照

以下限制适用于标签：

- 每个资源的最大标签数是 50。
- 每个资源的每个标签键都必须是唯一的。每个标签键只能有一个值。
- 最大键长度为 128 个 Unicode 字符（采用 UTF-8 格式）。
- 最大值长度为 256 个 Unicode 字符（采用 UTF-8 格式）。
- 如果在多个服务和资源中使用您的标记方案，请记住，其它服务可能对允许使用的字符有限制。通常允许使用的字符包括：字母、数字、空格以及以下字符：`+ - = . _ : / @`。
- 标签键和值区分大小写。
- 请不要使用 `aws:` 作为键或值的前缀。此前缀是专门预留下来以供 AWS 使用的。

主题

创建标签

完成以下步骤以为 Lightsail for Research 虚拟计算机创建标签。以下步骤与针对 Lightsail for Research 磁盘和快照的步骤类似。

1. 在 Lightsail for Research 控制台登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择虚拟计算机。
3. 选择要为其创建标签的虚拟计算机。
4. 选择标签选项卡。
5. 选择管理标签。
6. 选择添加新标签。
7. 在键字段中输入键名称。例如，项目。
8. （可选）在值字段中输入值名称。例如，博客。
9. 选择保存更改，将密钥保存到您的虚拟计算机。

删除标签

完成以下步骤以为 Lightsail for Research 虚拟计算机删除标签。以下步骤与针对 Lightsail for Research 磁盘和快照的步骤类似。

1. 在 Lightsail for Research 控制台登录 Lightsail for Research 控制台。
2. 在导航窗格中，选择虚拟计算机。
3. 选择要从中删除标签的虚拟计算机。
4. 选择标签选项卡。
5. 选择管理标签。
6. 选择删除以从资源中删除标签。

> **Note**
>
> 如果您只想删除标签的值，请找到该值，然后选择其旁边的 X 图标。

7. 选择保存更改。

用于研究的 Amazon Lightsail 中的安全

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

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

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

本文档可帮助您了解在使用 Lightsail 进行研究时如何应用分担责任模型。以下主题向您展示如何配置 Lightsail for Research 以实现您的安全和合规目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Lightsail for Research 资源。

主题

亚马逊 Lightsail 研究版中的数据保护

分担责任模型 AWS 分担责任模型适用于 Amazon Lightsail for Research 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础设施上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

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

- 对每个账户使用多重身份验证 (MFA)。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-2 版》。

我们强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括你 AWS 服务 使用控制台、API 或 SDK 与 Lightsail for Research 或其他机构 AWS CLI合作时。 AWS 在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

适用于亚马逊 Lightsail 研究版的身份和访问管理 Lightsail

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

> **Note**
>
> 亚马逊 Lightsail 和 Lightsail for Research 共享相同的 IAM 策略参数。对 Lightsail for Research 政策所做的更改也将影响 Lightsail 政策。例如，如果用户有权在 Lightsail for Research 中创建磁盘，则该用户也可以在 Lightsail 中创建磁盘。

主题

受众

你的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于你在 Lightsail for Research 中所做的工作。

服务用户 — 如果您使用 Lightsail for Research 服务完成工作，则您的管理员会为您提供所需的凭据和权限。当你使用更多 Lightsail for Research 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Lightsail for Research 中的某项功能，请参阅。对用于研究的 Amazon Lightsail 身份和访问权限进行故障排除

服务管理员 — 如果你负责公司的 Lightsail for Research 资源，那么你可能拥有使用 Lightsail for Research 的完全访问权限。你的工作是确定你的服务用户应该访问哪些 Lightsail for Research 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。要详细了解贵公司如何将 IAM 与 Lightsail 用于研究的 Lightsail 配合使用，请参阅。亚马逊 Lightsail for Research 如何与 IAM 合作

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 Lightsail for Research 的访问权限。要查看您可以在 IAM 中使用的基于身份的 Lightsail for Research 策略示例，请参阅。亚马逊 Lightsail 研究版基于身份的政策示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅 IAM 用户指南中的签署 AWS API 请求。

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

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

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

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

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。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：

- 联合用户访问 – 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的 为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限 – IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取 – 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，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅《IAM 用户指南》中的 IAM 角色与基于资源的策略有何不同。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 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。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 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分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon EC2 上运行的应用程序 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该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

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概览。

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

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，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。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

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

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。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括

AWS 托管策略和客户托管策略。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。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACL)

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF要了解有关 ACL 的更多信息，请参阅 Amazon Simple Storage Service 开发人员指南 中的访问控制列表（ACL）概览。

其它策略类型

AWS 支持其他不太常见的策略类型。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特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅 IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCP)-SCP 是 JSON 策略，用于指定组织或组织单位 (OU) 的最大权限。 AWS Organizations AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organizations 和 SCP 的更多信息，请参阅 AWS Organizations 用户指南中的 SCP 的工作原理。
- 会话策略 – 会话策略是当您以编程方式为角色或联合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。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

亚马逊 Lightsail for Research 如何与 IAM 合作

在使用 IAM 管理 Lightsail for Research 的访问权限之前，请先了解有哪些 IAM 功能可用于 Lightsail for Research。

你可以在 Amazon Lightsail 研究版中使用的 IAM 功能

IAM 功能	Lightsail 用于研究支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键（特定于服务）	是
ACL	否
ABAC（策略中的标签）	部分
临时凭证	是
主体权限	否
服务角色	否
服务相关角色	否

要全面了解 Lightsail for Research 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

Lightsail for Research 的基于身份的政策

支持基于身份的策略	是

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 策略。

通过使用 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允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Lightsail for Research 基于身份的策略示例

要查看 Lightsail for Research 基于身份的策略示例，请参阅。亚马逊 Lightsail 研究版基于身份的政策示例

Lightsail for Research 内部基于资源的政策

支持基于资源的策略	否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Simple Storage Service（Amazon S3）存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户存取，您可以将整个账户或其它账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，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。

研究版 Lightsail 的政策行动

支持策略操作	是

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

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

在策略中包含操作以授予执行关联操作的权限。

要查看 Lightsail for Research 操作列表，请参阅《服务授权参考》中的 Amazon Lightsail 为研究定义的操作。

Lightsail for Research 中的策略操作在操作前使用以下前缀：

```
lightsail
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "lightsail:action1",
      "lightsail:action2"
         ]
```

要查看 Lightsail for Research 基于身份的策略示例，请参阅。亚马逊 Lightsail 研究版基于身份的政策示例

Lightsail 研究版的政策资源

支持策略资源	是

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

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称 (ARN) 指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符 (*) 指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Lightsail for Research 资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 Amazon Lightsail 为研究定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 A mazon Lightsail 为研究定义的操作。

要查看 Lightsail for Research 基于身份的策略示例，请参阅。亚马逊 Lightsail 研究版基于身份的政策示例

研究版 Lightsail 的政策条件密钥

支持特定于服务的策略条件键	是

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

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅 IAM 用户指南中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Lightsail for Research 条件密钥列表，请参阅《服务授权参考》中的 Amazon Lightsail 研究用条件密钥。要了解您可以使用条件键的操作和资源，请参阅 Amazon Lightsail 为研究定义的操作。

要查看 Lightsail for Research 基于身份的策略示例，请参阅。亚马逊 Lightsail 研究版基于身份的政策示例

Lightsail 中用于研究的 ACL

支持 ACL	否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC 使用 Lightsail 进行研究

支持 ABAC（策略中的标签）	部分

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为 Yes（是）。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为 Partial（部分）。

有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

在 Lightsail 中使用临时证书进行研究

支持临时凭证	是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的 切换到角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Lightsail for Research 的跨服务主体权限

支持转发访问会话（FAS）	否

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Lightsail 研究版的服务职位

支持服务角色	否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 Lightsail for Research 的功能。只有当 Lightsail for Research 提供相关指导时，才能编辑服务角色。

Lightsail for Research 的服务相关角色

支持服务相关角色	否

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的AWS 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

亚马逊 Lightsail 研究版基于身份的政策示例

默认情况下，用户和角色无权创建或修改 Lightsail for Research 资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM policy。

有关 Lightsail for Research 定义的操作和资源类型（包括每种资源类型的 ARN 格式）的详细信息，请参阅《服务授权参考》中的 Amazon Lightsail 用于研究的操作、资源和条件密钥。

主题

- 策略最佳实践
- 使用研究版 Lightsail 控制台
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 Lightsail for Research 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限 – 在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。

- 使用 IAM 策略中的条件进一步限制访问权限 – 您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。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 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言 (JSON) 和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用研究版 Lightsail 控制台

要访问 Amazon Lightsail for Research 控制台，您必须拥有一组最低权限。这些权限必须允许您在中列出和查看有关 Lightsail for Research 资源的详细信息。 AWS 账户如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Lightsail for Research 控制台，还要将 Lightsail for Research *ConsoleAccess* 或*ReadOnly* AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
```

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

对用于研究的 Amazon Lightsail 身份和访问权限进行故障排除

使用以下信息来帮助您诊断和修复在使用 Lightsail for Research 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Lightsail for Research 中执行任何操作
- 我想允许我以外的人访问我的 Lightsail for Research 资源 AWS 账户

我无权在 Lightsail for Research 中执行任何操作

如果您收到错误提示，表明您无权执行某个操作，则您必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 *my-example-widget* 资源的详细信息，但不拥有虚构 lightsail:*GetWidget* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 lightsail:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 lightsail:*GetWidget* 操作访问 *my-example-widget* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我的 Lightsail for Research 资源 AWS 账户

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

要了解更多信息，请参阅以下内容：

- 要了解 Lightsail for Research 是否支持这些功能，请参阅。亚马逊 Lightsail for Research 如何与 IAM 合作
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅 IAM 用户指南中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户存取之间的差别，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。

亚马逊 Lightsail 研究版的合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全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，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规性 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合AWS 规资源 — 此工作簿和指南集合可能适用于您的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

亚马逊 Lightsail 研究版的弹性

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础架构外，Lightsail for Research 还提供多项功能，以帮助支持您的数据弹性和备份需求。有关更多信息，请参阅 快照 和 创建快照。

Amazon Lightsail 研究版中的基础设施安全

作为一项托管服务，Amazon Lightsail for Research 受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Lightsail for Research。客户端必须支持以下内容：

- 传输层安全性协议 (TLS)。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

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

Amazon Lightsail 研究版中的配置和漏洞分析

配置和 IT 控制由您（我们的客户）共同 AWS 负责。有关更多信息，请参阅责任 AWS 共担模型。

Amazon Lightsail 研究版的安全最佳实践

Lightsail for Research 提供了许多安全功能，供您在制定和实施自己的安全策略时考虑。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

为防止与您使用 Lightsail for Research 相关的潜在安全事件，请遵循以下最佳实践：

- 通过对第一个控制台进行身份验证，即可访问 Lightsail for Research 控制台。 AWS Management Console 不要共享您的个人控制台凭证。互联网上的任何人都可以浏览到控制台，但除非他们拥有有效的控制台凭证，否则他们无法登录或启动会话。

《Lightsail for Research 用户指南》的文档历史记录

下表介绍了 Lightsail for Research 的文档版本。

变更	说明	日期
首次发布	《Lightsail for Research 用户指南》的初始版本。	2023 年 2 月 28 日

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