aws

User Guide

Amazon Lightsail for Research

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Lightsail for Research: User Guide

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What is Amazon Lightsail for Research? 1
Pricing 1
Availability 1
Setting up 2
Sign up for AWS 2
Create an IAM user 2
Get started tutorial 4
Step 1: Complete the prerequisites 4
Step 2: Create a virtual computer 4
Step 3: Launch a virtual computer's application 5
Step 4: Connect to your virtual computer 6
Step 5: Add storage to your virtual computer 7
Step 6: Create a snapshot 7
Step 7: Clean up 8
Tutorials 9
Get started with JupyterLab 9
Step 1: Complete the prerequisites 10
Step 2: (Optional) Add storage space 10
Step 3: Upload and download files 10
Step 4: Launch the JupyterLab application 11
Step 5: Read the JupyterLab documentation 15
Step 6: (Optional) Monitor usage and costs 15
Step 7: (Optional) Create a cost control rule 17
Step 8: (Optional) Create a snapshot 18
Step 9: (Optional) Stop or delete your virtual computer 18
Get started with RStudio 19
Step 1: Complete the prerequisites 20
Step 2: (Optional) Add storage space 20
Step 3: Upload and download files 20
Step 4: Launch the RStudio application 21
Step 5: Read the RStudio documentation 25
Step 6: (Optional) Monitor usage and costs 27
Step 7: (Optional) Create a cost control rule 28
Step 8: (Optional) Create a snapshot 29

Step 9: (Optional) Stop or delete your virtual computer ... 29
Virtual computers ... 31
Applications and hardware plans ... 31
Applications ... 32
Plans ... 33
Create a virtual computer ... 34
View virtual computer details ... 35
Launch a virtual computer's application ... 36
Access a virtual computer's operating system ... 36
Manage ports ... 37
Protocols ... 38
Ports ... 38
Why open and close ports ... 39
Complete the prerequisites ... 39
Get port states for a virtual computer ... 40
Open ports for a virtual computer ... 41
Close ports for a virtual computer ... 42
Continue to the next steps ... 43
Get a key pair for a virtual computer ... 44
Complete the prerequisites ... 45
Get a key pair for a virtual computer ... 45
Continue to the next steps ... 49
Connect to a virtual computer using SSH ... 50
Complete the prerequisites ... 50
Connect to a virtual computer using SSH ... 51
Continue to the next steps ... 57
Transfer files to a virtual computer using SCP ... 57
Complete the prerequisites ... 58
Connect to a virtual computer using SCP ... 59
Delete a virtual computer ... 63
Storage ... 64
Create a disk ... 64
View disks ... 65
Attach a disk to a virtual computer ... 65
Detach a disk from a virtual computer ... 66
Delete a disk ... 67

Snapshots 68
Create snapshot 68
View snapshots 69
Create virtual computer or disk from snapshot 69
Delete snapshot 70
Cost and usage 71
Monitor cost and usage estimates. 71
Cost control 74
Create a rule 74
Delete a rule 75
Tags 76
Create a tag 77
Delete a tag 77
Security 78
Data protection 79
Identity and Access Management 80
Audience 80
Authenticating with identities 81
Managing access using policies 84
How Amazon Lightsail for Research works with IAM 87
Identity-based policy examples 94
Troubleshooting 97
Compliance validation 98
Resilience 99
Infrastructure security 99
Configuration and vulnerability analysis 100
Security best practices 100
Document history 101

What is Amazon Lightsail for Research?

With Amazon Lightsail for Research, academics and researchers can create powerful virtual computers in the Amazon Web Services (AWS) Cloud. These virtual computers come with pre-installed research applications, such as RStudio and Scilab.

With Lightsail for Research, you can upload data directly from a web browser to begin your work. You can create and delete your virtual computers at any time, which gives you on-demand access to powerful computing resources.

You pay only for as long as you need the virtual computer. Lightsail for Research offers budgeting controls that can automatically stop your computer when it reaches a preconfigured cost limit, so you don't have to worry about overage charges.

Everything you do in the Lightsail for Research console is backed by a publicly available API. Learn how to install and use the AWS CLI and API for Amazon Lightsail.

Pricing

With Lightsail for Research, you pay only for the resources you create and use. For more information, see Lightsail for Research pricing.

Availability

Lightsail for Research is available in the same AWS Regions as Amazon Lightsail, with the exception of the US East (N. Virginia) Region. Lightsail for Research also uses the same endpoints as Lightsail. To view the currently supported AWS Regions and endpoints for Lightsail, see Lightsail Endpoints and Quotas in the *AWS General Reference*.

Setting up Amazon Lightsail for Research

If you're a new AWS customer, complete the setup prerequisites that are listed on this page before you start using Amazon Lightsail for Research. For these setup procedures, you use the AWS Identity and Access Management (IAM) service. For complete information about IAM, see the IAM User Guide.

Topics

- Sign up for AWS
- Create an IAM user

Sign up for AWS

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform tasks that require root user access.

Create an IAM user

To create an administrator user, choose one of the following options.

Choose one way to manage your administrator	To	By	You can also
In IAM Identity Center (Recommended)	Use short-term credentials to access AWS. This aligns with the security best practices. For information about best practices, see Security best practices in IAM in the *IAM User Guide*.	Following the instructions in Getting started in the *AWS IAM Identity Center User Guide*.	Configure programmatic access by Configuring the AWS CLI to use AWS IAM Identity Center in the *AWS Command Line Interface User Guide*.
In IAM (Not recommended)	Use long-term credentials to access AWS.	Following the instructions in Creating your first IAM admin user and user group in the *IAM User Guide*.	Configure programmatic access by Managing access keys for IAM users in the *IAM User Guide*.

Tutorial: Get started with Lightsail for Research virtual computers

Use this tutorial to get started with Amazon Lightsail for Research virtual computers. You'll learn how to create, connect to, and use a virtual computer. In Lightsail for Research, a virtual computer is a research workstation that you create and manage in the AWS Cloud. Virtual computers are based on Lightsail instances with the Ubuntu operating system. On your virtual computer, you can preconfigure a research application like JupyterLab, RStudio, Scilab, and more.

The virtual computer that you create in this tutorial will incur usage fees from the time that you create the virtual computer until you delete it. Deletion is the final step of this tutorial. For more information about pricing, see Lightsail for Research pricing.

Topics

- Step 1: Complete the prerequisites
- Step 2: Create a virtual computer
- Step 3: Launch a virtual computer's application
- Step 4: Connect to your virtual computer
- Step 5: Add storage to your virtual computer
- Step 6: Create a snapshot
- Step 7: Clean up

Step 1: Complete the prerequisites

If you're a new AWS customer, complete the setup prerequisites before you start using Amazon Lightsail for Research. For more information, see Setting up Amazon Lightsail for Research.

Step 2: Create a virtual computer

You can create a virtual computer by using the Lightsail for Research console as described in the following procedure. This tutorial is intended to help you quickly launch your first virtual computer. We also recommend exploring the available applications and hardware plans. For more information, see Applications and hardware plans and Create a virtual computer.

1. Sign in to the Lightsail for Research console.

2. On the home page, choose **Create virtual computer**.
3. Select an AWS Region for your virtual computer.

   Choose a Region that is closest to your physical location for improved latency.
4. Choose an application, also known as a blueprint in the Lightsail API.

   The application you choose is installed and configured on your virtual computer when you create it.
5. Choose a hardware plan, also known as a bundle in the Lightsail API.

   Hardware plans offer different amounts of processing power including vCPU cores, memory, storage, and monthly data transfer. Lightsail for Research offers standard plans and GPU plans for virtual computers. Choose a standard plan when the computational requirement of your work is low. Choose a GPU plan when that requirement is high, such as when running machine learning models or other computationally intensive tasks.
6. Enter a name for your virtual computer.
7. Choose **Create virtual computer** in the **Summary** panel.

After your new virtual computer is up and running, continue to the next step of this tutorial to learn how to launch the computer's application.

Step 3: Launch a virtual computer's application

After you create a virtual computer and it's in a *Running* state, you can launch a virtual session in your web browser. With the session, you can interact with and manage the application that's installed on your virtual computer.

1. Choose **Virtual computers** in the navigation pane of the Lightsail for Research console.
2. Locate the name of the virtual computer that you created in **Step 1**, and choose **Launch application**. For example, **Launch JupyterLab**. An application session opens in a new web browser window.

   > **Important**
   >
   > If your web browser has a pop-up blocker installed, you might need to allow pop-ups from the **aws.amazon.com** domain before opening your session.

To learn how to connect to your virtual computer, continue to the next step of this tutorial.

Step 4: Connect to your virtual computer

You can connect to your virtual computer using the following methods:

- Use the browser-based NICE DCV client available in the Lightsail for Research console. With NICE DCV, you can use a graphical user interface (GUI) to interact with your research application and your virtual computer's operating system.
- Use a secure shell (SSH) client such as OpenSSH, PuTTY, or Windows Subsystem for Linux to access your virtual computer's command line interface. With an SSH client, you can edit scripts and configuration files.
- Use Secure Copy (SCP) to securely transfer files between your local computer and your virtual computer. With SCP, you can start your work locally and continue it on your virtual computer. You can also download files from your virtual computer to copy your work to your local computer.

> **Note**
>
> You can also access your virtual computer's command line interface and transfer files by using the browser-based NICE DCV client.

You must provide your virtual computer's key pair to connect to it using SSH or to transfer files using SCP. A key pair is a set of security credentials that you use to prove your identity when connecting to a Lightsail for Research virtual computer. A key pair consists of a public key and a private key.

For more information about connecting to your virtual computer, see the following documentation:

- Establish a remote display protocol connection:
  - Launch a virtual computer's application
  - Access a virtual computer's operating system
- Establish an SSH connection or transfer files using SCP:
  - Get a key pair for a virtual computer
  - Connect to a virtual computer using Secure Shell

- Transfer files to a virtual computer using Secure Copy

To learn about storage for your virtual computer, continue to the next step of this tutorial.

Step 5: Add storage to your virtual computer

Lightsail for Research provides block-level storage volumes (disks) that you can attach to a virtual computer. Even though your virtual computer comes with a system disk, you can attach additional disks to your virtual computer as your storage needs change. You can also detach a disk from a virtual computer and attach it to another virtual computer.

When you attach a disk to your virtual computer using the console, Lightsail for Research automatically formats and mounts the disk in your operating system. This process takes a few minutes, so you should confirm that the disk is in *Mounted* status before you start using it.

For more information about creating, attaching, and managing a disk, see the following documentation:

- Create a disk
- View disks
- Attach a disk to a virtual computer
- Detach a disk from a virtual computer
- Delete a disk

To learn about backing up your virtual computer, continue to the next step of this tutorial.

Step 6: Create a snapshot

Snapshots are a point-in-time copy of your data. You can create snapshots of your virtual computers and use them as baselines to create new computers or for data backup. A snapshot contains all of the data that's needed to restore your computer (from the moment when the snapshot was taken).

For more information about creating and managing snapshots, see the following documentation:

- Create a snapshot

- View snapshots
- Create a virtual computer or disk from a snapshot
- Delete a snapshot

To learn about cleaning up your virtual computer resources, continue to the next step of this tutorial.

Step 7: Clean up

After you're done with the virtual computer that you created for this tutorial, you can delete it. This stops incurring charges for the virtual computer if you don't need it.

Deleting a virtual computer doesn't delete its associated snapshots or attached disks. If you created snapshots and disks, you should delete those manually to stop incurring charges for them.

To save your virtual computer for later, but to avoid incurring charges at standard hourly prices, you can stop the virtual computer instead of deleting it. Then you can start it again later. For more information, see View virtual computer details. For more information about pricing, see Lightsail for Research pricing.

> **Important**
>
> Deleting a Lightsail for Research resource is a permanent action. The deleted data cannot be recovered. If you might need the data later, create a snapshot of your virtual computer before you delete it. For more information, see Create a snapshot.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane.
3. Choose the virtual computer to delete.
4. Choose **Actions**, then choose **Delete virtual computer**.
5. Type **confirm** in the text block. Then, choose **Delete virtual computer.**

Get started tutorials for Amazon Lightsail for Research

The following tutorials provide additional information about how to get started with specific applications that are available in Lightsail for Research.

Topics

- Get started with JupyterLab
- Get started with RStudio

> **Note**
>
> An in-depth tutorial for getting started with Lightsail for Research and RStudio is published to the AWS Public Sector Blog. For more information, see Getting started with Amazon Lightsail for Research: A tutorial using RStudio.

Get started with JupyterLab

In this tutorial, we show you how to get started with managing and using your JupyterLab virtual computer in Amazon Lightsail for Research.

Topics

- Step 1: Complete the prerequisites
- Step 2: (Optional) Add storage space
- Step 3: Upload and download files
- Step 4: Launch the JupyterLab application
- Step 5: Read the JupyterLab documentation
- Step 6: (Optional) Monitor usage and costs
- Step 7: (Optional) Create a cost control rule
- Step 8: (Optional) Create a snapshot
- Step 9: (Optional) Stop or delete your virtual computer

Step 1: Complete the prerequisites

Create a virtual computer using the JupyterLab application if you haven't already. For more information, see Create a virtual computer.

After your new virtual computer is up and running, continue to the launch the JupyterLab application section of this tutorial.

Step 2: (Optional) Add storage space

Your virtual computer comes with a system disk. However, as your storage needs change, you can attach additional disks to your virtual computer to increase its storage space.

You can also store your working files to an attached disk. Then you can detach the disk and attach it to a different virtual computer to quickly move your files from one computer to another.

Alternatively, you can create a snapshot of an attached disk that has your working files, and then create a duplicate disk from the snapshot. Then you can then attach the new duplicate disk to another computer to duplicate your work across different virtual computers. For more information, see Create a disk and Attach a disk to a virtual computer.

> **Note**
>
> When you attach a disk to your virtual computer using the console, Lightsail for Research automatically formats and mounts the disk. This process takes a few minutes, so you should confirm that the disk has reached a **Mounted** mounting status before you start using it. By default, Lightsail for Research mounts disks to the `/home/lightsail-user/<disk-name>` directory. `<disk-name>` is the name that you gave your disk.

Step 3: Upload and download files

You can upload files to your JupyterLab virtual computer, and download files from it. To do so, you must complete the following steps:

1. Obtain a key pair from Amazon Lightsail. For more information, see Get a key pair for a virtual computer.

2. After you have the key pair, you can use it to establish a connection using the Secure Copy (SCP) utility. SCP lets you upload and download files using Command Prompt or Terminal. For more information, see Transfer files to a virtual computer using Secure Copy.
3. (Optional) You can also use the key pair to connect to your virtual computer with SSH. For more information, see Connect to a virtual computer using Secure Shell.

> **Note**
>
> You can also access your virtual computer's command line interface and transfer files by using the browser-based NICE DCV client. NICE DCV is available in the Lightsail for Research console. For more information, see Launch a virtual computer's application and Access a virtual computer's operating system.

To manage your project files in an attached storage disk, make sure to upload them to the correct mount directory for the attached disk. When you attach a disk to your virtual computer using the console, Lightsail for Research automatically formats and mounts the disk to the `/home/lightsail-user/<disk-name>` directory. *`<disk-name>`* is the name that you gave your disk.

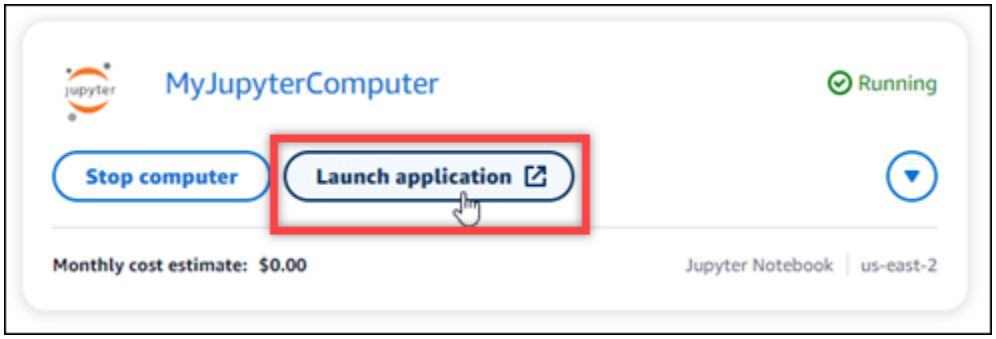
Step 4: Launch the JupyterLab application

Complete the following procedure to launch the JupyterLab application on your new virtual computer.

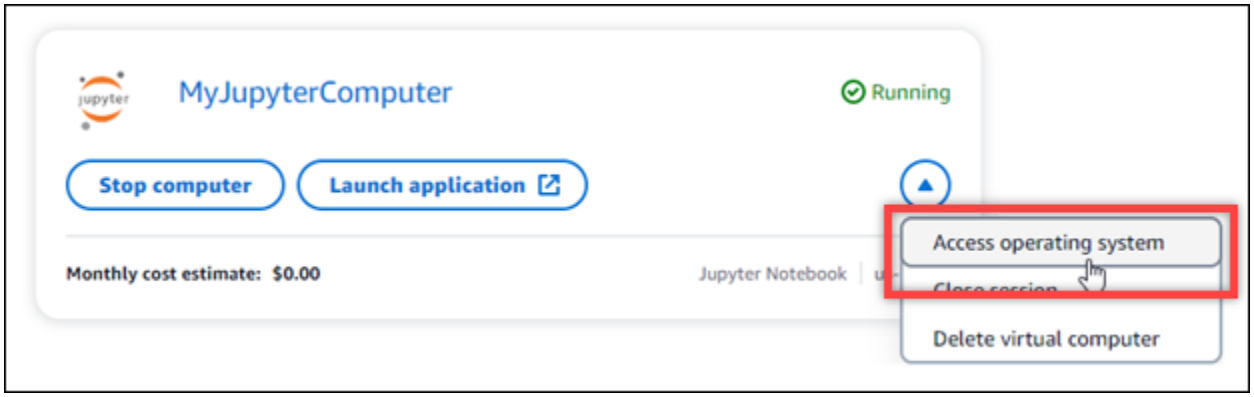
> **Important**
>
> Don't update the operating system or the JupyterLab application even if you are prompted to do so. Instead, choose the option to close or ignore those prompts. Furthermore, don't modify any of the files that are in the **/home/lightsail-admin/** directory. These actions might render the virtual computer unusable.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane to view the virtual computers that are available in your account.
3. In the **Virtual computers** page, find your virtual computer and choose one of the following options to connect to it:

a. (Recommended) Choose **Launch application** to launch the JupyterLab application in focused mode. If you haven't connected to your virtual computer recently, you might have to wait a few minutes while Lightsail for Research prepares your session.



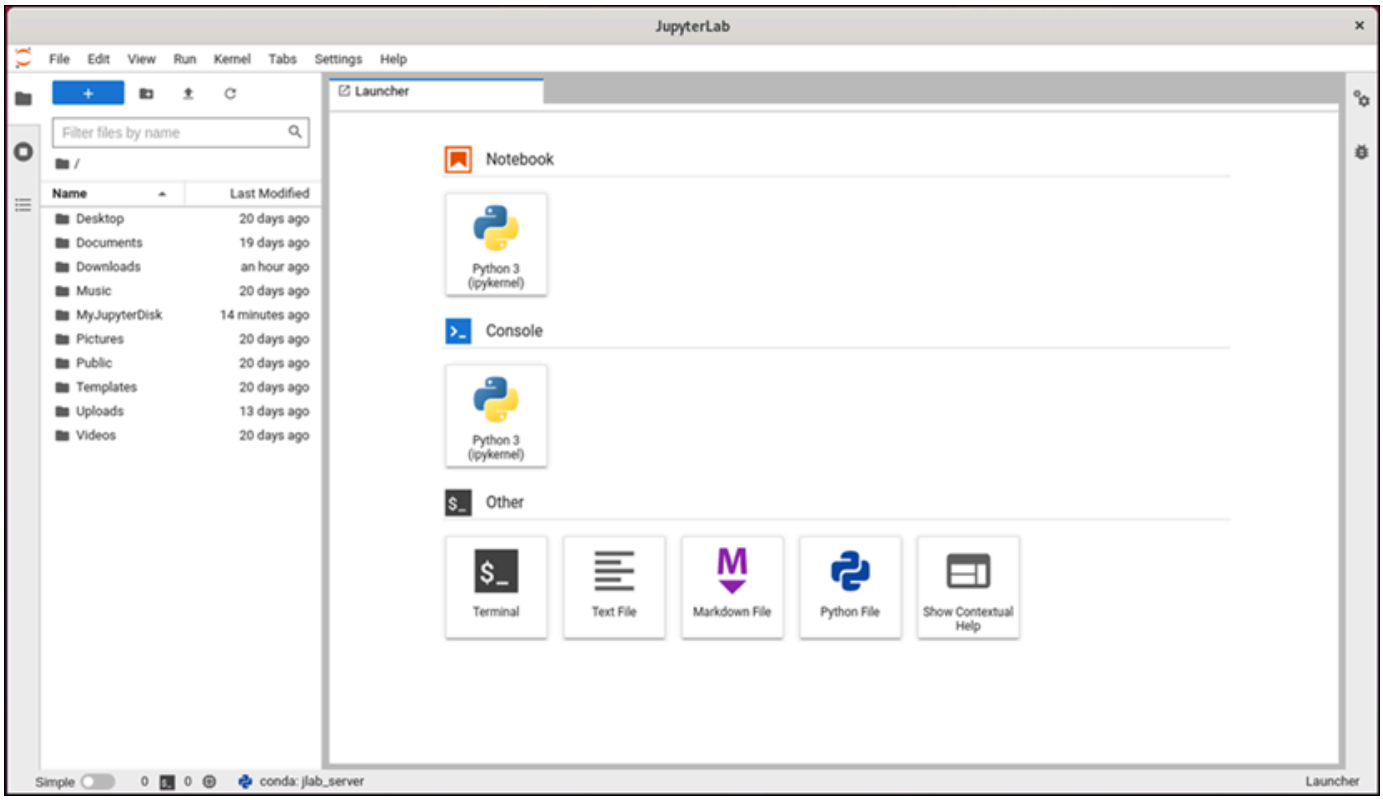
b. Choose the dropdown menu for the computer, and then choose **Access operating system** to access your virtual computer's desktop.



Lightsail for Research runs a few commands to initiate the remote display protocol connection. After a few moments, a new browser tab window opens with a virtual desktop connection established to your virtual computer. If you chose the **Launch application** option, continue to the next step of this procedure to open a file in the JupyterLab application. If you chose the **Access operating system** option, you can open other applications through the Ubuntu desktop.

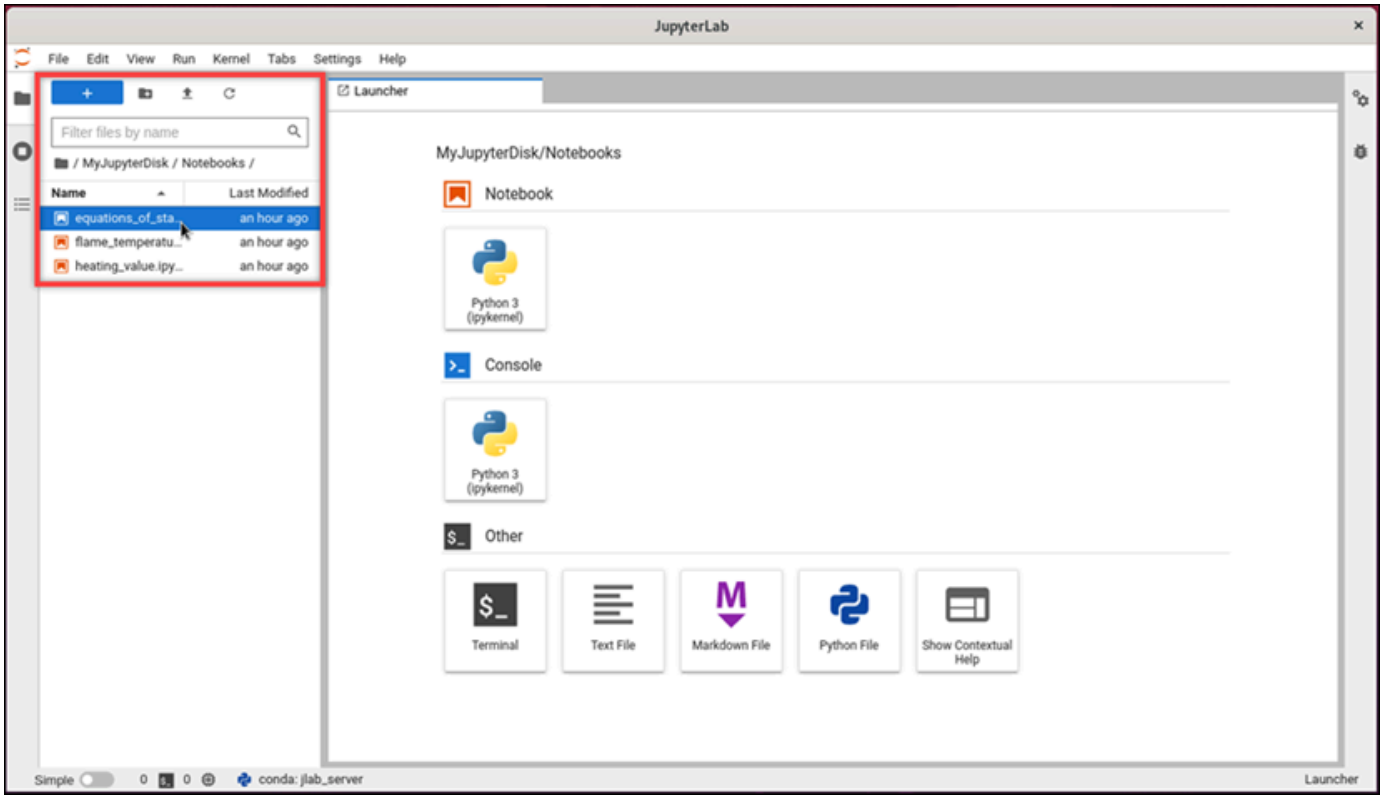
> **Note**
>
> Your browser might prompt you to authorize sharing of your clipboard. Allowing this lets you copy and paste between your local computer and your virtual computer. Ubuntu might also prompt you for an initial setup. Follow the prompts until you complete the setup and can use the operating system.

4. The JupyterLab application opens. In the launcher menu, you can create a new notebook, launch the console, launch the terminal, and create various files.

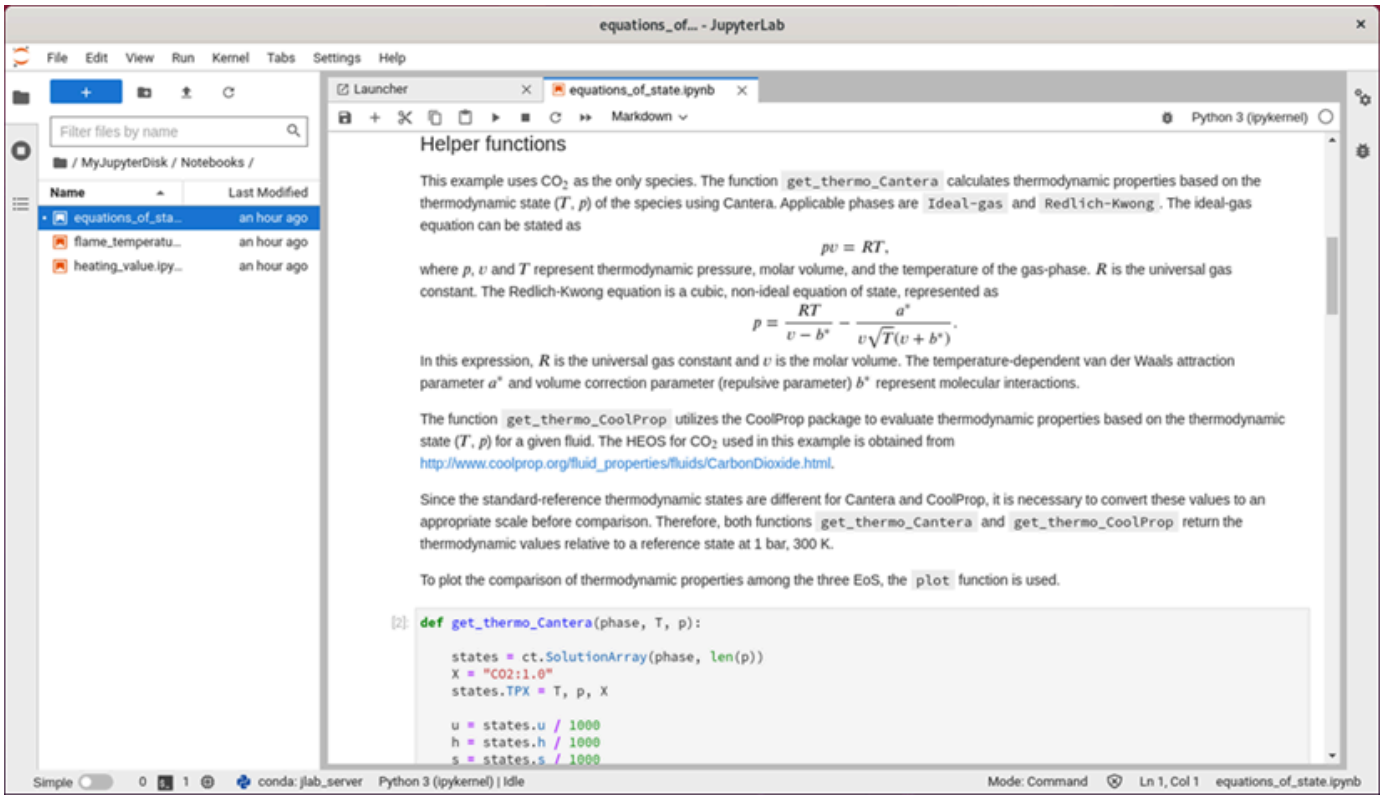


5. To open a file in JupyterLab, in the **File Browser** pane, choose the directory or folder where your project files are stored. Then choose the file to open.

   If you uploaded your project files to an attached disk, look for the directory where the disk is mounted. By default, Lightsail for Research mounts disks to the `/home/lightsail-user/<disk-name>` directory. *`<disk-name>`* is the name you gave your disk. In the following example, the `MyJupyterDisk` directory represents the mounted disk, and the `Notebooks` subdirectory contains our Jupyter notebook files.



In the following example, we have opened the `equations_of_state.ipynb` Jupyter notebook file.



For information about how to get started, continue to the Step 5: Read the JupyterLab documentation section of this tutorial.

Step 5: Read the JupyterLab documentation

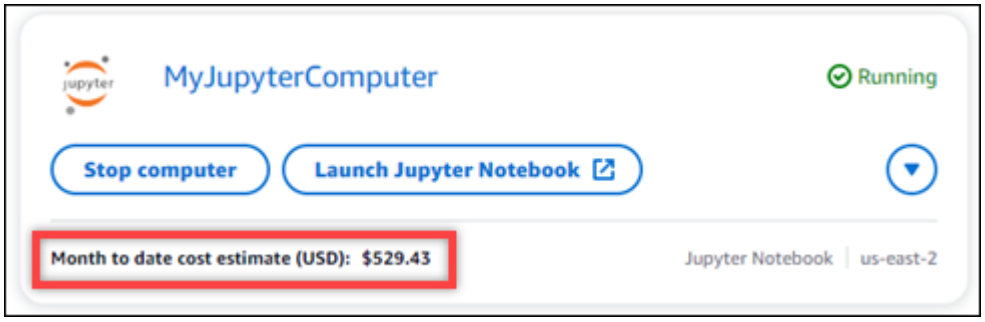
If you're not familiar with JupyterLab, we recommend that you read their official documentation. The following JupyterLab online resources are available:

- JupyterLab Documentation
- Jupyter Discourse Forum
- JupyterLab on StackOverflow
- JupyterLab on GitHub

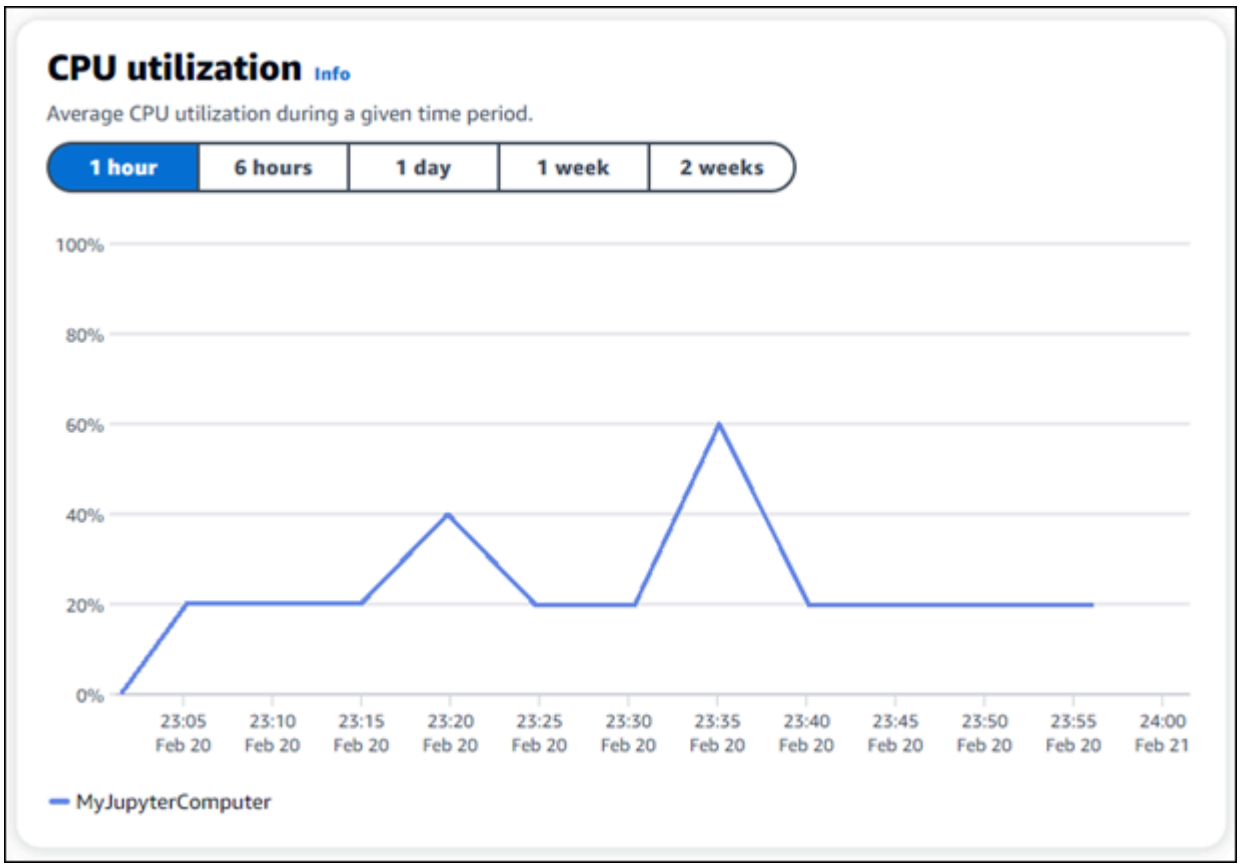
Step 6: (Optional) Monitor usage and costs

Month to date cost and usage estimates for your Lightsail for Research resources are displayed in the following areas of the Lightsail for Research console.

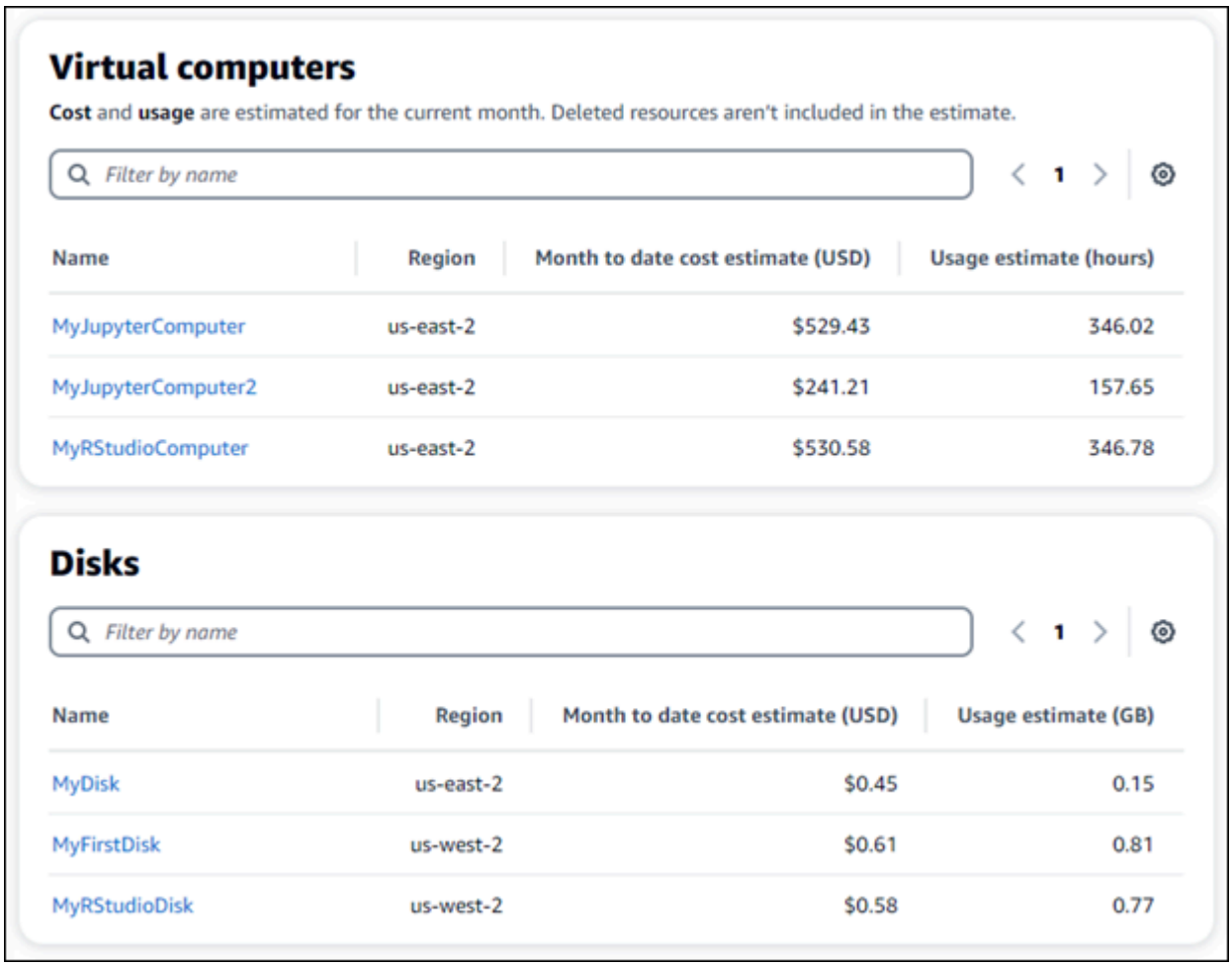
1. Choose **Virtual computers** in the navigation pane of the Lightsail for Research console. The month to date cost estimate for your virtual computers is listed under each running virtual computer.



2. To view the CPU utilization for a virtual computer, choose the name of the virtual computer, and then choose the **Dashboard** tab.



3. To view the month to date cost and usage estimates for all of your Lightsail for Research resources, choose **Usage** in the navigation pane.



Step 7: (Optional) Create a cost control rule

Manage the usage and cost of your virtual computers by creating cost control rules. You can create a **Stop virtual computer on idle** rule that stops a running computer when it reaches a specified percentage of its CPU utilization during a given period. For example, a rule can automatically stop a specific computer when its CPU utilization is equal to or less than 5% during a 30-minute period. This might mean that the computer is idle, and Lightsail for Research stops the computer so that you don't incur charges for an idle resource.

> **Important**
>
> Before you create a rule to stop your virtual computer on idle, we recommend monitoring its CPU utilization for a few days. Take note of the CPU utilization while your virtual computer is under different loads. For example, when it's compiling code, processing an operation, and idling. This will help you determine an accurate threshold for the rule.

For more information, see the Step 6: (Optional) Monitor usage and costs section of this tutorial.

If you create a rule with a CPU utilization threshold that's higher than your workload, the rule can consecutively stop your virtual computer. For example, if you start your virtual computer immediately after a rule stops it, the rule reactivates and the computer stops again.

Detailed instructions for creating, and managing cost control rules can be found in the following guides:

- Cost control
- Create a rule
- Delete a rule

Step 8: (Optional) Create a snapshot

Snapshots are a point-in-time copy of your data. You can create snapshots of your virtual computers and use them as baselines to create new computers or for data backup. A snapshot contains all of the data that's needed to restore your computer (from the moment when the snapshot was taken).

Detailed instructions for creating, and managing snapshots can be found in the following guides:

- Create a snapshot
- View snapshots
- Create a virtual computer or disk from a snapshot
- Delete a snapshot

Step 9: (Optional) Stop or delete your virtual computer

After you're done with the virtual computer that you created for this tutorial, you can delete it. This stops incurring charges for the virtual computer if you don't need it.

Deleting a virtual computer doesn't delete its associated snapshots or attached disks. If you created snapshots and disks, you should delete those manually to stop incurring charges for them.

To save your virtual computer for later, but to avoid incurring charges at standard hourly prices, you can stop the virtual computer instead of deleting it. Then you can start it again later. For more information, see View virtual computer details. For more information about pricing, see Lightsail for Research pricing.

> **Important**
>
> Deleting a Lightsail for Research resource is a permanent action. The deleted data cannot be recovered. If you might need the data later, create a snapshot of your virtual computer before you delete it. For more information, see Create a snapshot.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane.
3. Choose the virtual computer to delete.
4. Choose **Actions**, then choose **Delete virtual computer**.
5. Type **confirm** in the text block. Then, choose **Delete virtual computer.**

Get started with RStudio

In this tutorial, we show you how to get started with managing and using your RStudio virtual computer in Amazon Lightsail for Research.

> **Note**
>
> An in-depth tutorial for getting started with Lightsail for Research and RStudio is published to the AWS Public Sector Blog. For more information, see Getting started with Amazon Lightsail for Research: A tutorial using RStudio.

Topics

- Step 1: Complete the prerequisites
- Step 2: (Optional) Add storage space
- Step 3: Upload and download files
- Step 4: Launch the RStudio application
- Step 5: Read the RStudio documentation

- Step 6: (Optional) Monitor usage and costs
- Step 7: (Optional) Create a cost control rule
- Step 8: (Optional) Create a snapshot
- Step 9: (Optional) Stop or delete your virtual computer

Step 1: Complete the prerequisites

Create a virtual computer using the RStudio application if you haven't already. For more information, see Create a virtual computer.

After your new virtual computer is up and running, continue to Step 4 of this tutorial.

Step 2: (Optional) Add storage space

Your virtual computer comes with a system disk. However, as your storage needs change, you can attach additional disks to your virtual computer to increase its storage space.

You can also store your working files to an attached disk. Then you can detach the disk and attach it to a different virtual computer to quickly move your files from one computer to another.

Alternatively, you can create a snapshot of an attached disk that has your working files, and then create a duplicate disk from the snapshot. Then you can attach the new duplicate disk to another computer to duplicate your work across different virtual computers. For more information, see Create a disk and Attach a disk to a virtual computer.

> **Note**
>
> When you attach a disk to your virtual computer using the console, Lightsail for Research automatically formats and mounts the disk. This process takes a few minutes, so you should confirm that the disk has reached a **Mounted** mounting status before you start using it. By default, Lightsail for Research mounts disks to the `/home/lightsail-user/<disk-name>` directory `<disk-name>` is the name you gave your disk.

Step 3: Upload and download files

You can upload files to your RStudio virtual computer, and download files from it. To do so, you must complete the following steps:

1. Obtain a key pair from Amazon Lightsail. For more information, see Get a key pair for a virtual computer.
2. After you have the key pair, you can use it to establish a connection using the Secure Copy (SCP) utility. SCP lets you upload and download files using Command Prompt or Terminal. For more information, see Transfer files to a virtual computer using Secure Copy.
3. (Optional) You can also use the key pair to connect to your virtual computer with SSH. For more information, see Connect to a virtual computer using Secure Shell.

> **Note**
>
> You can also access your virtual computer's command line interface and transfer files by using the browser-based NICE DCV client. NICE DCV is available in the Lightsail for Research console. For more information, see Launch a virtual computer's application and Access a virtual computer's operating system.

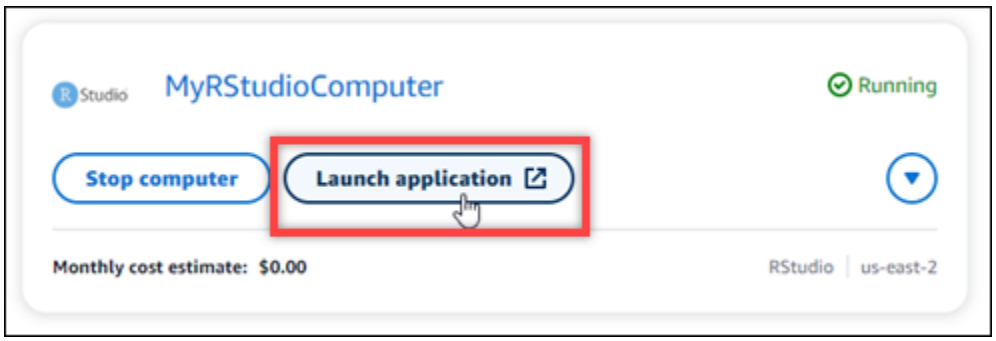
Step 4: Launch the RStudio application

Complete the following procedure to launch the RStudio application on your new virtual computer.

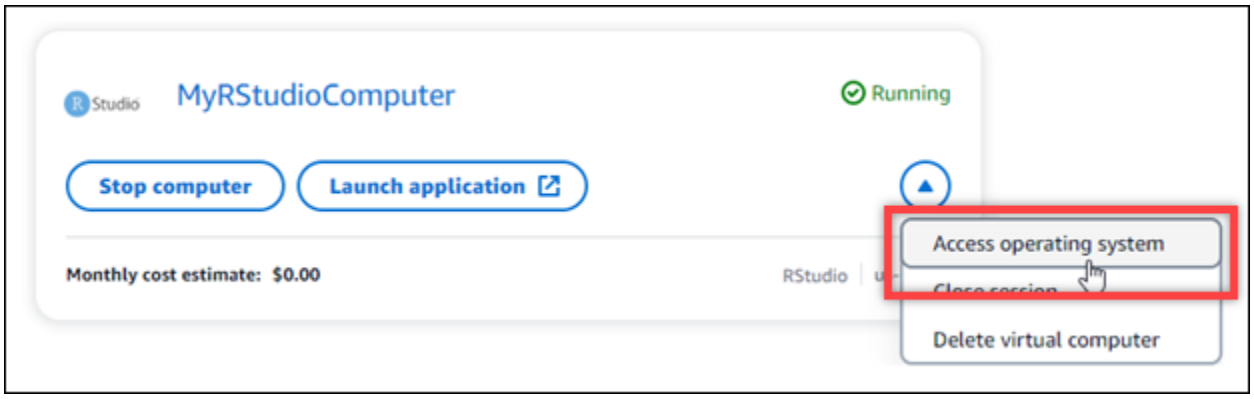
> **Important**
>
> Don't update the operating system or the RStudio application even if you are prompted to do so. Instead, choose the option to close or ignore those prompts. Furthermore, don't modify any of the files that are in the **/home/lightsail-admin/** directory. These actions might render the virtual computer unusable.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane to view the virtual computers that are available in your account.
3. In the **Virtual computers** page, find your virtual computer and choose one of the following options to connect to it:

    a. (Recommended) Choose **Launch application** to launch the RStudio application in focused mode. If you haven't connected to your virtual computer recently, you might have to wait a few minutes while Lightsail for Research prepares your session.



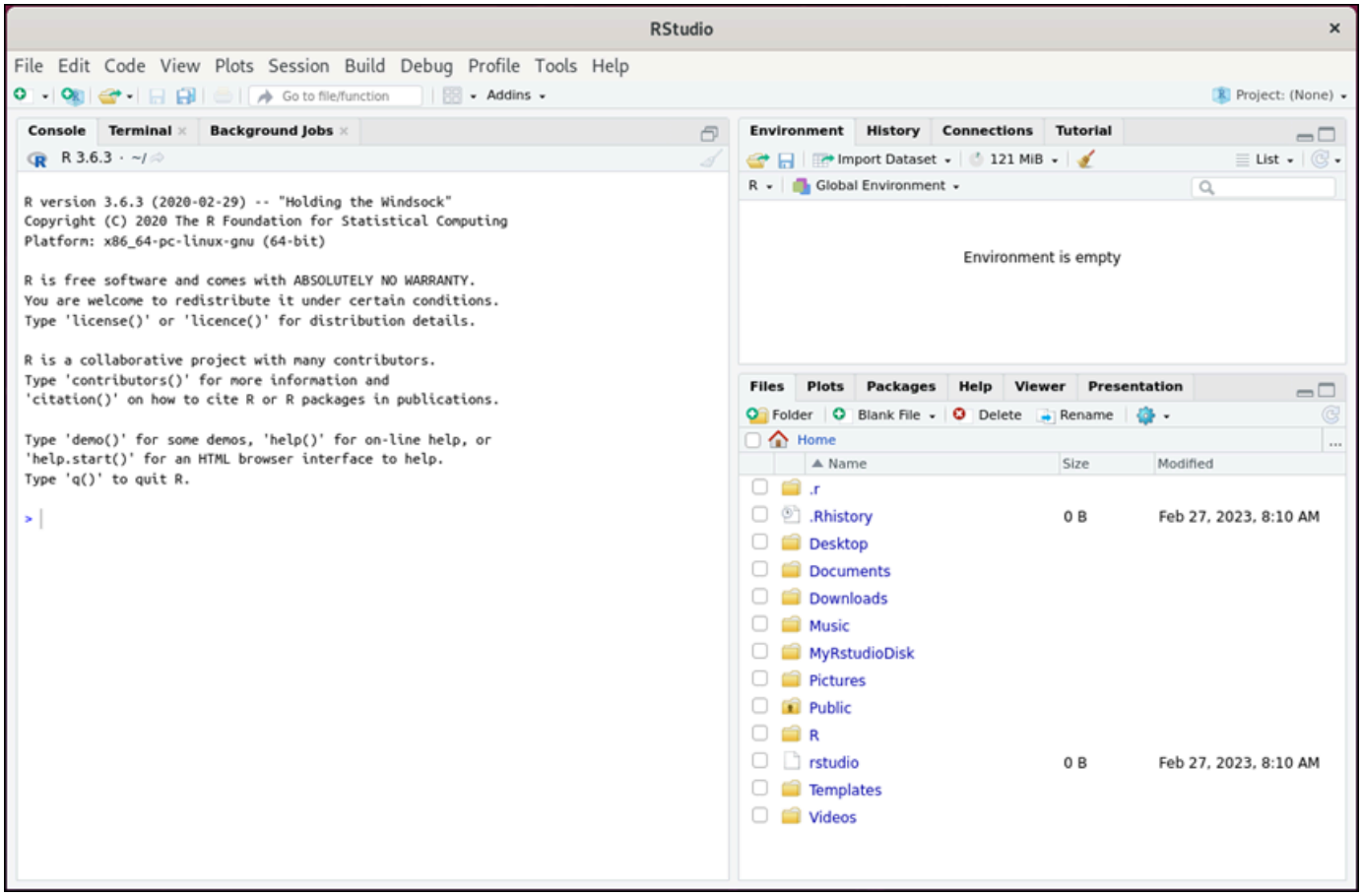
b. Choose the dropdown menu for the computer, and then choose **Access operating system** to access your virtual computer's desktop. Do this if you want to install a different application on the operating system.



Lightsail for Research runs a few commands to initiate the remote display protocol connection. After a few moments, a new browser tab window opens with a virtual desktop connection established to your virtual computer. If you chose the **Launch application** option, continue to the next step of this procedure to open a file in the RStudio application. If you chose the **Access operating system** option, you can open other applications through the Ubuntu desktop.

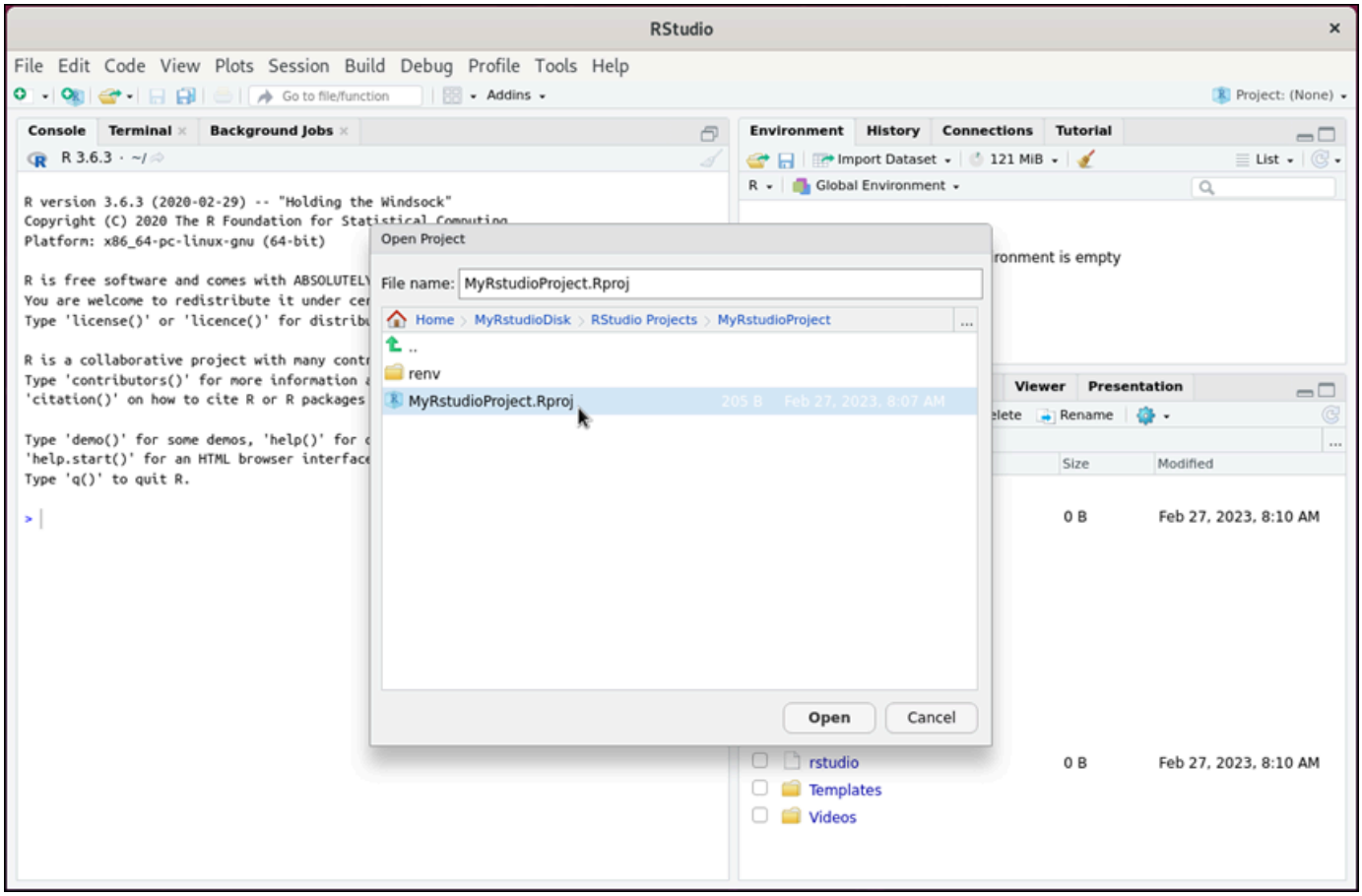
> **Note**
>
> Your browser might prompt you to authorize sharing of your clipboard. Allowing this lets you copy and paste between your local computer and your virtual computer. Ubuntu might also prompt you for an initial setup. Follow the prompts until you complete the setup and can use the operating system.

4. The RStudio application opens.

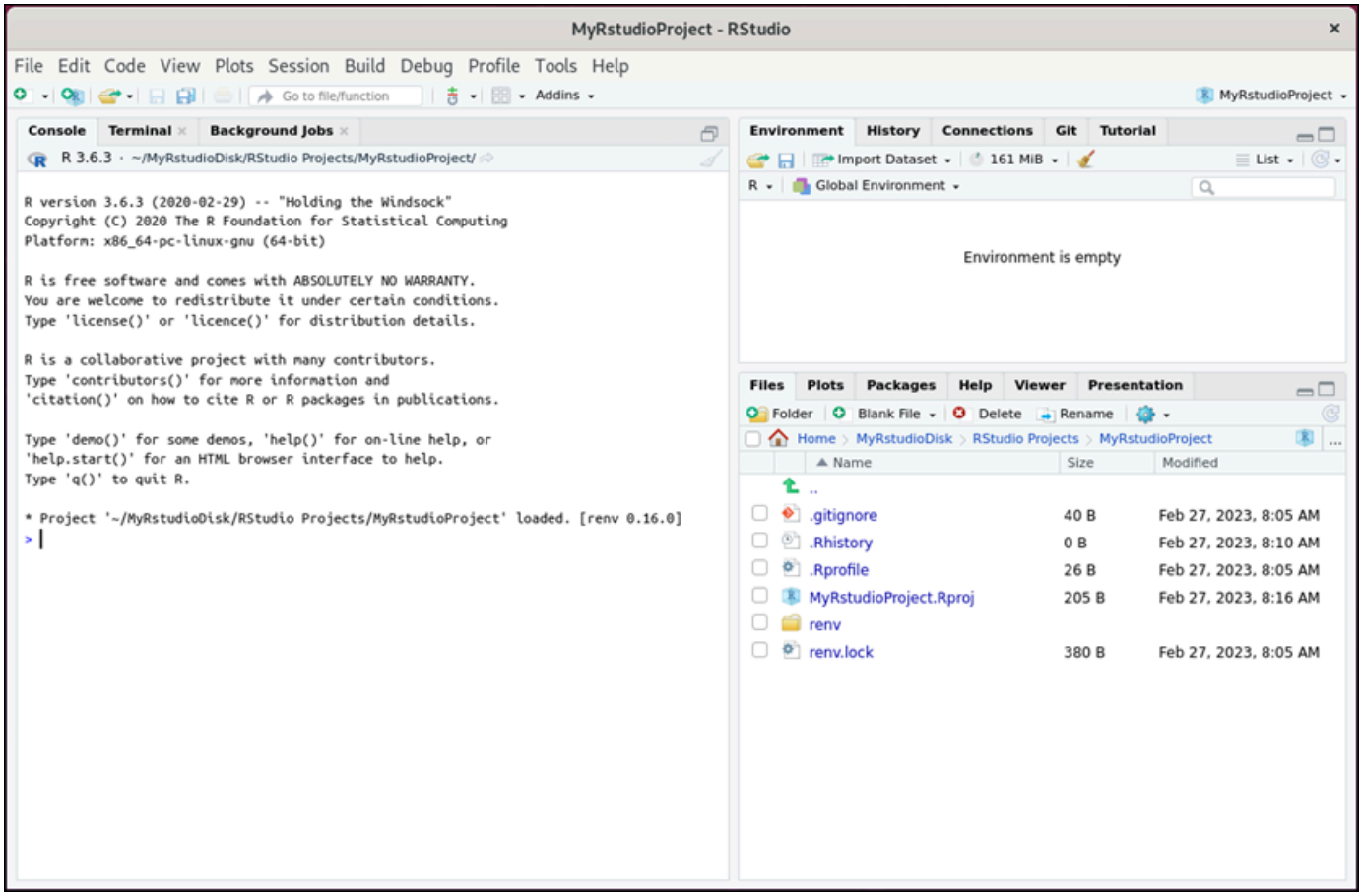


5. To open a project in RStudio, choose the **File** menu, and then choose **Open project**. Browse to the directory or folder where your project files are stored. Then choose the file to open.

   If you uploaded your project files to an attached disk, look for the directory where the disk is mounted. By default, Lightsail for Research mounts disks to the `/home/lightsail-user/<disk-name>` directory. *<disk-name>* is the name you gave your disk. In the following example, the `MyRstudioDisk` directory represents the mounted disk, and the `Projects` subdirectory contains our RStudio project files.



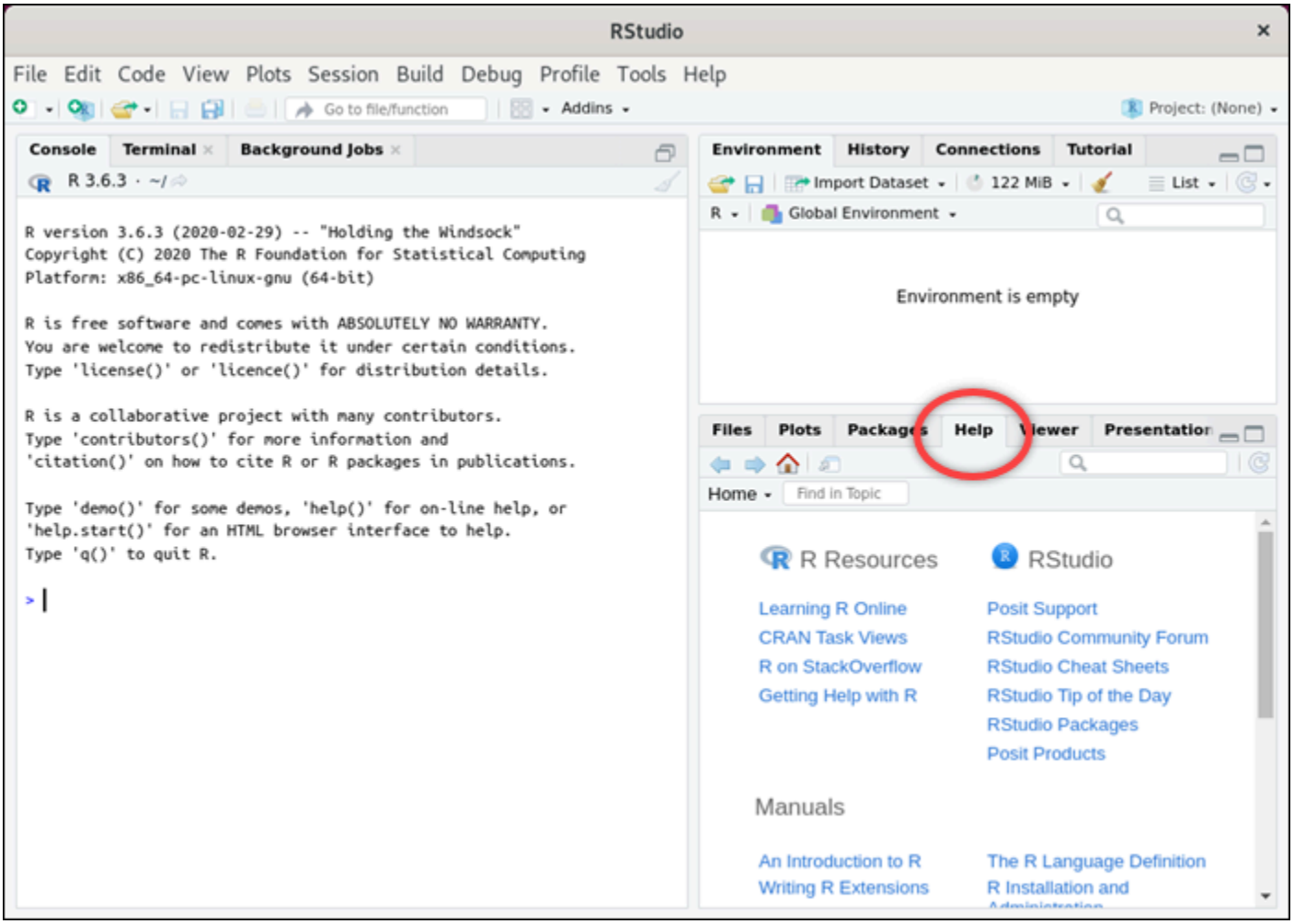
In the following example, we have opened the `MyRstudioProject.Rproj` project file.



For information about how to get started with RStudio, continue to the Step 5: Read the RStudio documentation section of this tutorial.

Step 5: Read the RStudio documentation

The RStudio application is bundled with a comprehensive documentation package. To get started with learning RStudio, we recommend that you access the **Help** tab in RStudio as shown in the following example.



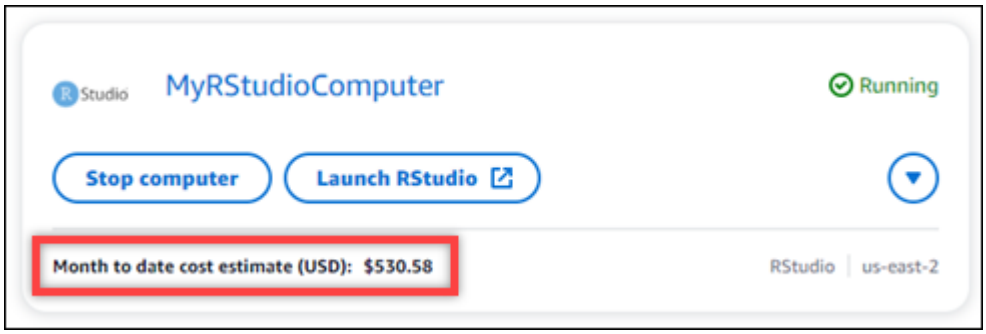
The following RStudio online resources are also available:

- Learning R Online
- R on StackOverflow
- Getting Help with R
- Posit Support
- RStudio Community Forum
- RStudio Cheat Sheets
- RStudio Tip of the Day (Twitter)
- RStudio Packages

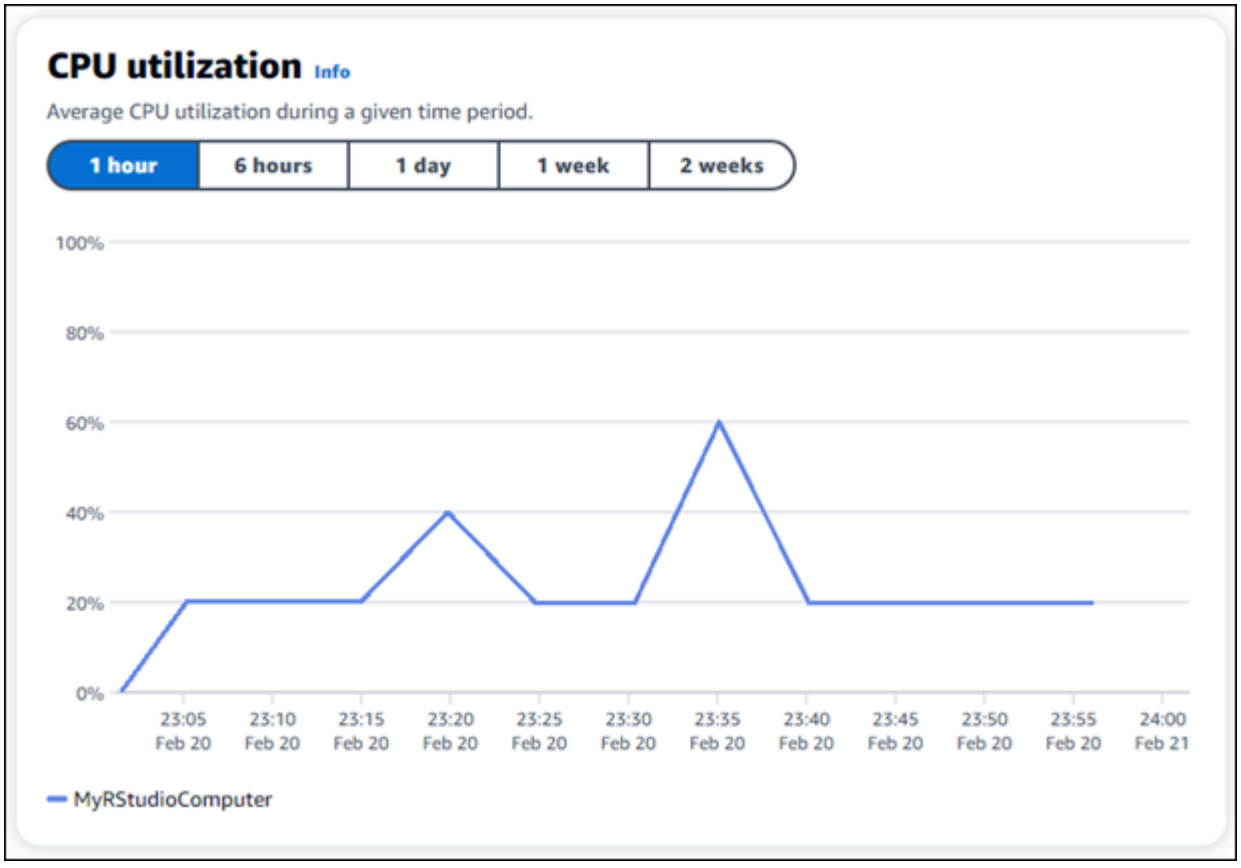
Step 6: (Optional) Monitor usage and costs

Month to date cost and usage estimates for your Lightsail for Research resources are displayed in the following areas of the Lightsail for Research console.

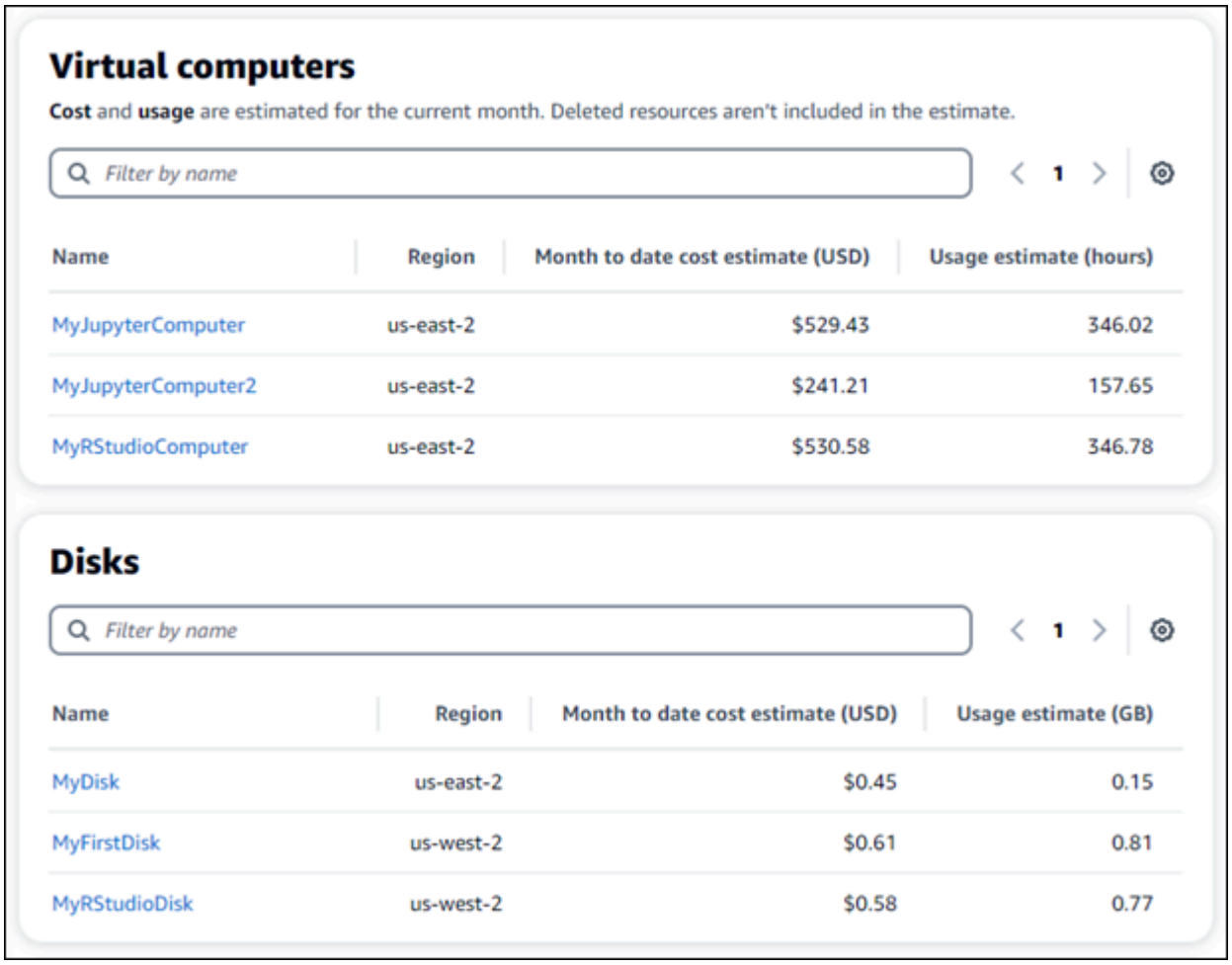
1. Choose **Virtual computers** in the navigation pane of the Lightsail for Research console. The month to date cost estimate for your virtual computers is listed under each running virtual computer.



2. To view the CPU utilization for a virtual computer, choose the name of the virtual computer, and then choose the **Dashboard** tab.



3. To view the month to date cost and usage estimates for all of your Lightsail for Research resources, choose **Usage** in the navigation pane.



Step 7: (Optional) Create a cost control rule

Manage the usage and cost of your virtual computers by creating cost control rules. You can create a **Stop virtual computer on idle** rule that stops a running computer when it reaches a specified percentage of its CPU utilization during a given period. For example, a rule can automatically stop a specific computer when its CPU utilization is equal to or less than 5% during a 30-minute period. This might mean that the computer is idle, and Lightsail for Research stops the computer so that you don't incur charges for an idle resource.

> **Important**
>
> Before you create a rule to stop your virtual computer on idle, we recommend monitoring its CPU utilization for a few days. Take note of the CPU utilization while your virtual

computer is under different loads. For example, when it's compiling code, processing an operation, and idling. This will help you determine an accurate threshold for the rule. For more information, see the Step 6: (Optional) Monitor usage and costs section of this tutorial.
If you create a rule with a CPU utilization threshold that's higher than your workload, the rule can consecutively stop your virtual computer. For example, if you start your virtual computer immediately after a rule stops it, the rule reactivates and the computer stops again.

Detailed instructions for creating, and managing cost control rules can be found in the following guides:

- Cost control
- Create a rule
- Delete a rule

Step 8: (Optional) Create a snapshot

Snapshots are a point-in-time copy of your data. You can create snapshots of your virtual computers and use them as baselines to create new computers or for data backup. A snapshot contains all of the data that's needed to restore your computer (from the moment when the snapshot was taken).

Detailed instructions for creating, and managing snapshots can be found in the following guides:

- Create a snapshot
- View snapshots
- Create a virtual computer or disk from a snapshot
- Delete a snapshot

Step 9: (Optional) Stop or delete your virtual computer

After you're done with the virtual computer that you created for this tutorial, you can delete it. This stops incurring charges for the virtual computer if you don't need it.

Deleting a virtual computer doesn't delete its associated snapshots or attached disks. If you created snapshots and disks, you should delete those manually to stop incurring charges for them.

To save your virtual computer for later, but to avoid incurring charges at standard hourly prices, you can stop the virtual computer instead of deleting it. Then you can start it again later. For more information, see View virtual computer details. For more information about pricing, see Lightsail for Research pricing.

> **Important**
>
> Deleting a Lightsail for Research resource is a permanent action. The deleted data cannot be recovered. If you might need the data later, create a snapshot of your virtual computer before you delete it. For more information, see Create a snapshot.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane.
3. Choose the virtual computer to delete.
4. Choose **Actions**, then choose **Delete virtual computer**.
5. Type **confirm** in the text block. Then, choose **Delete virtual computer.**

Virtual computers

With Amazon Lightsail for Research, you can create virtual computers in the AWS Cloud.

When you create a virtual computer, you choose an application and a hardware plan to use. You can set a spend limit for your virtual computer, and choose what happens when the virtual computer reaches that limit. For example, you can choose to automatically stop the virtual computer so that you're not charged more than your configured budget.

> **Important**
>
> As of March 22, 2024, Lightsail for Research virtual computers will have IMDSv2 enforced by default.

Topics

- Applications and hardware plans
- Create a virtual computer
- View virtual computer details
- Launch a virtual computer's application
- Access a virtual computer's operating system
- Manage firewall ports for virtual computers
- Get a key pair for a virtual computer
- Connect to a virtual computer using Secure Shell
- Transfer files to a virtual computer using Secure Copy
- Delete a virtual computer

Applications and hardware plans

When you create an Amazon Lightsail for Research virtual computer, you select an application and a hardware plan (plan) for it.

An *application* provides a software configuration (for example, an application and operating system). A *plan* provides the hardware of the virtual computer, such as the number of vCPUs,

memory, storage space, and monthly data transfer allowance. Together, the application and plan make up the virtual computer configuration.

> **Note**
>
> You can't change the application or plan of your virtual computer after it's created. However, you can create a snapshot of the virtual computer, and then choose a new plan when creating a new virtual computer from the snapshot. For more information about snapshots, see Snapshots.

Topics

- Applications
- Plans

Applications

Amazon Lightsail for Research provides and manages machine images that contain the application and operating system required to launch a virtual computer. You choose from a list of applications when you create a virtual computer in Lightsail for Research. All Lightsail for Research application images use the Ubuntu (Linux) operating system.

The following applications are available in Lightsail for Research:

- **JupyterLab** – JupyterLab is a web-based Integrated Development Environment (IDE) for notebooks, code, and data. With its flexible interface you can configure and arrange workflows in data science, scientific computing, computational journalism, and machine learning. For more information, see the Jupyter Project Documentation.
- **RStudio** – RStudio is an open-source Integrated Development Environment (IDE) for R, a programming language for statistical computing and graphics, and Python. It combines a source code editor, build automation tools and a debugger, as well as tools for plotting and workspace management. For more information, see the RStudio IDE.
- **VSCodium** – VSCodium is a community-driven, binary distribution of Microsoft's editor VS Code. For more information, see VSCodium.
- **Scilab** – Scilab is an open source numerical computational package, and a high-level, numerically oriented programming language. For more information, see Scilab.

- **Ubuntu 20.04 LTS** – Ubuntu is an open source Linux distribution based on Debian. Lean, fast and powerful, Ubuntu Server delivers services reliably, predictably and economically. It's a great base on which to build your virtual computers. For more information, see Ubuntu releases.

Plans

A plan provides the hardware specifications and determines the pricing for your Lightsail for Research virtual computer. A plan includes a fixed amount of memory (RAM), compute (vCPUs), SSD-based storage volume (disk) space, and a monthly data transfer allowance. Plans are charged on an hourly, on-demand basis, so you only pay for the time your virtual computer is running.

The plan that you choose might depend on the resources that your workload requires. Lightsail for Research offers the following plans types:

- **Standard** – Standard plans are compute-optimized and ideal for compute-bound applications that benefit from high-performance processors.
- **GPU** – GPU plans provide a cost-effective, high-performance platform for general purpose GPU computing. You can use these plans to accelerate scientific, engineering, and rendering applications and workloads.

Standard plans

Following are the hardware specifications of the standard plans available in Lightsail for Research.

Plan name	vCPUs	Memory	Storage space	Monthly data transfer allowance
Standard XL	4	8 GB	50 GB	512 GB
Standard 2XL	8	16 GB	50 GB	512 GB
Standard 4XL	16	32 GB	50 GB	512 GB

GPU plans

Following are the hardware specifications of the GPU plans available in Lightsail for Research.

Plan name	vCPUs	Memory	Storage space	Monthly data transfer allowance
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

Create a virtual computer

Complete the following steps to create a Lightsail for Research virtual computer running an application.

1. Sign in to the Lightsail for Research console.
2. On the home page, choose **Create virtual computer**.
3. Select an AWS Region for your virtual computer that is near your physical location.
4. Choose an application and hardware plan. For more information, see Applications and hardware plans.
5. Enter a name for your virtual computer. Valid characters include alphanumeric characters, numbers, periods, hyphens, and underscores.

   Virtual computer names must also meet the following requirements:

   - Be unique within each AWS Region in your Lightsail for Research account.
   - Contain 2–255 characters.
   - Start and end with an alphanumeric character or number.
6. Choose **Create virtual computer** in the **Summary** panel.

Within minutes, your Lightsail for Research virtual computer is ready and you can connect to it through a graphical user interface (GUI) session. For more information about connecting to your Lightsail for Research virtual computer, see Launch a virtual computer's application.

> **Important**
>
> Newly created virtual computers have a set of firewall ports open by default. For more information about these ports, see Manage firewall ports for virtual computers.

View virtual computer details

Complete the following steps to view a list of virtual computers and their details in your Lightsail for Research account.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane to see a list of virtual computers in your account.

Choose a virtual computer's name to navigate to its management page. Following is the information that the management page provides:

- **Virtual computer name** – The name of your virtual computer.
- **Status** – Your virtual computer can have one of the following status codes:
  - Creating
  - Running
  - Stopping
  - Stopped
  - Unknown
- **AWS Region** – The AWS Region your virtual computer was created in.
- **Application & Hardware** – The application and hardware plan of the virtual computer.
- **Monthly usage estimate** – The estimated hourly usage for this virtual computer, for the current billing cycle.
- **Month to date cost estimate** – The estimated cost (in USD) for the virtual computer, for this billing cycle.
- **Dashboard** – From the **Dashboard** tab, you can launch a session to access the virtual computer's application. You can also view the CPU utilization. CPU utilization identifies the processing power that's used by the virtual computer's applications. Each data point shown in the graph represents the average CPU utilization over a period of time.

- **Cost control rules** – Rules that you define to help manage the usage and costs of your virtual computer.
- **Virtual computer usage** – A cost and usage estimate for the given billing cycle. You can filter this by date and time.
- **Storage** – Create, attach, and detach virtual computer disks from the **Storage** tab. A disk is a storage volume that you can attach to a virtual computer and mount as a hard drive.
- **Tags** – Manage your virtual computer tags from the tags tab. A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources, or track your AWS costs.

Launch a virtual computer's application

Complete the following steps to launch the application that's running on your Lightsail for Research virtual computer.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane.
3. Locate the name of the virtual computer that you want to launch the application from.

   > **Note**
   >
   > If the virtual computer is stopped, first choose the **Start computer** button to turn it on.

4. Choose **Launch application**. For example, **Launch JupyterLab**. An application session will open in a new web browser window.

   > **Important**
   >
   > If your web browser has a pop-up blocker installed, you might need to allow pop-ups from the **aws.amazon.com** domain before opening your session.

Access a virtual computer's operating system

Complete the following steps to access the operating system for your Lightsail for Research virtual computer.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane.
3. Locate the name of your virtual computer and then choose the actions button dropdown under the computer's status.

> **Note**
>
> If the virtual computer is stopped, first choose the **Start** button to turn it on.

4. Choose **Access operating system**. An operating system session will open in a new browser window.

> **Important**
>
> If your web browser has a pop-up blocker installed, you might need to allow pop-ups from the **aws.amazon.com** domain before to opening your session.

Manage firewall ports for virtual computers

A firewall in Amazon Lightsail for Research controls the traffic allowed to connect to your virtual computer. You add rules to your virtual computer's firewall that specify the protocol, ports, and the source IPv4 or IPv6 addresses that are allowed to connect to it. Firewall rules are always permissive; you can't create rules that deny access. You add rules to your virtual computer's firewall to allow traffic to reach your virtual computer. Each virtual computer has two firewalls; one for IPv4 addresses and another for IPv6 addresses. Both firewalls are independent of each other, and contain a preconfigured set of rules that filter traffic coming into the instance.

Protocols

A protocol is the format in which data is transmitted between two computers. You can specify the following protocols in a firewall rule:

- **Transmission Control Protocol (TCP)** is primarily used for establishing and maintaining a connection between clients and the application that's running on your virtual computer. It is a widely used protocol, and one that you might often specify in your firewall rules.
- **User Datagram Protocol (UDP)** is primarily used for establishing low-latency and loss-tolerating connections between clients and the application that's running on your virtual computer. Its ideal use is for network applications in which perceived latency is critical, such as gaming, voice, and video communications.
- **Internet Control Message Protocol (ICMP)** is primarily used to diagnose network communication issues, such as to determine if data is reaching its intended destination in a timely manner. Its ideal use is for the Ping utility, which you can use to test the speed of the connection between your local computer and your virtual computer. It reports how long it takes data to reach your virtual computer and come back to your local computer.
- **All** is used to allow all protocol traffic to flow into your virtual computer. Specify this protocol when you're unsure which protocol to specify. This includes all internet protocols, not only the ones specified here. For more information, see Protocol Numbers on the *Internet Assigned Numbers Authority website*.

Ports

Similar to physical ports on your computer, which let your computer communicate with peripherals like your keyboard and pointer, firewall ports serve as internet communications endpoints for your virtual computer. When a client seeks to connect with your virtual computer, it will expose a port to establish the communication.

The ports that you can specify in a firewall rule can range from 0 to 65535. When you create a firewall rule to allow a client to establish a connection with your virtual computer, you specify the protocol to use. You also specify the port numbers through which the connection can be established and the IP addresses that are allowed to establish a connection.

The following ports are open by default for newly created virtual computers.

- TCP

- 22 - Used for Secure Shell (SSH).
- 80 - Used for Hypertext Transfer Protocol (HTTP).
- 443 - Used for Hypertext Transfer Protocol Secure (HTTPS).
- 8443 - Used for Hypertext Transfer Protocol Secure (HTTPS).

Why open and close ports

When you open ports, you allow a client to establish a connection with your virtual computer. When you close ports, you block connections to your virtual computer. For example, to allow an SSH client to connect to your virtual computer, you configure a firewall rule that allows TCP over port 22 only from the IP address of the computer that needs to establish a connection. In this case, you don't want to allow any IP address to establish an SSH connection to your virtual computer. Doing so could lead to a security risk. If this rule is already configured on your instance's firewall, then you can delete it to block the SSH client from connecting to your virtual computer.

The following procedures show you how to get the ports that are currently open on your virtual computer, open new ports, and close ports.

Topics

- Complete the prerequisites
- Get port states for a virtual computer
- Open ports for a virtual computer
- Close ports for a virtual computer
- Continue to the next steps

Complete the prerequisites

Complete the following prerequisites before you get started.

- Create a virtual computer in Lightsail for Research. For more information, see Create a virtual computer.
- Download and install the AWS Command Line Interface (AWS CLI). For more information, see Installing or updating the latest version of the AWS CLI in the *AWS Command Line Interface User Guide for Version 2*.

- Configure the AWS CLI to access your AWS account. For more information, see Configuration basics in the *AWS Command Line Interface User Guide for Version 2*.

Get port states for a virtual computer

Complete the following procedure to get the port states for a virtual computer. This procedure uses the `get-instance-port-states` AWS CLI command to obtain the firewall port states for a specific Lightsail for Research virtual computer, the IP addresses allowed to connect to the virtual computer through the ports, and the protocol. For more information, see get-instance-port-states in the *AWS CLI Command Reference*.

1. This step is determined by the operating system of your local computer.
   - If your local computer uses a Windows operating system, open a Command Prompt window.
   - If your local computer uses a Linux or Unix-based operating system (including macOS), open a Terminal window.
2. Enter the following command to get the firewall port states and allowed IP addresses and protocols. In the command, replace *REGION* with the code of the AWS Region in which the virtual computer was created, such as `us-east-2`. Replace *NAME* with the name of your virtual computer.

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

   Example

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

   The response will display the open ports and protocols, and the IP CIDR ranges that are allowed to connect to your virtual computer.

   ```
   [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
   ```

For information about how to open ports, continue to the next section.

Open ports for a virtual computer

Complete the following procedure to open ports for a virtual computer. This procedure uses the `open-instance-public-ports` AWS CLI command. Open firewall ports to allow connections to be established from a trusted IP address or range of IP addresses. For example, to allow the IP address `192.0.2.44`, specify `192.0.2.44` or `192.0.2.44/32`. To allow the IP addresses `192.0.2.0` to `192.0.2.255`, specify `192.0.2.0/24`. For more information, see open-instance-public-ports in the *AWS CLI Command Reference*.

1. This step is determined by the operating system of your local computer.

   - If your local computer uses a Windows operating system, open a Command Prompt window.
   - If your local computer uses a Linux or Unix-based operating system (including macOS), open a Terminal window.

2. Enter the following command to open ports.

   In the command, replace the following items:

   - Replace *REGION* with the code of the AWS Region in which the virtual computer was created, such as `us-east-2`.
   - Replace *NAME* with the name of your virtual computer.
   - Replace *FROM-PORT* with the first port in a range of ports that you want to open.
   - Replace *PROTOCOL* with the IP protocol name. For example, TCP.
   - Replace *TO-PORT* with the last port in a range of ports that you want to open.
   - Replace *IP* with the IP address or range of IP address that you want to allow to connect to your virtual computer.

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

   Example

```
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
```

The response will display the newly added ports, protocols, and IP CIDR ranges that are allowed to connect to your virtual computer.

For information about how to close ports, continue to the next section.

Close ports for a virtual computer

Complete the following procedure to close ports for a virtual computer. This procedure uses the `close-instance-public-ports` AWS CLI command. For more information, see close-instance-public-ports in the *AWS CLI Command Reference*.

1. This step is determined by the operating system of your local computer.

   - If your local computer uses a Windows operating system, open a Command Prompt window.
   - If your local computer uses a Linux or Unix-based operating system (including macOS), open a Terminal window.

2. Enter the following command to close ports.

   In the command, replace the following items:

   - Replace *REGION* with the code of the AWS Region in which the virtual computer was created, such as `us-east-2`.
   - Replace *NAME* with the name of your virtual computer.
   - Replace *FROM-PORT* with the first port in a range of ports that you want to close.

- Replace *PROTOCOL* with the IP protocol name. For example, TCP.
- Replace *TO-PORT* with the last port in a range of ports that you want to close.
- Replace *IP* with the IP address or range of IP address that you want to remove.

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

Example

```
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
```

The response will display the ports, protocols, and IP CIDR ranges that have been closed and are no longer allowed to connect to your virtual computer.

```
[redacted] % aws lightsail close-instance-public-ports --instance-name MyUbuntu
--port-info fromPort=22,protocol=TCP,toPort=22,cidrs=192.0.2.0/24
{
    "operation": {
        "id": "a7f3191a-e9ea-497d-b662-4428121f127c",
        "resourceName": "MyUbuntu",
        "resourceType": "Instance",
        "createdAt": "2023-02-15T16:48:42.459000-08:00",
        "location": {
            "availabilityZone": "us-east-2a",
            "regionName": "us-east-2"
        },
        "isTerminal": true,
        "operationDetails": "22/tcp(192.0.2.0/24)",
        "operationType": "CloseInstancePublicPorts",
        "status": "Succeeded",
        "statusChangedAt": "2023-02-15T16:48:42.459000-08:00"
    }
}
```

Continue to the next steps

You can complete the following additional next steps after you've successfully managed the firewall ports for your virtual computer:

- Get your virtual computer's key pair. With the key pair, you can establish a connection using numerous SSH clients, such as OpenSSH, PuTTY, and Windows Subsystem for Linux. For more information, see Get a key pair for a virtual computer.
- Connect to your virtual computer using SSH to manage it using the command line. For more information, see Transfer files to a virtual computer using Secure Copy.

- Connect to your virtual computer using SCP to securely transfer files. For more information, see Transfer files to a virtual computer using Secure Copy.

Get a key pair for a virtual computer

A key pair, consisting of a public key and a private key, is a set of security credentials that you use to prove your identity when connecting to an Amazon Lightsail for Research virtual computer. The public key is stored on each virtual computer in Lightsail for Research, and you keep the private key on your local computer. The private key allows you to securely establish a Secure Shell Protocol (SSH) with your virtual computer. Anyone who possesses the private key can connect to your virtual computer, so it's important that you store your private key in a secure place.

An Amazon Lightsail default key pair (DKP) is automatically created the first time that you create a Lightsail instance or a Lightsail for Research virtual computer. The DKP is specific to each AWS Region in which you create an instance or virtual computer. For example, the Lightsail DKP for the US East (Ohio) Region (us-east-2) applies to all computers that you create in US East (Ohio) in Lightsail and Lightsail for Research that were configured to use the DKP when they were created. Lightsail for Research automatically stores the public key of the DKP on the virtual computers you create. You can download the private key of the DKP at any time by making an API call to the Lightsail service.

In this document, we show you how to get the DKP for a virtual computer. After you have the DKP, you can establish a connection using numerous SSH clients, such as OpenSSH, PuTTY, and Windows Subsystem for Linux. You can also use Secure Copy (SCP) to securely transfer files from your local computer to your virtual computer.

> **Note**
>
> You can also establish a remote display protocol connection to your virtual computer using the browser-based NICE DCV client. NICE DCV is available in the Lightsail for Research console. That RDP client does not require that you obtain a key pair for your computer. For more information, see Launch a virtual computer's application and Access a virtual computer's operating system.

Topics

- Complete the prerequisites

- Get a key pair for a virtual computer
- Continue to the next steps

Complete the prerequisites

Complete the following prerequisites before you get started.

- Create a virtual computer in Lightsail for Research. For more information, see Create a virtual computer.
- Download and install the AWS Command Line Interface (AWS CLI). For more information, see Installing or updating the latest version of the AWS CLI in the *AWS Command Line Interface User Guide for Version 2*.
- Configure the AWS CLI to access your AWS account. For more information, see Configuration basics in the *AWS Command Line Interface User Guide for Version 2*.
- Download and install jq. It's a lightweight and flexible command line JSON processor used in the following procedures to extract key pair details from JSON outputs of the AWS CLI. For more information about downloading and installing jq, see Download jq on the *jq website*.

Get a key pair for a virtual computer

Complete one of the following procedures to get the Lightsail DKP for a virtual computer in Lightsail for Research.

Get a key pair for a virtual computer using a Windows local computer

This procedure applies to you if your local computer uses a Windows operating system. This procedure uses the `download-default-key-pair` AWS CLI command to obtain the Lightsail DKP for an AWS Region. For more information, see download-default-key-pair in the *AWS CLI Command Reference*.

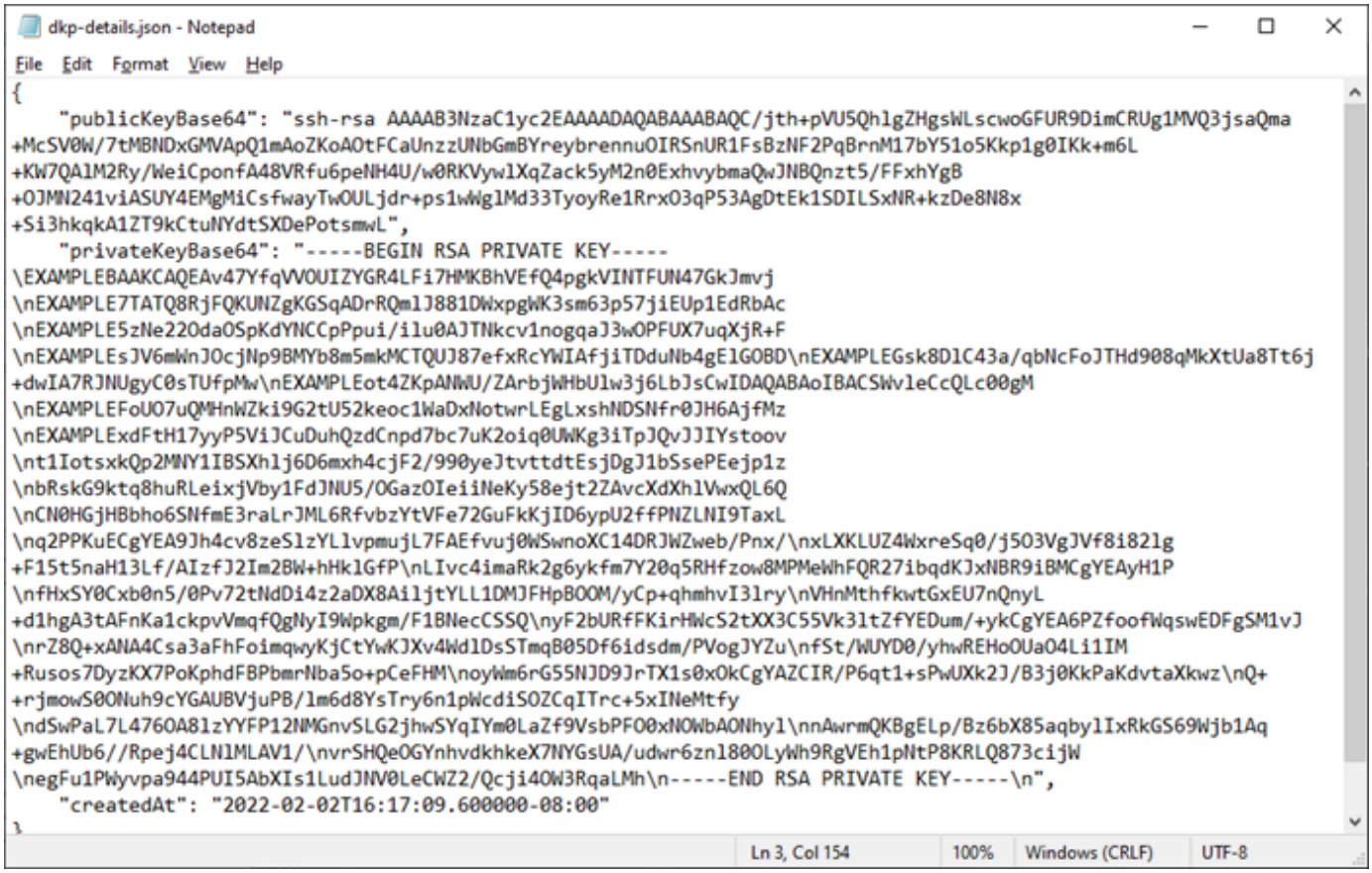
1. Open a Command Prompt window.
2. Enter the following command to get the Lightsail DKP for a specific AWS Region. This command saves the information to a `dkp-details.json` file. In the command, replace *`region-code`* with the code of the AWS Region in which the virtual computer was created, such as `us-east-2`.

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

Example

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

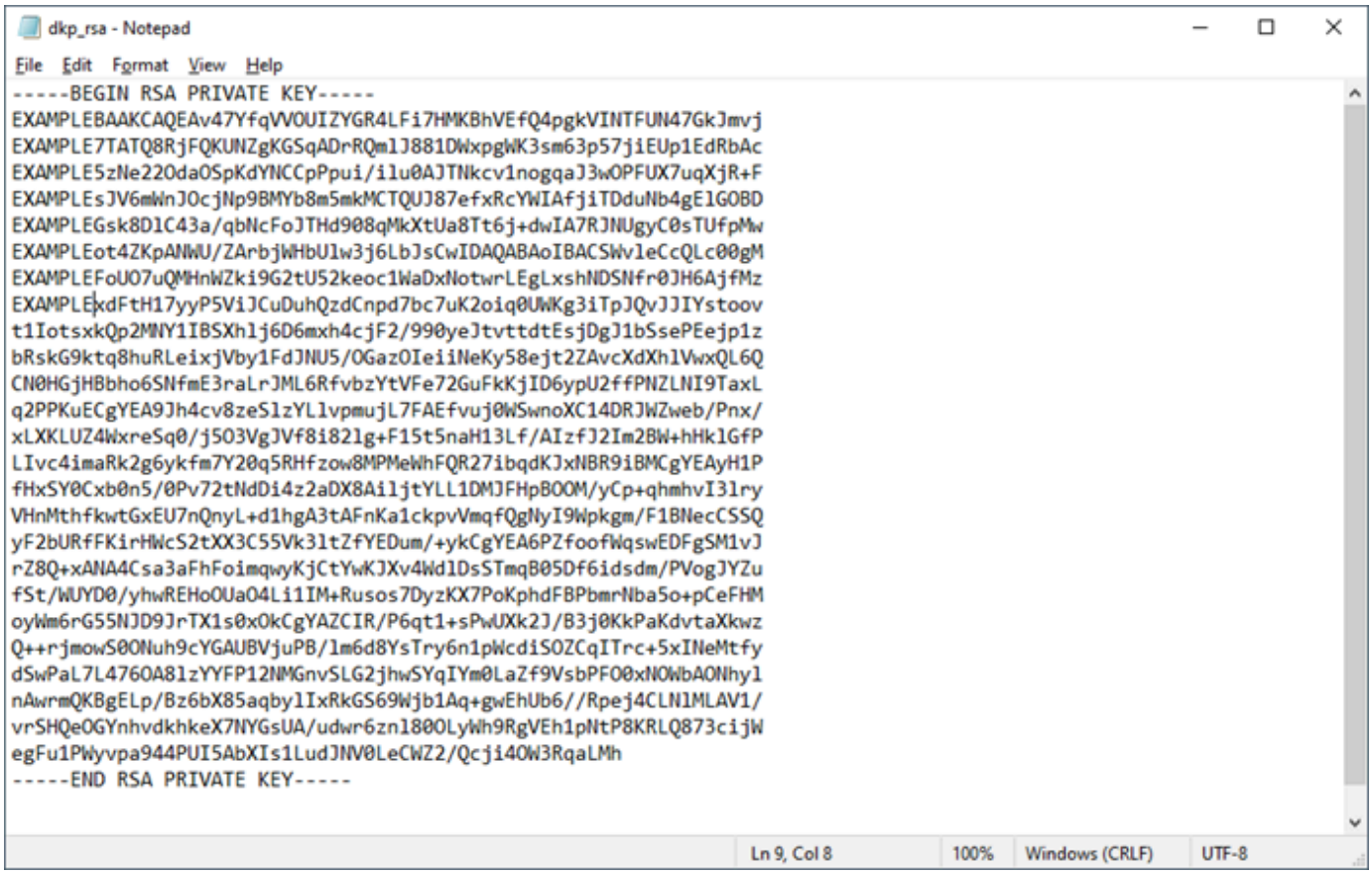
There is no response to the command. You can confirm if the command was successful by opening the `dkp-details.json` file and seeing if the Lightsail DKP information was saved. The contents of the `dkp-details.json` file should look like the following example. The command failed if the file is blank.



3. Enter the following command to extract the private key information from the `dkp-details.json` file and add it to a new `dkp_rsa` private key file.

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

There is no response to the command. You can confirm if the command was successful by opening the `dkp_rsa` files and seeing if it contains information. The contents of the `dkp_rsa` file should look like the following example. The command failed if the file is blank.



You now have the required private key to establish an SSH or SCP connection to your virtual computer. Continue to the next section for additional next steps.

Get a key pair for a virtual computer using a Linux, Unix, or a macOS local computer

This procedure applies to you if your local computer uses a Linux, Unix, or a macOS operating system. This procedure uses the `download-default-key-pair` AWS CLI command to obtain the Lightsail DKP for an AWS Region. For more information, see download-default-key-pair in the *AWS CLI Command Reference*.

1. Open a Terminal window.
2. Enter the following command to get the Lightsail DKP for a specific AWS Region. This command saves the information to a `dkp-details.json` file. In the command, replace

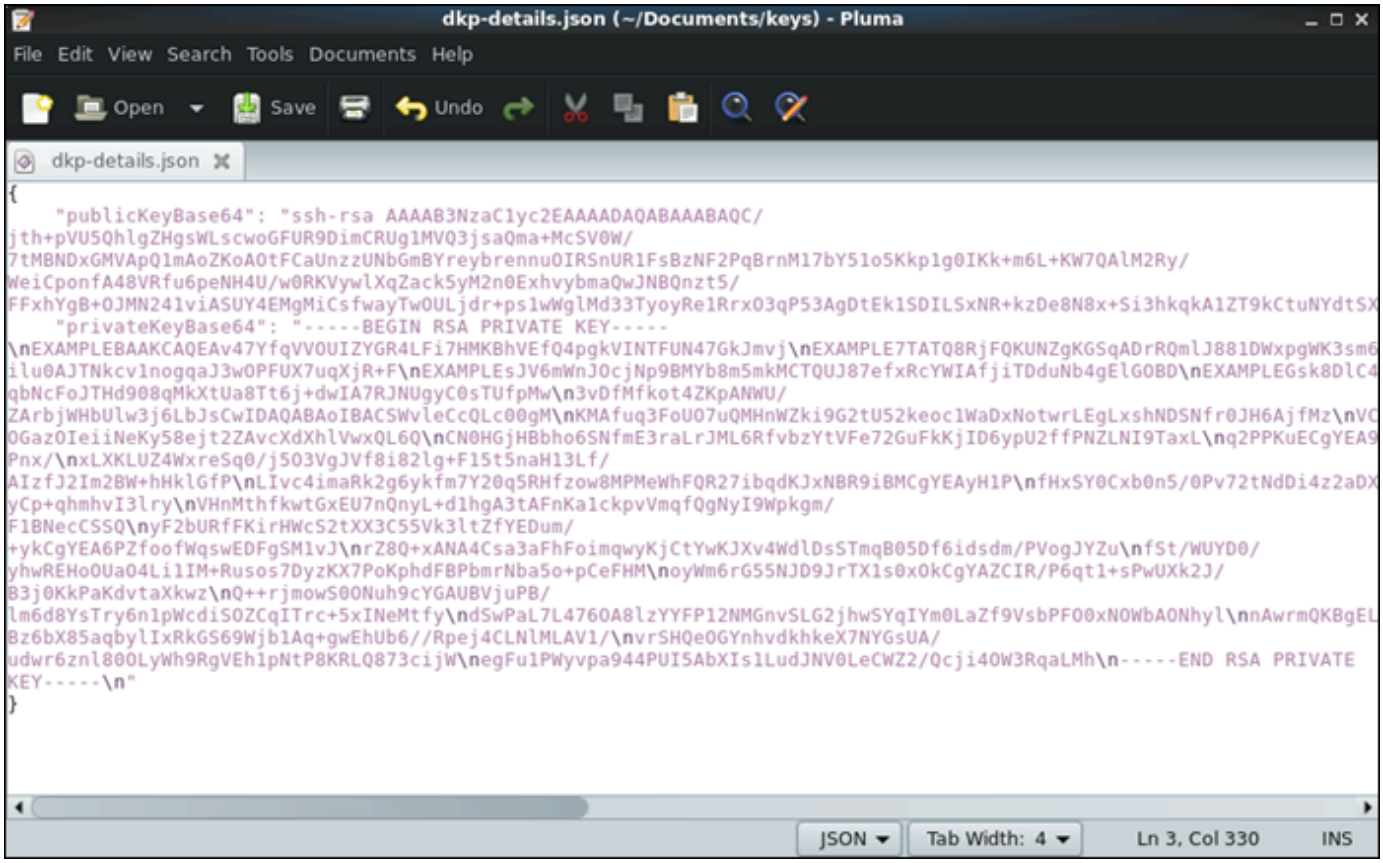
region-code with the code of the AWS Region in which the virtual computer was created, such as us-east-2.

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

Example

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

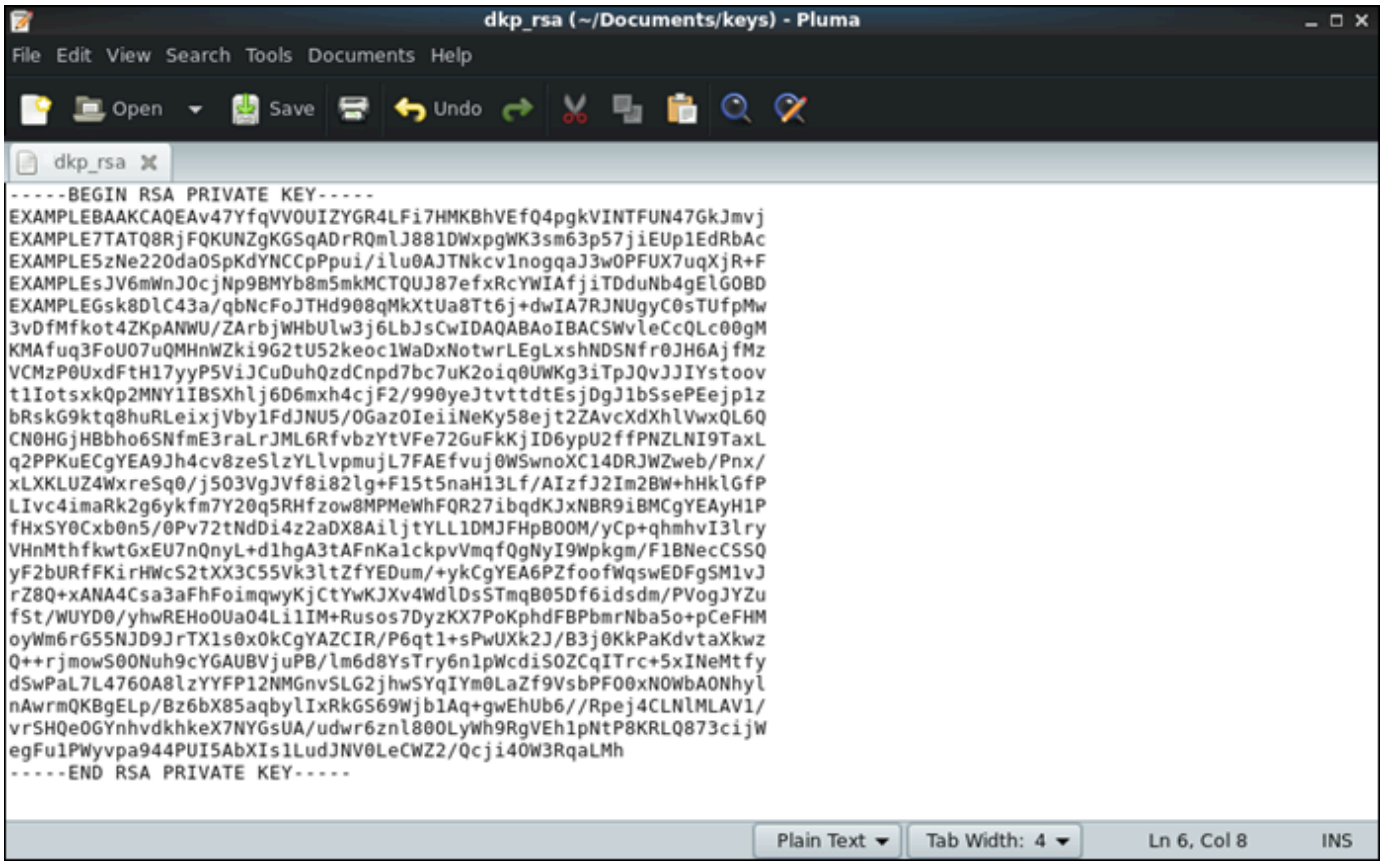
There is no response to the command. You can confirm if the command was successful by opening the dkp-details.json file and seeing if the Lightsail DKP information was saved. The contents of the dkp-details.json file should look like the following example. The command failed if the file is blank.



3. Enter the following command to extract the private key information from the dkp-details.json file and add it to a new dkp_rsa private key file.

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

There is no response to the command. You can confirm if the command was successful by opening the `dkp_rsa` files and seeing if it contains information. The contents of the `dkp_rsa` file should look like the following example. The command failed if the file is blank.



4. Enter the following command to set permissions for the `dkp_rsa` file.

```
chmod 600 dkp_rsa
```

You now have the required private key to establish an SSH or SCP connection to your virtual computer. Continue to the next section for additional next steps.

Continue to the next steps

You can complete the following additional next steps after you've successfully obtained the key pairs for your virtual computer:

- Connect to your virtual computer using SSH to manage it using command line. For more information, see Connect to a virtual computer using Secure Shell.

- Connect to your virtual computer using SCP to securely transfer files. For more information, see Transfer files to a virtual computer using Secure Copy.

Connect to a virtual computer using Secure Shell

You can connect to a virtual computer in Amazon Lightsail for Research using the Secure Shell Protocol (SSH). You can use SSH to manage your virtual computer remotely so that you can sign in to your computer over the internet and run commands.

> **Note**
>
> You can also establish a remote display protocol connection to your virtual computer using the browser-based NICE DCV client. NICE DCV is available in the Lightsail for Research console. For more information, see Access a virtual computer's operating system.

Topics

- Complete the prerequisites
- Connect to a virtual computer using SSH
- Continue to the next steps

Complete the prerequisites

Complete the following prerequisites before you get started.

- Create a virtual computer in Lightsail for Research. For more information, see Create a virtual computer.
- Make sure the virtual computer that you want to connect to is in a running state. Also, note the name of the virtual computer and the AWS Region in which it was created. You'll need this information later in this process. For more information, see View virtual computer details.
- Make sure that port 22 is open on the virtual computer that you want to connect to. That is the default port used for SSH. It's open by default. But if you closed it, you must reopen it before continuing. For more information, see Manage firewall ports for virtual computers.
- Get the Lightsail default key pair (DKP) for your virtual computer. For more information, see Get a key pair for a virtual computer.

> **Tip**
>
> If you plan to use AWS CloudShell to connect to your virtual computer, see Connect to a virtual computer using AWS CloudShell in the next section. For more information, see What is AWS CloudShell. Otherwise, continue to the next prerequisite.

- Download and install the AWS Command Line Interface (AWS CLI). For more information, see Installing or updating the latest version of the AWS CLI in the *AWS Command Line Interface User Guide for Version 2*.
- Configure the AWS CLI to access your AWS account. For more information, see Configuration basics in the *AWS Command Line Interface User Guide for Version 2*.
- Download and install jq. It's a lightweight and flexible command line JSON processor used in the following procedures to extract key pair details. For more information about downloading and installing jq, see Download jq on the *jq website*.

Connect to a virtual computer using SSH

Complete one of the following procedures to establish an SSH connection to your virtual computer in Lightsail for Research.

Connect to a virtual computer using AWS CloudShell

This procedure applies if you prefer minimal setup to connect to your virtual computer. AWS CloudShell uses a browser-based, pre-authenticated shell that you can launch directly from the AWS Management Console. You can run AWS CLI commands using your preferred shell, such as Bash, PowerShell, or Z shell. You can do this without downloading or installing command line tools. For more information, see Getting started with AWS CloudShell in the *AWS CloudShell User Guide*.

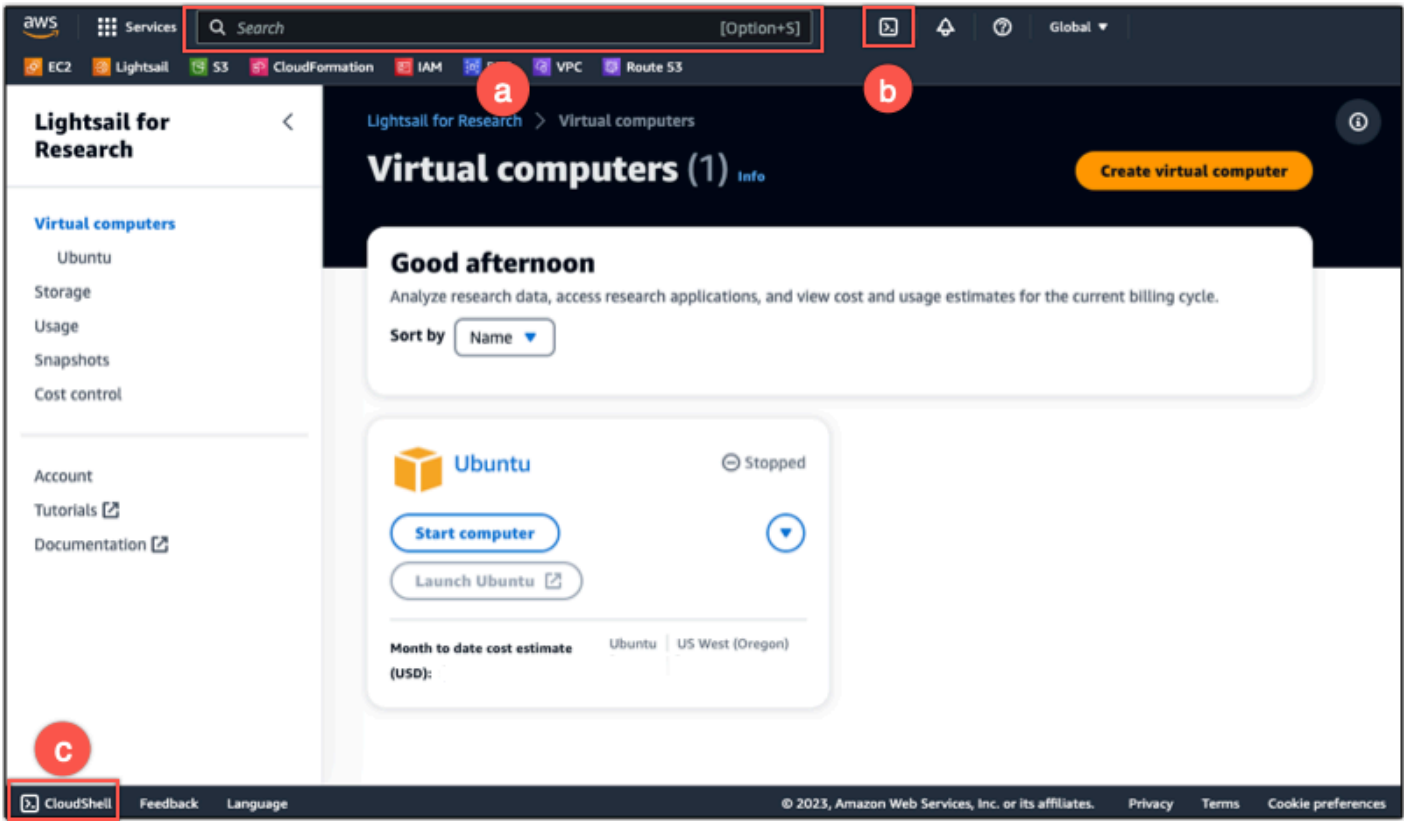
> **Important**
>
> Before you start, make sure to get the Lightsail default key pair (DKP) for the virtual computer that you're connecting to. For more information, see Get a key pair for a virtual computer.

1. From the Lightsail for Research console, launch CloudShell by choosing one of the following options:

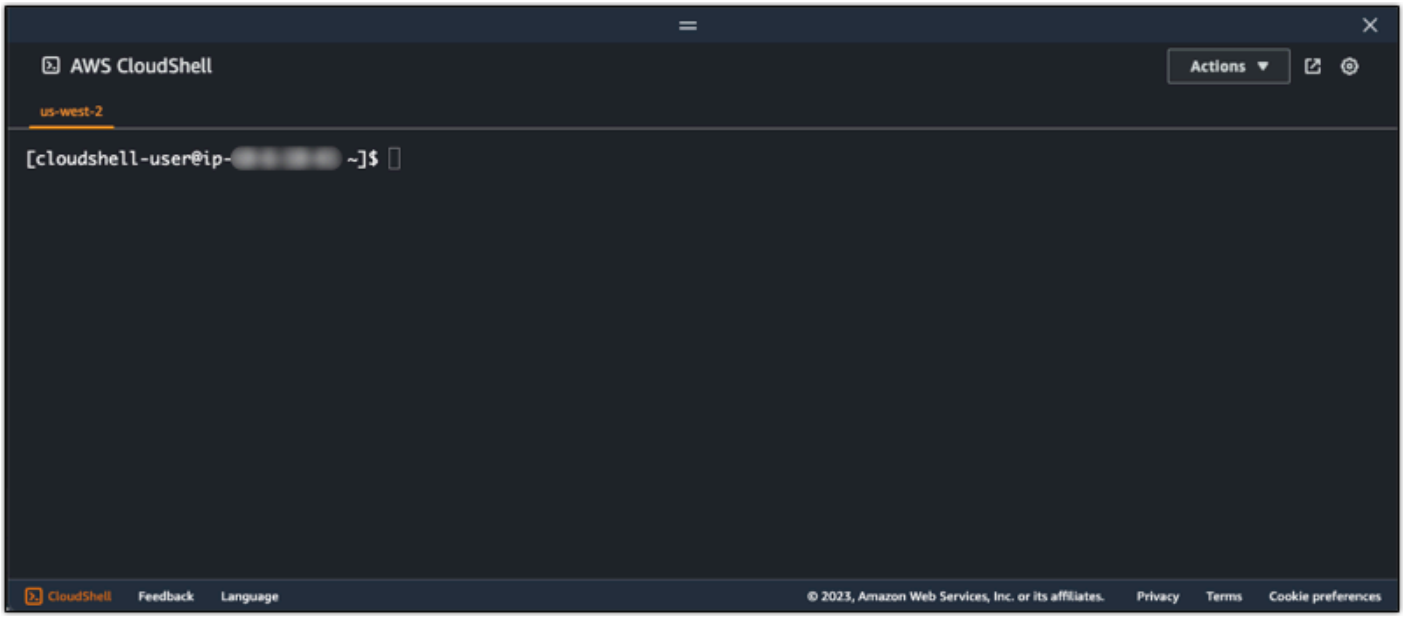
a. In the Search box, type "CloudShell", and then choose **CloudShell**.

b. On the navigation bar, choose the **CloudShell** icon.

c. Choose **CloudShell** on the Console Toolbar in the lower left of the console.



When the command prompt displays, the shell is ready for interaction.



2. Choose a pre-installed shell to work with. To change the default shell, enter one of the following program names at the command line prompt. Bash is the default shell that's running when you launch AWS CloudShell.

   Bash

   ```
   bash
   ```

   If you switch to Bash, the symbol at the command prompt updates to $.

   PowerShell

   ```
   pwsh
   ```

   If you switch to PowerShell, the symbol at the command prompt updates to PS>.

   Z shell

   ```
   zsh
   ```

   If you switch to Z shell, the symbol at the command prompt updates to %.

3. To connect to a virtual computer from the CloudShell terminal window, see Connect to a virtual computer using SSH on a Linux, Unix, or a macOS local computer.

For information about the pre-installed software in the CloudShell environment, see AWS CloudShell compute environment in the *AWS CloudShell User Guide*.

Connect to a virtual computer using SSH on a Windows local computer

This procedure applies if your local computer uses a Windows operating system. This procedure uses the `get-instance` AWS CLI command to obtain the username and public IP address of the instance you want to connect to. For more information, see get-instance in the *AWS CLI Command Reference*.

> **Important**
>
> Make sure you get the Lightsail default key pair (DKP) for the virtual computer you're trying to connect to before you start this procedure. For more information, see Get a key pair for a virtual computer. That procedure outputs the private key of the Lightsail DKP to a `dkp_rsa` file that is used in one of the following commands.

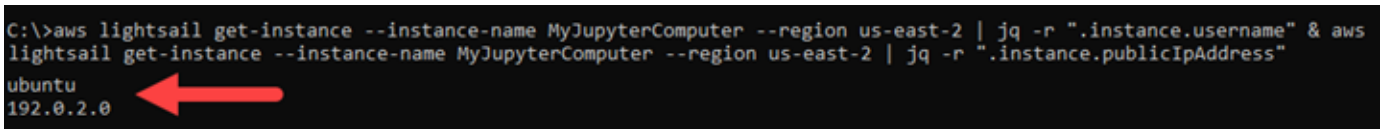
1. Open a Command Prompt window.
2. Enter the following command to display the public IP address and username of your virtual computer. In the command, replace *region-code* with the code of the AWS Region in which the virtual computer was created, such as `us-east-2`. Replace *computer-name* with the name of the virtual computer that you want to connect to.

```
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"
```

Example

```
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"
```

The response will display the username and public IP address of the virtual computer as shown in the following example. Note these values, because you need them in the following step of this procedure.



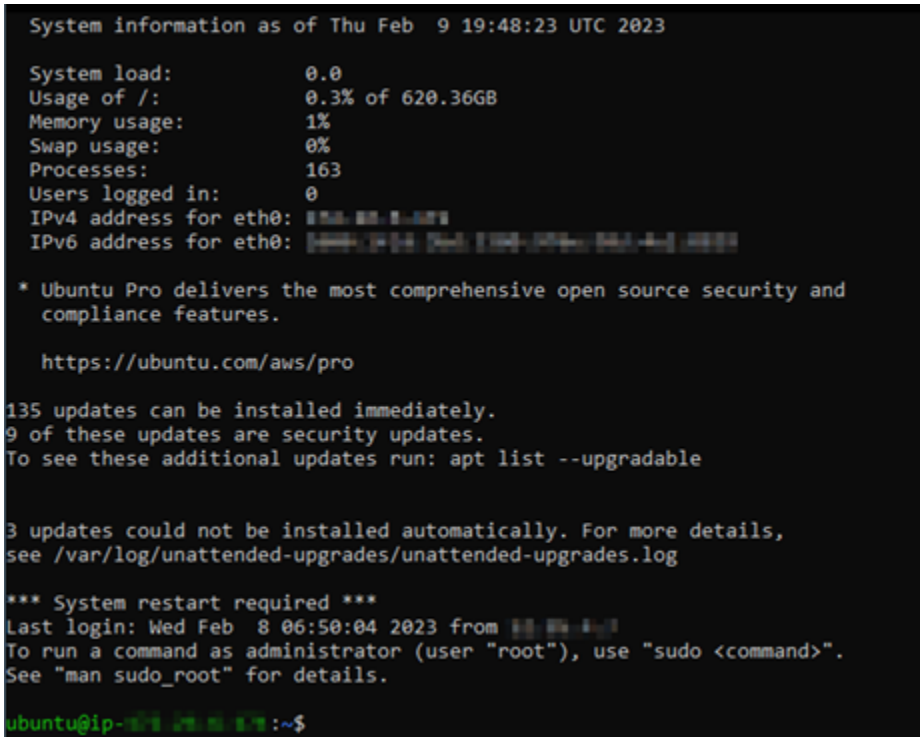
3. Enter the following command to establish an SSH connection with your virtual computer. In the command, replace *user-name* with the sign-in in username, and replace *public-ip-address* with the public IP address of your virtual computer.

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

Example

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

You should see a response similar to the following example, which shows an SSH connection established with an Ubuntu virtual computer in Lightsail for Research.



Now that you've successfully established an SSH connection to your virtual computer, continue to the next section for additional next steps.

Connect to a virtual computer using SSH on a Linux, Unix, or a macOS local computer

This procedure applies if your local computer uses a Linux, Unix, or a macOS operating system. This procedure uses the `get-instance` AWS CLI command to obtain the username and public IP address of the instance you want to connect to. For more information, see get-instance in the *AWS CLI Command Reference*.

> **Important**
>
> Make sure you get the Lightsail default key pair (DKP) for the virtual computer you're trying to connect to before you start this procedure. For more information, see Get a key pair for a virtual computer. That procedure outputs the private key of the Lightsail DKP to a `dkp_rsa` file that is used in one of the following commands.

1. Open a Terminal window.
2. Enter the following command to display the public IP address and username of your virtual computer. In the command, replace *`region-code`* with the code of the AWS Region in which

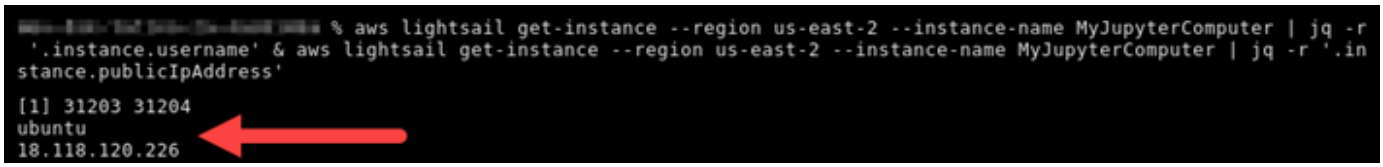
the virtual computer was created, such as `us-east-2`. Replace *computer-name* with the name of the virtual computer that you want to connect to.

```
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'
```

Example

```
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'
```

The response will display the username and public IP address of the virtual computer as shown in the following example. Note these values, because you need them in the following step of this procedure.



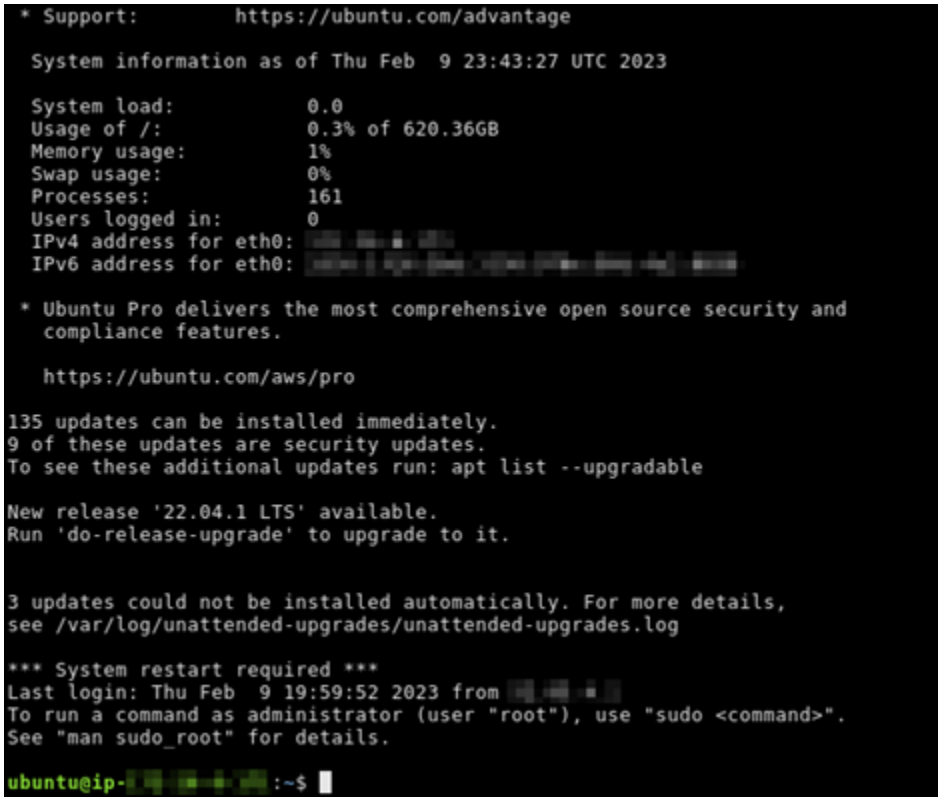
3. Enter the following command to establish an SSH connection with your virtual computer. In the command, replace *user-name* with the sign-in username, and replace *public-ip-address* with the public IP address of your virtual computer.

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

Example

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

You should see a response similar to the following example, which shows an SSH connection established with an Ubuntu virtual computer in Lightsail for Research.



Now that you've successfully established an SSH connection to your virtual computer, continue to the next section for additional next steps.

Continue to the next steps

You can complete the following additional next steps after you've successfully established an SSH connection to your virtual computer:

- Connect to your virtual computer using SCP to securely transfer files. For more information, see Transfer files to a virtual computer using Secure Copy.

Transfer files to a virtual computer using Secure Copy

You can transfer files from your local computer to a virtual computer in Amazon Lightsail for Research using Secure Copy (SCP). With this process, you can transfer multiple files, or entire directories, at one time.

> **Note**
>
> You can also establish a remote display protocol connection to your virtual computer using the browser-based NICE DCV client available in the Lightsail for Research console. With the NICE DCV client, you can quickly transfer individual files. For more information, see Access a virtual computer's operating system.

Topics

- Complete the prerequisites
- Connect to a virtual computer using SCP

Complete the prerequisites

Complete the following prerequisites before you get started.

- Create a virtual computer in Lightsail for Research. For more information, see Create a virtual computer.
- Make sure the virtual computer that you want to connect to is in a running state. Also, make note of the name of the virtual computer and the AWS Region in which it was created. You will need this information later in this process. For more information, see View virtual computer details.
- Download and install the AWS Command Line Interface (AWS CLI). For more information, see Installing or updating the latest version of the AWS CLI in the *AWS Command Line Interface User Guide for Version 2*.
- Configure the AWS CLI to access your AWS account. For more information, see Configuration basics in the *AWS Command Line Interface User Guide for Version 2*.
- Download and install jq. It's a lightweight and flexible command line JSON processor used in the following procedures to extract key pair details. For more information about downloading and installing jq, see Download jq on the *jq website*.
- Make sure that port 22 is open on the virtual computer you want to connect to. That is the default port used for SSH. It's open by default. But if you closed it, you must reopen it before continuing. For more information, see Manage firewall ports for virtual computers.
- Get the Lightsail default key pair (DKP) for your virtual computer. For more information, see Create a virtual computer.

Connect to a virtual computer using SCP

Complete one of the following procedures to connect to your virtual computer in Lightsail for Research using SCP.

Connect to a virtual computer using SCP on a Windows local computer

This procedure applies to you if your local computer uses a Windows operating system. This procedure uses the `get-instance` AWS CLI command to obtain the username and public IP address of the instance you want to connect to. For more information, see get-instance in the *AWS CLI Command Reference*.

> **Important**
>
> Make sure you get the Lightsail default key pair (DKP) for the virtual computer you're trying to connect to before you start this procedure. For more information, see Get a key pair for a virtual computer. That procedure outputs the private key of the Lightsail DKP to a `dkp_rsa` file that is used in one of the following commands.

1. Open a Command Prompt window.
2. Enter the following command to display the public IP address and username of your virtual computer. In the command, replace *`region-code`* with the code of the AWS Region in which the virtual computer was created, such as `us-east-2`. Replace *`computer-name`* with the name of the virtual computer that you want to connect to.

   ```
   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"
   ```

   Example

   ```
   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"
   ```

   The response will display the username and public IP address of the virtual computer as shown in the following example. Note these values, because you need them in the following step of this procedure.

```
C:\>aws lightsail get-instance --instance-name MyJupyterComputer --region us-east-2 | jq -r ".instance.username" & aws
lightsail get-instance --instance-name MyJupyterComputer --region us-east-2 | jq -r ".instance.publicIpAddress"
ubuntu
192.0.2.0
```

3. Enter the following command to establish an SCP connection with your virtual computer and transfer files to it.

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

In the command, replace:

- *source-folder* with the folder on your local computer that contains the files you want to transfer.
- *user-name* with the username from the previous step of this procedure (such as ubuntu).
- *public-ip-address* with the public IP address of your virtual computer from the previous step of this procedure.
- *destination-directory* with the path to the directory on the virtual computer where you want to copy your files.

The following example copies all files from the `C:\Files` folder on the local computer to the `/home/lightsail-user/Uploads/` directory on the remote virtual computer.

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

You should see a response similar to the following example. It shows each file that was transferred from the origin folder to the destination directory. You should now be able to access those files on your virtual computer.

```
C:\>scp -i dkp_rsa -r "C:\Files" ubuntu@192.0.2.0:/home/lightsail-user/Uploads/
myfile.txt                                    100%   11     0.2KB/s   00:00
myfile1.txt                                   100%    9     0.2KB/s   00:00
myfile10.txt                                  100%    7     0.1KB/s   00:00
myfile11.txt                                  100%    4     0.1KB/s   00:00
myfile12.txt                                  100%   13     0.2KB/s   00:00
myfile2.txt                                   100%   10     0.2KB/s   00:00
myfile3.txt                                   100%   10     0.2KB/s   00:00
myfile4.txt                                   100%    9     0.1KB/s   00:00
myfile5.txt                                   100%   10     0.2KB/s   00:00
myfile6.txt                                   100%   10     0.2KB/s   00:00
myfile7.txt                                   100%    8     0.1KB/s   00:00
myfile8.txt                                   100%    9     0.2KB/s   00:00
myfile9.txt                                   100%    9     0.2KB/s   00:00
```

Connect to a virtual computer using SCP on a Linux, Unix, or a macOS local computer

This procedure applies to you if your local computer uses a Linux, Unix, or a macOS operating system. This procedure uses the `get-instance` AWS CLI command to obtain the username and public IP address of the instance you want to connect to. For more information, see get-instance in the *AWS CLI Command Reference*.

> **Important**
>
> Make sure you get the Lightsail default key pair (DKP) for the virtual computer you're trying to connect to before you start this procedure. For more information, see Get a key pair for a virtual computer. That procedure outputs the private key of the Lightsail DKP to a `dkp_rsa` file that is used in one of the following commands.

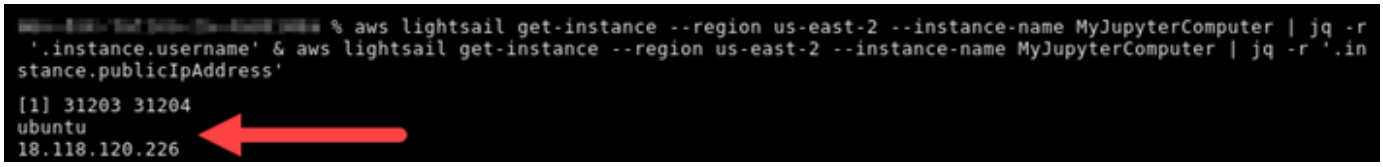
1. Open a Terminal window.
2. Enter the following command to display the public IP address and username of your virtual computer. In the command, replace *`region-code`* with the code of the AWS Region in which the virtual computer was created, such as `us-east-2`. Replace *`computer-name`* with the name of the virtual computer that you want to connect to.

```
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'
```

Example

```
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'
```

The response will display the username and public IP address of the virtual computer as shown in the following example. Note these values, because you need them in the following step of this procedure.



3. Enter the following command to establish an SCP connection with your virtual computer and transfer files to it.

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

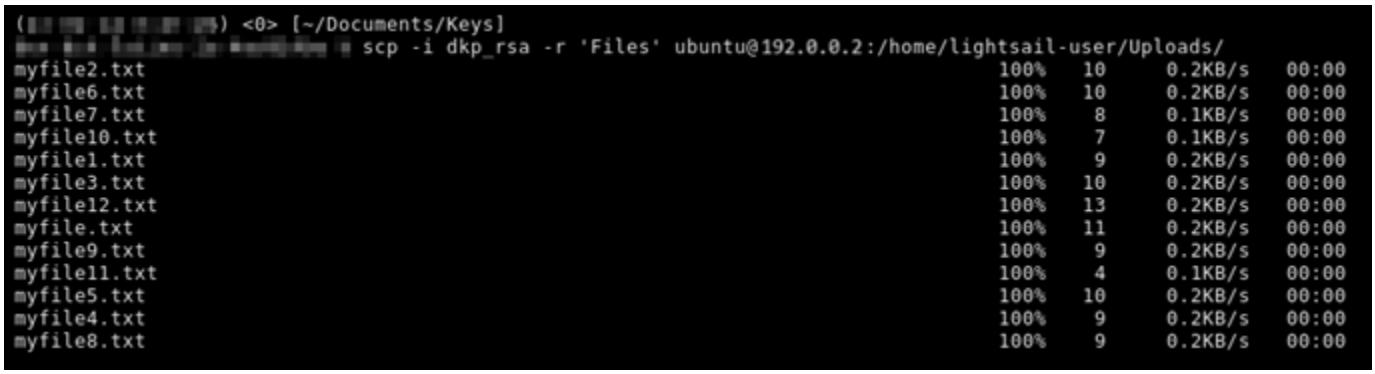
In the command, replace:

- *source-folder* with the folder on your local computer that contains the files you want to transfer.
- *user-name* with the username from the previous step of this procedure (such as ubuntu).
- *public-ip-address* with the public IP address of your virtual computer from the previous step of this procedure.
- *destination-directory* with the path to the directory on the virtual computer where you want to copy your files.

The following example copies all files from the C:\Files folder on the local computer to the /home/lightsail-user/Uploads/ directory on the remote virtual computer.

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

You should see a response similar to the following example. It shows each file that was transferred from the origin folder to the destination directory. You should now be able to access those files on your virtual computer.



Delete a virtual computer

Complete the following steps to delete your Lightsail for Research virtual computer when you no longer need it. You stop incurring charges for the virtual computer as soon as it's deleted. Resources that were attached to the deleted computer, such as snapshots, continue to incur charges until you delete them.

> **Important**
>
> Deleting a virtual computer is a permanent action, and the computer cannot be recovered. If you might need your data later, create a snapshot of your virtual computer before you delete it. For more information, see Create a snapshot.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane.
3. Choose the virtual computer to delete.
4. Choose **Actions**, then choose **Delete virtual computer**.
5. Type **confirm** in the text block. Then, choose **Delete virtual computer.**

Storage

Amazon Lightsail for Research provides block-level storage volumes (disks) that you can attach to a running Lightsail for Research virtual computer. You can use a disk as a primary storage device for data that requires frequent and granular updates. For example, disks are the recommended storage option when you run a database on a Lightsail for Research virtual computer.

A disk behaves like an unformatted external block device that you can attach to a single virtual computer. The volume persists independently from the running life of a computer. After you attach a disk to a computer, you can use it like any other physical hard drive.

You can attach multiple disks to a computer. You can also detach a disk from one computer and attach it to another computer.

To keep a backup copy of your data, create a snapshot of the disk. You can create a new disk from a snapshot and attach it to another computer.

Topics

- Create a disk
- View disks
- Attach a disk to a virtual computer
- Detach a disk from a virtual computer
- Delete a disk

Create a disk

Complete the following steps to create a disk for your Lightsail for Research virtual computer.

1. Sign in to the Lightsail for Research console.
2. Choose **Storage** in the navigation pane.
3. Choose **Create disk**.
4. Enter a name for your disk. Valid characters include alphanumeric characters, numbers, periods, hyphens, and underscores.

   Disk names must also meet the following requirements:

- Be unique within each AWS Region in your Lightsail for Research account.
- Contain 2–255 characters.
- Start and end with an alphanumeric character or number.

5. Choose an AWS Region for your disk.

   The disk must be in the same Region as the virtual computer that you will attach it to.
6. Choose your disk size in GB.
7. Continue to the Attach a disk section for information about attach disks to your virtual computer.

View disks

Complete the following steps to view the disks in your Lightsail for Research account and their details.

1. Sign in to the Lightsail for Research console.
2. Choose **Storage** in the navigation pane.

   The **Storage** page provides a comprehensive view of the disks in your Lightsail for Research account.

   The following information is displayed on the page:

   - **Name** – The name of your storage disk.
   - **Size** – The size of your disk (in GB).
   - **AWS Region** – The AWS Region your disk was created in.
   - **Attached to** – The Lightsail computer that your disk is attached to.
   - **Date created** – The date your disk was created.

Attach a disk to a virtual computer

Complete the following steps to attach a disk to a virtual computer in Lightsail for Research. You can attach up to 15 disks to a virtual computer. When you attach a disk to your virtual computer using the Lightsail for Research console, it is automatically formatted and mounted by the service. This process takes a few minutes, so you should confirm that the disk has reached a **Mounted**

mounting status before you start using it. By default, Lightsail for Research mounts disks to the `/home/lightsail-user/<disk-name>` directory; where *<disk-name>* is the name you gave your disk.

> **Important**
>
> Before you can attach a disk to a virtual computer, the virtual computer must be in a *Running* state. If you attach a disk to a virtual computer while it's in a *Stopped* state, the disk will be attached but fail to mount. If the disk's **Mount status** is *Failed*, you must detach the disk then reattach it when the virtual computer is in a *Running* state.

1. Sign in to the Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane.
3. Choose the computer to attach the disk to.
4. Choose the **Storage** tab.
5. Choose **Attach disk**.
6. Select the name of the disk to attach to the computer.
7. Choose **Attach**.

Detach a disk from a virtual computer

Complete the following steps to detach a disk from a computer.

1. Sign in to the Lightsail for Research console.
2. Choose **Storage** in the navigation pane.
3. Find the disk to detach. Under the **Attached to** column, choose the computer name that the disk is attached to.
4. Choose **Stop** to stop the computer. You must stop the computer before you can detach the disk.
5. Confirm you want to stop the computer, then choose **Stop computer computer**.
6. Choose the **Storage** tab.
7. Select the disk to detach, and then choose **Detach**.
8. Confirm that you want to detach your disk from the computer, then choose **Detach**.

Delete a disk

Complete the following steps to delete a storage disk when you don't need it anymore. You stop incurring charges for the disk as soon as it's deleted.

If the disk is attached to a computer, you must first detach it before you can delete it. For more information, see Detach a disk from a virtual computer.

1. Sign in to the Lightsail for Research console.
2. Choose **Storage** in the navigation pane.
3. Find and select the disk to delete.
4. Choose **Delete disk**.
5. Confirm that you want to delete your disk. Then, choose **Delete**.

Snapshots

Snapshots are a point-in-time copy of your data. You can create snapshots of your Amazon Lightsail for Research virtual computers and storage disks, and use them as baselines to create new computers or for data backup.

A snapshot contains all of the data that's needed to restore your computer (from the moment when the snapshot was taken). When you create a new virtual computer from a snapshot, it begins as an exact replica of the original computer that was used to create the snapshot.

Because your resources might fail at any time, we recommend creating frequent snapshots to avoid permanent data loss.

Topics

- Create a snapshot
- View snapshots
- Create a virtual computer or disk from a snapshot
- Delete a snapshot

Create a snapshot

Complete the following steps to create a snapshot of your Lightsail for Research virtual computer or disk.

1. Sign in to the Lightsail for Research console.
2. Choose **Snapshots** in the navigation pane.
3. Complete on of the following steps:

   - Under **Virtual computer snapshots**, find the name of the computer you want to snapshot and choose **Create snapshot**.
   - Under **Disk snapshots**, find the name of the disk you want to snapshot and choose **Create snapshot**.
4. Enter a name for your snapshot. Valid characters include alphanumeric characters, numbers, periods, hyphens, and underscores.

   Snapshot names must also meet the following requirements:

- Be unique within each AWS Region in your Lightsail for Research account.
- Contain 2–255 characters.
- Start and end with an alphanumeric character or number.

5. Choose **Create snapshot**.

View snapshots

Complete the following steps to view snapshots of your virtual computers and disks.

1. Sign in to the Lightsail for Research console.
2. Choose **Snapshots** in the navigation pane.

   The **Snapshots** page displays virtual computer and disk snapshots that you have created.

   Archived snapshots are located on this page as well. Archived snapshots are snapshots of resources that have been deleted from your account.

Create a virtual computer or disk from a snapshot

Complete the following steps to create a new Lightsail for Research virtual computer or disk from a snapshot.

When you create a virtual computer from a snapshot, use a plan that's the same size or larger than the one used for the original computer. You can't use a smaller plan than the original virtual computer.

When you create a disk from a snapshot, choose a disk size that's larger than the original disk. You can't use a smaller disk than the original.

1. Sign in to the Lightsail for Research console.
2. Choose **Snapshots** in the navigation pane.
3. On the **Snapshots** page, locate the name of the computer or disk snapshot you'll use for creating the new computer or disk. Choose the **Snapshots** dropdown menu to view a list of available snapshots for that resource.
4. Select the snapshot that you want to use to create the virtual computer.
5. Choose the **Actions** dropdown menu. Then, choose **Create virtual computer** or **Create disk**.

Delete a snapshot

Complete the following steps to delete a snapshot.

1. Sign in to the Lightsail for Research console.
2. Choose **Snapshots** in the navigation pane.
3. On the **Snapshots** page, locate the name of the computer or disk snapshot want to delete. Choose the **Snapshots** dropdown menu to view a list of available snapshots for that resource.
4. Select the snapshot that you want to delete.
5. Choose the **Actions** dropdown menu. Then, choose **Delete snapshot**.
6. Verify that the snapshot name is correct. Then, choose **Delete snapshot**.

Cost and usage estimates in Amazon Lightsail for Research

Amazon Lightsail for Research offers cost and usage estimates for your AWS resources. You can use these estimates to help you plan how you spend, find cost saving opportunities, and make informed decisions when using Lightsail for Research.

When you create a virtual computer or disk, cost and usage estimates are shown for that resource. A cost and usage estimate begins to track as soon as a resource is created, and is in an *Available* or *Running* state. The estimate will appear in the AWS Management Console within 15 minutes after the resource is created. Resources that have been deleted aren't included in an estimate.

Important

An estimate is an estimated cost that's based on the usage of the resource. Your actual cost will be based on the actual use of your resources, not the estimate that's shown in the Lightsail for Research console. The actual costs are shown on your AWS Billing account statement.
Sign in to the AWS Management Console and open the AWS Billing console at https://console.aws.amazon.com/billing/.

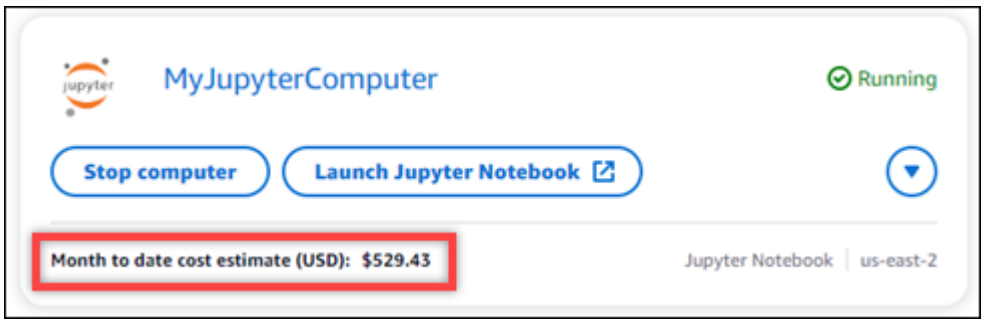
Topics

- Monitor cost and usage estimates.

Monitor cost and usage estimates.

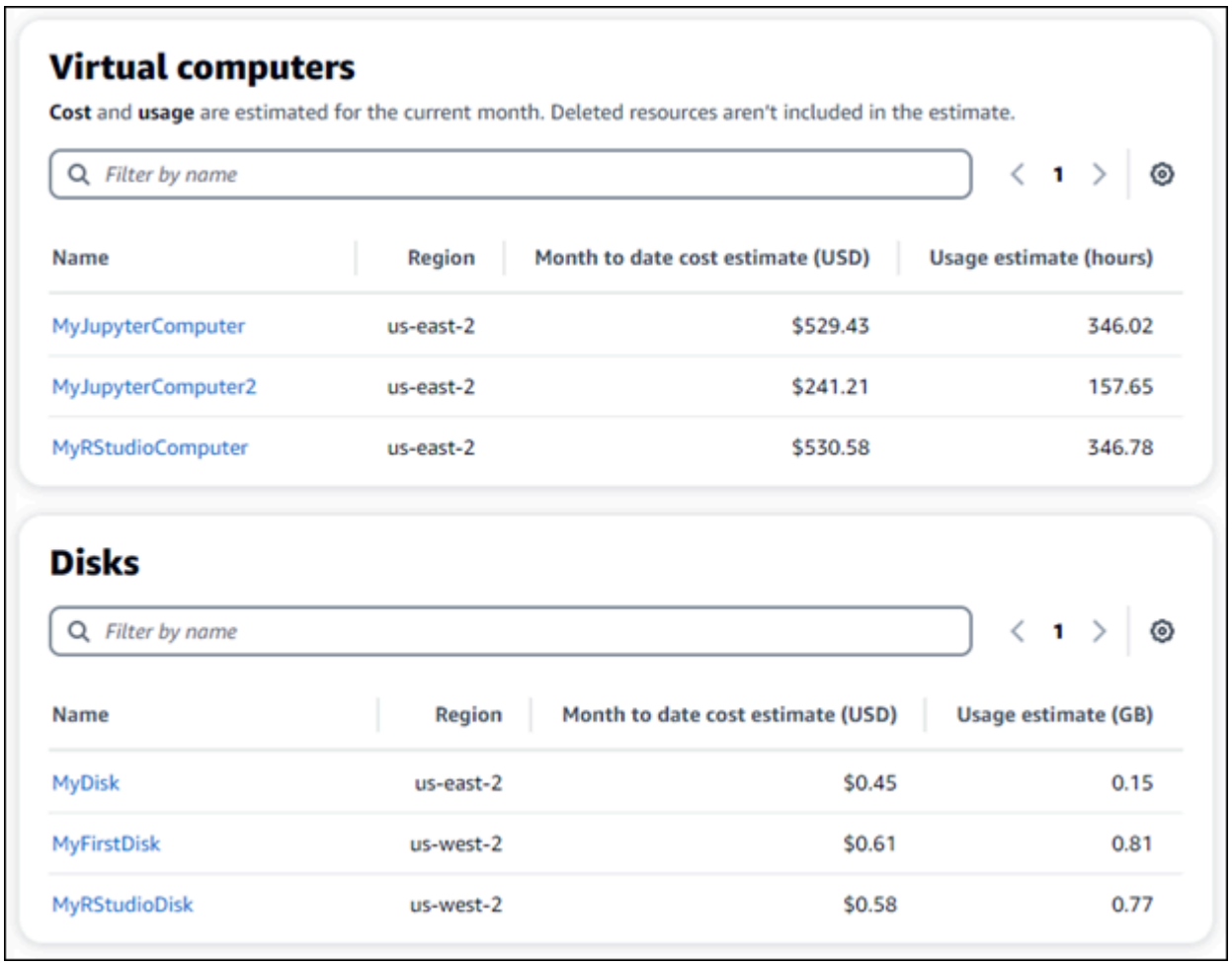
Month to date cost and usage estimates for your Lightsail for Research resources are displayed in the following areas of the Lightsail for Research console.

1. Choose **Virtual computers** in the navigation pane of the Lightsail for Research console. The month to date cost estimate for your virtual computers is listed under each running virtual computer.



2. To view the CPU utilization for a virtual computer, choose the name of the virtual computer, and then choose the **Dashboard** tab.

3. To view the month to date cost and usage estimates for all of your Lightsail for Research resources, choose **Usage** in the navigation pane.



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

Cost control

Cost control uses rules that you define to help manage the usage and cost of your Lightsail for Research virtual computers.

You can create a **Stop virtual computer on idle** rule that stops a running computer when it reaches a specified percentage of its CPU utilization during a given period. For example, a rule can automatically stop a specific computer when its CPU utilization is equal to or less than 5% during a 30-minute period. This signifies that the computer is idle, and Lightsail for Research stops the computer. You no longer incur the standard hourly charges after the virtual computer is stopped.

Topics

- Create a rule
- Delete a rule

Create a rule

Complete the following steps to create a rule for your Lightsail for Research virtual computer.

> **Note**
>
> The only supported rule action at this time is to stop a virtual computer. CPU utilization is the only metric currently monitored by rules, and the only supported operation is *less than or equal to*.

1. Sign in to the Lightsail for Research console.
2. Choose **Cost control** in the navigation pane.
3. Choose **Create rule**.
4. Select the resource to apply the rule to.
5. Specify the CPU utilization percentage and time period at which the rule should run.

   For example, you can specify 5 percent and 30 minutes. Lightsail for Research automatically stops the computer when its CPU utilization is less than or equal to 5 percent during a 30-minute period.

6. Choose **Create rule**.
7. Confirm that the information for your new rule is correct, and then choose **Confirm**.

Delete a rule

Complete the following steps to delete a rule for your Lightsail for Research virtual computer.

1. Sign in to the Lightsail for Research console.
2. Choose **Cost control** in the navigation pane.
3. Select the rule to delete.
4. Choose **Delete**.
5. Verify that you want to delete the rule, and choose **Delete**.

Tags

With Amazon Lightsail for Research, you can assign tags to your resources. Each tag is a label that consists of a **key** and an optional **value** that can make it efficient to manage your resources. A key without a value is referred to as a key-only tag, and a key with a value is referred to as a key-value tag. Although there are no inherent types of tags, they let you categorize your resources by purpose, owner, environment, or other criteria. This is useful when you have many resources of the same type. You can quickly identify a specific resource based on the tags you've assigned to it. For example, you can define a set of tags that help you track each resource's project, or priority.

The following resources can be tagged in the Amazon Lightsail for Research console:

- Virtual computers
- Storage disks
- Snapshots

The following restrictions apply to tags:

- The maximum number of tags per resource is 50.
- For each resource, each tag key must be unique. Each tag key can have only one value.
- The maximum **key** length is 128 Unicode characters in UTF-8.
- The maximum **value** length is 256 Unicode characters in UTF-8.
- If your tagging schema is used across multiple services and resources, remember that other services might have restrictions on allowed characters. Generally allowed characters are: letters, numbers, and spaces, and the following characters: `+ - = . _ : / @`
- Tag keys and values are case-sensitive.
- Don't use the `aws:` prefix for keys or values. That prefix is reserved for AWS use.

Topics

- Create a tag
- Delete a tag

Create a tag

Complete the following steps to create a tag for your Lightsail for Research virtual computer. The steps are similar for Lightsail for Research disks and snapshots.

1. Sign in to the Lightsail for Research console at Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane.
3. Choose the virtual computer that you want to create a tag for.
4. Choose the **Tags** tab.
5. Choose **Manage tags**.
6. Choose **Add new tag**.
7. Enter a key name into the **Key** field. For example, *Project*.
8. (Optional) Enter a value name into the **value** field. For example, *Blog*.
9. Choose **Save changes** to save the key to your virtual computer.

Delete a tag

Complete the following steps to delete a tag from your Lightsail for Research virtual computer. The steps are similar for Lightsail for Research disks and snapshots.

1. Sign in to the Lightsail for Research console at Lightsail for Research console.
2. Choose **Virtual computers** in the navigation pane.
3. Choose the virtual computer that you want to delete the tag from.
4. Choose the **Tags** tab.
5. Choose **Manage tags**.
6. Choose **Remove** to delete the tag from the resource.

> **Note**
>
> If you only want to remove the tag's **Value**, locate the value, then choose the X icon that's next to it.

7. Choose **Save changes**.

Security in Amazon Lightsail for Research

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from data centers and network architectures that are built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to Amazon Lightsail for Research, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Lightsail for Research. The following topics show you how to configure Lightsail for Research to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Lightsail for Research resources.

Topics

- Data protection in Amazon Lightsail for Research
- Identity and Access Management for Amazon Lightsail for Research
- Compliance validation for Amazon Lightsail for Research
- Resilience in Amazon Lightsail for Research
- Infrastructure security in Amazon Lightsail for Research
- Configuration and vulnerability analysis in Amazon Lightsail for Research
- Security best practices for Amazon Lightsail for Research

Data protection in Amazon Lightsail for Research

The AWS shared responsibility model applies to data protection in Amazon Lightsail for Research. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. You are also responsible for the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Lightsail for Research or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Identity and Access Management for Amazon Lightsail for Research

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Lightsail for Research resources. IAM is an AWS service that you can use with no additional charge.

> **Note**
>
> Amazon Lightsail and Lightsail for Research share the same IAM policy parameters. Changes made to Lightsail for Research policies will also affect Lightsail policies. For example, if a user has permission to create a disk in Lightsail for Research, that same user can create a disk in Lightsail, too.

Topics

- Audience
- Authenticating with identities
- Managing access using policies
- How Amazon Lightsail for Research works with IAM
- Identity-based policy examples for Amazon Lightsail for Research
- Troubleshooting Amazon Lightsail for Research identity and access

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Lightsail for Research.

Service user – If you use the Lightsail for Research service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Lightsail for Research features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If

you cannot access a feature in Lightsail for Research, see Troubleshooting Amazon Lightsail for Research identity and access.

Service administrator – If you're in charge of Lightsail for Research resources at your company, you probably have full access to Lightsail for Research. It's your job to determine which Lightsail for Research features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Lightsail for Research, see How Amazon Lightsail for Research works with IAM.

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Lightsail for Research. To view example Lightsail for Research identity-based policies that you can use in IAM, see Identity-based policy examples for Amazon Lightsail for Research.

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see How to sign in to your AWS account in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see Signing AWS API requests in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Multi-factor authentication in the

AWS IAM Identity Center User Guide and Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access AWS services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the AWS Directory Service, the Identity Center directory, or any user that accesses AWS services by using credentials provided through an identity source. When federated identities access AWS accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use AWS IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your AWS accounts and applications. For information about IAM Identity Center, see What is IAM Identity Center? in the *AWS IAM Identity Center User Guide*.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the *IAM User Guide*.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier

to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Creating a role for a third-party Identity Provider in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.

- **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.
- **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.
- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM role to grant permissions to applications running on Amazon EC2 instances in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see When to create an IAM role (instead of a user) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access control list (ACL) overview in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

How Amazon Lightsail for Research works with IAM

Before you use IAM to manage access to Lightsail for Research, learn what IAM features are available to use with Lightsail for Research.

IAM features you can use with Amazon Lightsail for Research

IAM feature	Lightsail for Research support
Identity-based policies	Yes
Resource-based policies	No
Policy actions	Yes
Policy resources	Yes
Policy condition keys (service-specific)	Yes
ACLs	No
ABAC (tags in policies)	Partial
Temporary credentials	Yes
Principal permissions	No
Service roles	No
Service-linked roles	No

To get a high-level view of how Lightsail for Research and other AWS services work with most IAM features, see AWS services that work with IAM in the *IAM User Guide*.

Identity-based policies for Lightsail for Research

Supports identity-based policies	Yes

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the *IAM User Guide*.

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. You can't specify the principal in an identity-based policy because it applies to the user or role to which it is attached. To learn about all of the elements that you can use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Identity-based policy examples for Lightsail for Research

To view examples of Lightsail for Research identity-based policies, see Identity-based policy examples for Amazon Lightsail for Research.

Resource-based policies within Lightsail for Research

Supports resource-based policies	No

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

To enable cross-account access, you can specify an entire account or IAM entities in another account as the principal in a resource-based policy. Adding a cross-account principal to a resource-based policy is only half of establishing the trust relationship. When the principal and the resource are in different AWS accounts, an IAM administrator in the trusted account must also grant

the principal entity (user or role) permission to access the resource. They grant permission by attaching an identity-based policy to the entity. However, if a resource-based policy grants access to a principal in the same account, no additional identity-based policy is required. For more information, see Cross account resource access in IAM in the *IAM User Guide*.

Policy actions for Lightsail for Research

Supports policy actions	Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

To see a list of Lightsail for Research actions, see Actions Defined by Amazon Lightsail for Research in the *Service Authorization Reference*.

Policy actions in Lightsail for Research use the following prefix before the action:

```
lightsail
```

To specify multiple actions in a single statement, separate them with commas.

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

To view examples of Lightsail for Research identity-based policies, see Identity-based policy examples for Amazon Lightsail for Research.

Policy resources for Lightsail for Research

Supports policy resources	Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

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

To see a list of Lightsail for Research resource types and their ARNs, see Resources Defined by Amazon Lightsail for Research in the *Service Authorization Reference*. To learn with which actions you can specify the ARN of each resource, see Actions Defined by Amazon Lightsail for Research .

To view examples of Lightsail for Research identity-based policies, see Identity-based policy examples for Amazon Lightsail for Research.

Policy condition keys for Lightsail for Research

Supports service-specific policy condition keys	Yes

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

To see a list of Lightsail for Research condition keys, see Condition Keys for Amazon Lightsail for Research in the *Service Authorization Reference*. To learn with which actions and resources you can use a condition key, see Actions Defined by Amazon Lightsail for Research .

To view examples of Lightsail for Research identity-based policies, see Identity-based policy examples for Amazon Lightsail for Research.

ACLs in Lightsail for Research

Supports ACLs	No

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

ABAC with Lightsail for Research

Supports ABAC (tags in policies)	Partial

Attribute-based access control (ABAC) is an authorization strategy that defines permissions based on attributes. In AWS, these attributes are called *tags*. You can attach tags to IAM entities (users or roles) and to many AWS resources. Tagging entities and resources is the first step of ABAC. Then you design ABAC policies to allow operations when the principal's tag matches the tag on the resource that they are trying to access.

ABAC is helpful in environments that are growing rapidly and helps with situations where policy management becomes cumbersome.

To control access based on tags, you provide tag information in the condition element of a policy using the `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

If a service supports all three condition keys for every resource type, then the value is **Yes** for the service. If a service supports all three condition keys for only some resource types, then the value is **Partial**.

For more information about ABAC, see What is ABAC? in the *IAM User Guide*. To view a tutorial with steps for setting up ABAC, see Use attribute-based access control (ABAC) in the *IAM User Guide*.

Using temporary credentials with Lightsail for Research

Supports temporary credentials	Yes

Some AWS services don't work when you sign in using temporary credentials. For additional information, including which AWS services work with temporary credentials, see AWS services that work with IAM in the *IAM User Guide*.

You are using temporary credentials if you sign in to the AWS Management Console using any method except a user name and password. For example, when you access AWS using your company's single sign-on (SSO) link, that process automatically creates temporary credentials. You also automatically create temporary credentials when you sign in to the console as a user and then switch roles. For more information about switching roles, see Switching to a role (console) in the *IAM User Guide*.

You can manually create temporary credentials using the AWS CLI or AWS API. You can then use those temporary credentials to access AWS. AWS recommends that you dynamically generate temporary credentials instead of using long-term access keys. For more information, see Temporary security credentials in IAM.

Cross-service principal permissions for Lightsail for Research

Supports forward access sessions (FAS)	No

When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.

Service roles for Lightsail for Research

Supports service roles	No

A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.

> **Warning**
>
> Changing the permissions for a service role might break Lightsail for Research functionality. Edit service roles only when Lightsail for Research provides guidance to do so.

Service-linked roles for Lightsail for Research

Supports service-linked roles	No

A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

For details about creating or managing service-linked roles, see AWS services that work with IAM. Find a service in the table that includes a `Yes` in the **Service-linked role** column. Choose the **Yes** link to view the service-linked role documentation for that service.

Identity-based policy examples for Amazon Lightsail for Research

By default, users and roles don't have permission to create or modify Lightsail for Research resources. They also can't perform tasks by using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS API. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

To learn how to create an IAM identity-based policy by using these example JSON policy documents, see Creating IAM policies in the *IAM User Guide*.

For details about actions and resource types defined by Lightsail for Research, including the format of the ARNs for each of the resource types, see Actions, Resources, and Condition Keys for Amazon Lightsail for Research in the *Service Authorization Reference*.

Topics

- Policy best practices
- Using the Lightsail for Research console
- Allow users to view their own permissions

Policy best practices

Identity-based policies determine whether someone can create, access, or delete Lightsail for Research resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see AWS managed policies or AWS managed policies for job functions in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see Policies and permissions in IAM in the *IAM User Guide*.

- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see IAM Access Analyzer policy validation in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see Configuring MFA-protected API access in the *IAM User Guide*.

For more information about best practices in IAM, see Security best practices in IAM in the *IAM User Guide*.

Using the Lightsail for Research console

To access the Amazon Lightsail for Research console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Lightsail for Research resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (users or roles) with that policy.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that they're trying to perform.

To ensure that users and roles can still use the Lightsail for Research console, also attach the Lightsail for Research `ConsoleAccess` or `ReadOnly` AWS managed policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*.

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "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": "*"
        }
    ]
}
```

Troubleshooting Amazon Lightsail for Research identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Lightsail for Research and IAM.

Topics

- I am not authorized to perform an action in Lightsail for Research
- I want to allow people outside of my AWS account to access my Lightsail for Research resources

I am not authorized to perform an action in Lightsail for Research

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *`my-example-widget`* resource but doesn't have the fictional `lightsail:`*`GetWidget`* permissions.

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

In this case, the policy for the `mateojackson` user must be updated to allow access to the *`my-example-widget`* resource by using the `lightsail:`*`GetWidget`* action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I want to allow people outside of my AWS account to access my Lightsail for Research resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Lightsail for Research supports these features, see How Amazon Lightsail for Research works with IAM.

- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see Cross account resource access in IAM in the *IAM User Guide*.

Compliance validation for Amazon Lightsail for Research

To learn whether an AWS service is within the scope of specific compliance programs, see AWS services in Scope by Compliance Program and choose the compliance program that you are interested in. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- Architecting for HIPAA Security and Compliance on Amazon Web Services – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

> **Note**
>
> Not all AWS services are HIPAA eligible. For more information, see the HIPAA Eligible Services Reference.

- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- AWS Customer Compliance Guides – Understand the shared responsibility model through the lens of compliance. The guides summarize the best practices for securing AWS services and map

the guidance to security controls across multiple frameworks (including National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), and International Organization for Standardization (ISO)).

- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see Security Hub controls reference.
- Amazon GuardDuty – This AWS service detects potential threats to your AWS accounts, workloads, containers, and data by monitoring your environment for suspicious and malicious activities. GuardDuty can help you address various compliance requirements, like PCI DSS, by meeting intrusion detection requirements mandated by certain compliance frameworks.
- AWS Audit Manager – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in Amazon Lightsail for Research

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

In addition to the AWS global infrastructure, Lightsail for Research offers several features to help support your data resiliency and backup needs. For more information, see Snapshots and Create a snapshot.

Infrastructure security in Amazon Lightsail for Research

As a managed service, Amazon Lightsail for Research is protected by the AWS global network security. For information about AWS security services and how AWS protects infrastructure, see

AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access Lightsail for Research through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Configuration and vulnerability analysis in Amazon Lightsail for Research

Configuration and IT controls are a shared responsibility between AWS and you, our customer. For more information, see the AWS shared responsibility model.

Security best practices for Amazon Lightsail for Research

Lightsail for Research provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don't represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

To prevent potential security events associated with your use of Lightsail for Research, follow these best practices:

- Access the Lightsail for Research console by authenticating to the AWS Management Console first. Don't share share your personal console credentials. Anyone on the internet can browse to the console, but they can't sign in or start a session unless they have valid credentials to the console.

Document history for the Lightsail for Research User Guide

The following table describes the documentation releases for Lightsail for Research.

Change	Description	Date
Initial release	Initial release of the *Lightsail for Research User Guide*.	February 28, 2023