Guía del usuario de

Amazon Lightsail para la investigación

Amazon Lightsail para la investigación: Guía del usuario de

Table of Contents

¿Qué es Amazon Lightsail for Research?

Con Amazon Lightsail for Research, los académicos e investigadores pueden crear potentes ordenadores virtuales en la nube de Amazon Web Services AWS(). Estos ordenadores virtuales vienen con aplicaciones de investigación preinstaladas, como RStudio Scilab.

Con Lightsail for Research, puede cargar datos directamente desde un navegador web para empezar a trabajar. Puede crear y eliminar sus equipos virtuales en cualquier momento, lo que le proporciona acceso bajo demanda a recursos de computación eficaces.

Solo paga durante el tiempo que necesite el equipo virtual. Lightsail for Research ofrece controles de presupuestación que pueden detener automáticamente el ordenador cuando alcanza un límite de coste preconfigurado, para que no tenga que preocuparse por los cargos por exceso de uso.

Todo lo que hace en la consola de Lightsail for Research está respaldado por una API disponible públicamente. Aprenda a instalar y usar la API AWS CLIy de Amazon Lightsail.

Precios

Con Lightsail for Research, solo paga por los recursos que cree y utilice. Para obtener más información, consulte los precios de Lightsail for Research.

Disponibilidad

Lightsail for Research está disponible en las AWS mismas regiones que Amazon Lightsail, con la excepción de la región EE.UU. Este (Norte de Virginia). Lightsail for Research también utiliza los mismos puntos finales que Lightsail. Para ver las AWS regiones y puntos de enlace de Lightsail compatibles actualmente, consulte Puntos de enlace y cuotas de Lightsail en la referencia general.AWS

Configuración de Amazon Lightsail para la investigación

Si es un AWS cliente nuevo, complete los requisitos previos de configuración que se indican en esta página antes de empezar a utilizar Amazon Lightsail for Research.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión Consola de administración de AWScomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Tutorial: Cómo empezar a utilizar los ordenadores virtuales Lightsail for Research

Utilice este tutorial para empezar a utilizar los ordenadores virtuales Amazon Lightsail for Research. Obtendrá información sobre cómo crear y usar un equipo virtual, además de cómo conectarse. En Lightsail for Research, una computadora virtual es una estación de trabajo de investigación que se crea y administra en el. Nube de AWS Los ordenadores virtuales se basan en instancias de Lightsail Linux con el sistema operativo Ubuntu. En su computadora virtual, puede preconfigurar una aplicación de investigación como JupyterLab Scilab RStudio y más.

El equipo virtual que cree en este tutorial incurrirá en tarifas de uso desde el momento en que lo cree hasta que lo elimine. La eliminación es el último paso de este tutorial. Para obtener más información sobre los precios, consulte los precios de Lightsail for Research.

Temas

Paso 1: completar los requisitos previos

Si es un AWS cliente nuevo, complete los requisitos previos de configuración antes de empezar a utilizar Amazon Lightsail for Research. Para obtener más información, consulte Configuración de Amazon Lightsail para la investigación.

Paso 2: crear un equipo virtual

Puede crear un ordenador virtual mediante la consola Lightsail for Research, tal y como se describe en el siguiente procedimiento. Este tutorial tiene por objetivo brindarle ayuda para lanzar su primer

equipo virtual rápidamente. También recomendamos explorar las aplicaciones y los planes de hardware disponibles. Para obtener más información, consulte Elija imágenes de aplicaciones y planes de hardware para Lightsail for Research y Cree un ordenador virtual Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research.
2. En la página de inicio, seleccione Crear equipo virtual.
3. Seleccione una Región de AWS para su computadora virtual.

   Elija el Región de AWS que esté más cerca de su ubicación física para reducir la latencia.
4. Elija una aplicación, también conocida como plano en la API de Lightsail.

   La aplicación que elija se instalará y configurará en su equipo virtual al crearlo.
5. Elija un plan de hardware, también conocido como paquete en la API de Lightsail.

   Los planes de hardware ofrecen diferentes cantidades de potencia de procesamiento, incluidos los núcleos de vCPU, la memoria, el almacenamiento y la transferencia mensual de datos. Lightsail for Research ofrece planes estándar y planes de GPU para ordenadores virtuales. Elija un plan estándar cuando el requisito de computación de su trabajo sea bajo. Elija un plan de GPU cuando ese requisito sea elevado, por ejemplo, cuando ejecute modelos de machine learning u otras tareas con un uso intensivo de computación.
6. Escriba un nombre para el equipo virtual.
7. Seleccione Crear equipo virtual en el panel Resumen.

Una vez que su nuevo equipo virtual esté en funcionamiento, continúe con el siguiente paso de este tutorial para obtener información sobre cómo lanzar la aplicación del equipo.

Paso 3: lanzar la aplicación de un equipo virtual

Cuando cree un equipo virtual y este se encuentre en estado En ejecución, puede lanzar una sesión virtual en su navegador web. Con la sesión, puede interactuar con la aplicación que está instalada en su equipo virtual y administrarla.

1. Seleccione Ordenadores virtuales en el panel de navegación de la consola de Lightsail for Research.
2. Busque el nombre del equipo virtual que creó en el paso 1 y elija Lanzar aplicación. Por ejemplo, Launch. JupyterLab Se abre una sesión de aplicación en una nueva ventana del navegador web.

> **Important**
>
> Si el navegador web tiene instalado un bloqueador de ventanas emergentes, puede que tenga que permitir las ventanas emergentes del dominio aws.amazon.com antes de abrir la sesión.

Para obtener información sobre cómo conectarse al equipo virtual, continúe con el siguiente paso de este tutorial.

Paso 4: conectarse al equipo virtual

Puede conectarse al equipo virtual con los siguientes métodos:

- Utilice el cliente Amazon DCV basado en navegador disponible en la consola Lightsail for Research. Con Amazon DCV, puede utilizar una interfaz gráfica de usuario (GUI) para interactuar con la aplicación de investigación y el sistema operativo de su ordenador virtual.

  También puede acceder a la interfaz de línea de comandos de su ordenador virtual y transferir archivos mediante el cliente Amazon DCV basado en navegador.
- Utilice un cliente de Secure Shell (SSH), como OpenSSH, PuTTY o el Subsistema de Windows para Linux, para acceder a la interfaz de línea de comandos de su equipo virtual. Con un cliente de SSH, puede editar scripts y archivos de configuración.
- Utilice Secure Copy (SCP) para transferir archivos de forma segura entre el equipo local y el equipo virtual. Con SCP, puede empezar su trabajo de forma local y continuarlo en su equipo virtual. También puede descargar archivos de su equipo virtual para copiar el trabajo en su equipo local.

Debe proporcionar el par de claves de su equipo virtual para conectarse a este mediante SSH o para transferir archivos mediante SCP. Un key pair es un conjunto de credenciales de seguridad que se utilizan para demostrar su identidad al conectarse a un ordenador virtual de Lightsail for Research. Un par de claves consta de una clave pública y una clave privada.

Para obtener más información sobre la conexión al equipo virtual, consulte la siguiente documentación:

- Establezca una conexión de protocolo de pantalla remota:

  - Acceda a una aplicación informática virtual de Lightsail for Research
  - Acceda al sistema operativo de su ordenador virtual Lightsail for Research
- Establezca una conexión SSH o transfiera archivos mediante SCP:
  - Obtenga un par de claves para un ordenador virtual Lightsail for Research
  - Connect a un ordenador virtual de Lightsail for Research mediante Secure Shell
  - Transfiera archivos a ordenadores virtuales de Lightsail for Research mediante Secure Copy

Para obtener más información sobre el almacenamiento de su equipo virtual, continúe con el siguiente paso de este tutorial.

Paso 5: agregar almacenamiento al equipo virtual

Lightsail for Research proporciona volúmenes de almacenamiento a nivel de bloque (discos) que puede conectar a un ordenador virtual. Aunque el equipo virtual incluye un disco de sistema, puede adjuntar discos adicionales al equipo virtual según vayan cambiando sus necesidades de almacenamiento. También puede desasociar un disco de un equipo virtual y adjuntarlo a otro equipo virtual.

Al conectar un disco al ordenador virtual mediante la consola, Lightsail for Research formatea y monta automáticamente el disco en el sistema operativo. Este proceso tarda unos minutos, por lo que debe confirmar que el disco se encuentra en estado Montado antes de empezar a usarlo.

Para obtener más información acerca de cómo se crea, adjunta y administra un disco, consulte la siguiente documentación:

- Cree un disco de almacenamiento en la consola de Lightsail for Research
- Vea los detalles del disco de almacenamiento en la consola de Lightsail for Research
- Añada almacenamiento a un ordenador virtual en Lightsail for Research
- Separe un disco de un ordenador virtual en Lightsail for Research
- Elimine los discos de almacenamiento no utilizados en Lightsail for Research

Para obtener más información sobre cómo hacer una copia de seguridad de su equipo virtual, continúe con el siguiente paso de este tutorial.

Paso 6: crear una instantánea

Las instantáneas son una point-in-time copia de sus datos. Puede crear instantáneas de sus equipos virtuales y utilizarlas como puntos de referencia para crear nuevos equipos o para realizar copias de seguridad de los datos. Una instantánea contiene todos los datos necesarios para restaurar el equipo (desde el momento en que se hizo la instantánea).

Para obtener más información acerca de cómo crear y administrar instantáneas, consulte la siguiente documentación:

- Cree instantáneas de ordenadores o discos virtuales de Lightsail for Research
- Vea y gestione instantáneas de ordenadores y discos virtuales en Lightsail for Research
- Creación de un equipo virtual o un disco a partir de una instantánea
- Eliminar una instantánea en la consola de Lightsail for Research

Para obtener más información sobre la limpieza de los recursos de su equipo virtual, continúe con el siguiente paso de este tutorial.

Paso 7: limpiar

Cuando haya acabado con el equipo virtual que creó para este tutorial, puede eliminarlo. Así dejará de incurrir en cargos por el equipo virtual si no lo necesita.

Al eliminar un equipo virtual, no se eliminan las instantáneas ni los discos adjuntos asociados. Si ha creado instantáneas y discos, debe eliminarlos manualmente para que no se le cobre nada por ellos.

Si quiere guardar el equipo virtual para más adelante, pero evitar incurrir en cargos con los precios por hora estándar, puede detener el equipo virtual en lugar de eliminarlo. A continuación, podrá volver a iniciarlo más adelante. Para obtener más información, consulte Ver detalles de la computadora virtual de Lightsail for Research. Para obtener más información sobre los precios, consulte los precios de Lightsail for Research.

> **Important**
>
> Eliminar un recurso de Lightsail for Research es una acción permanente. Los datos eliminados no se pueden recuperar. Si necesita los datos más adelante, cree una

instantánea del equipo virtual antes de eliminarlo. Para obtener más información, consulte Create a snapshot.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Equipos virtuales.
3. Elija el equipo virtual que desea eliminar.
4. Seleccione Acciones y, a continuación, elija Eliminar equipo virtual.
5. Escriba confirmar en el bloque de texto. A continuación, elija Eliminar equipo virtual.

Comience con las aplicaciones de ciencia de datos en Lightsail for Research

Los siguientes tutoriales proporcionan información adicional sobre cómo empezar a utilizar aplicaciones específicas que están disponibles en Lightsail for Research.

Temas

> **Note**
>
> Se ha publicado un tutorial detallado para empezar a utilizar Lightsail for Research RStudio en el blog AWS del sector público. Para obtener más información, consulte Introducción a Amazon Lightsail for Research: un tutorial sobre el uso. RStudio

Lanzamiento y uso JupyterLab en Lightsail for Research

En este tutorial, le mostramos cómo empezar a gestionar y utilizar su ordenador JupyterLab virtual en Amazon Lightsail for Research.

Temas

Paso 1: completar los requisitos previos

Cree un ordenador virtual con la JupyterLab aplicación si aún no lo ha hecho. Para obtener más información, consulte Cree un ordenador virtual Lightsail for Research.

Una vez que su nueva computadora virtual esté en funcionamiento, continúe con la sección de inicio de la JupyterLab aplicación de este tutorial.

Paso 2: (opcional) agregar espacio de almacenamiento

El equipo virtual viene con un disco del sistema. Sin embargo, a medida que cambien sus necesidades de almacenamiento, puede adjuntar discos adicionales al equipo virtual para aumentar su espacio de almacenamiento.

También puede almacenar los archivos de trabajo en un disco adjunto. A continuación, puede separar el disco y adjuntarlo a un equipo virtual diferente para mover rápidamente los archivos de un equipo a otro.

Como alternativa, puede crear una instantánea de un disco adjunto que contenga los archivos de trabajo y, a continuación, crear un disco duplicado a partir de la instantánea. A continuación, puede adjuntar el nuevo disco duplicado a otro equipo para duplicar su trabajo en distintos equipos virtuales. Para obtener más información, consulte Cree un disco de almacenamiento en la consola de Lightsail for Research y Añada almacenamiento a un ordenador virtual en Lightsail for Research.

> **Note**
>
> Al conectar un disco a su ordenador virtual mediante la consola, Lightsail for Research formatea y monta automáticamente el disco. Este proceso tarda unos minutos, por lo que debe confirmar que el disco ha alcanzado el estado de montaje Montado antes de empezar a usarlo. De forma predeterminada, Lightsail for Research monta los discos en el directorio. `/home/lightsail-user/<disk-name>` `<disk-name>`es el nombre que le dio al disco.

Paso 3: cargar y descargar archivos

Puede cargar archivos a su ordenador JupyterLab virtual y descargarlos desde él. Para ello, debe completar los siguientes pasos:

1. Obtenga un key pair de Amazon Lightsail. Para obtener más información, consulte Obtenga un par de claves para un ordenador virtual Lightsail for Research.

2. Una vez que tenga el par de claves, puede usarlo para establecer una conexión mediante la utilidad Secure Copy (SCP). SCP le permite cargar y descargar archivos mediante el símbolo del sistema o el terminal. Para obtener más información, consulte Transfiera archivos a ordenadores virtuales de Lightsail for Research mediante Secure Copy.
3. (Opcional) También puede usar el par de claves para conectarse a su equipo virtual mediante SSH. Para obtener más información, consulte Connect a un ordenador virtual de Lightsail for Research mediante Secure Shell.

> **Note**
>
> También puede acceder a la interfaz de línea de comandos de su ordenador virtual y transferir archivos mediante el cliente Amazon DCV basado en navegador. Amazon DCV está disponible en la consola Lightsail for Research. Para obtener más información, consulte Acceda a una aplicación informática virtual de Lightsail for Research y Acceda al sistema operativo de su ordenador virtual Lightsail for Research.

Para administrar los archivos del proyecto en un disco de almacenamiento adjunto, asegúrese de cargarlos en el directorio de montaje correcto para el disco adjunto. Al conectar un disco a su ordenador virtual mediante la consola, Lightsail for Research formatea y monta automáticamente el disco en el directorio. `/home/lightsail-user/<disk-name>` `<disk-name>`es el nombre que le dio al disco.

Paso 4: inicia la JupyterLab aplicación

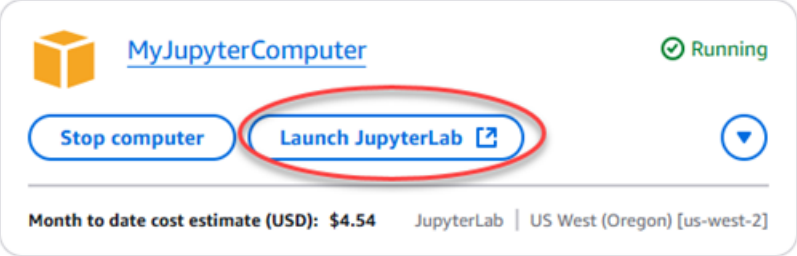
Complete el siguiente procedimiento para iniciar la JupyterLab aplicación en su nueva computadora virtual.

> **Important**
>
> No actualice el sistema operativo ni la JupyterLab aplicación aunque se le pida que lo haga. En su lugar, elija la opción de cerrar o ignorar esas indicaciones. Además, no modifique ninguno de los archivos que se encuentran en el directorio /home/lightsail-admin/. Estas acciones pueden inutilizar el equipo virtual.

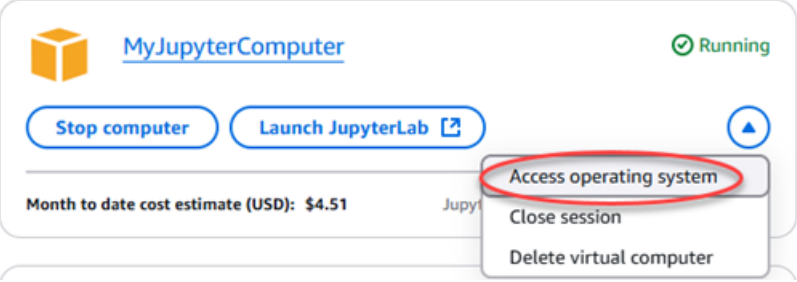
1. Inicie sesión en la consola de Lightsail for Research.

2. Elija Equipos virtuales en el panel de navegación para ver los equipos virtuales que están disponibles en la cuenta.
3. En la página Equipos virtuales, busque su equipo virtual y elija una de las siguientes opciones para conectarse a él:

   a. (Recomendado) Elija Launch JupyterLab para iniciar la JupyterLab aplicación en modo enfocado. Si no se ha conectado a su ordenador virtual recientemente, puede que tenga que esperar unos minutos mientras Lightsail for Research prepara la sesión.



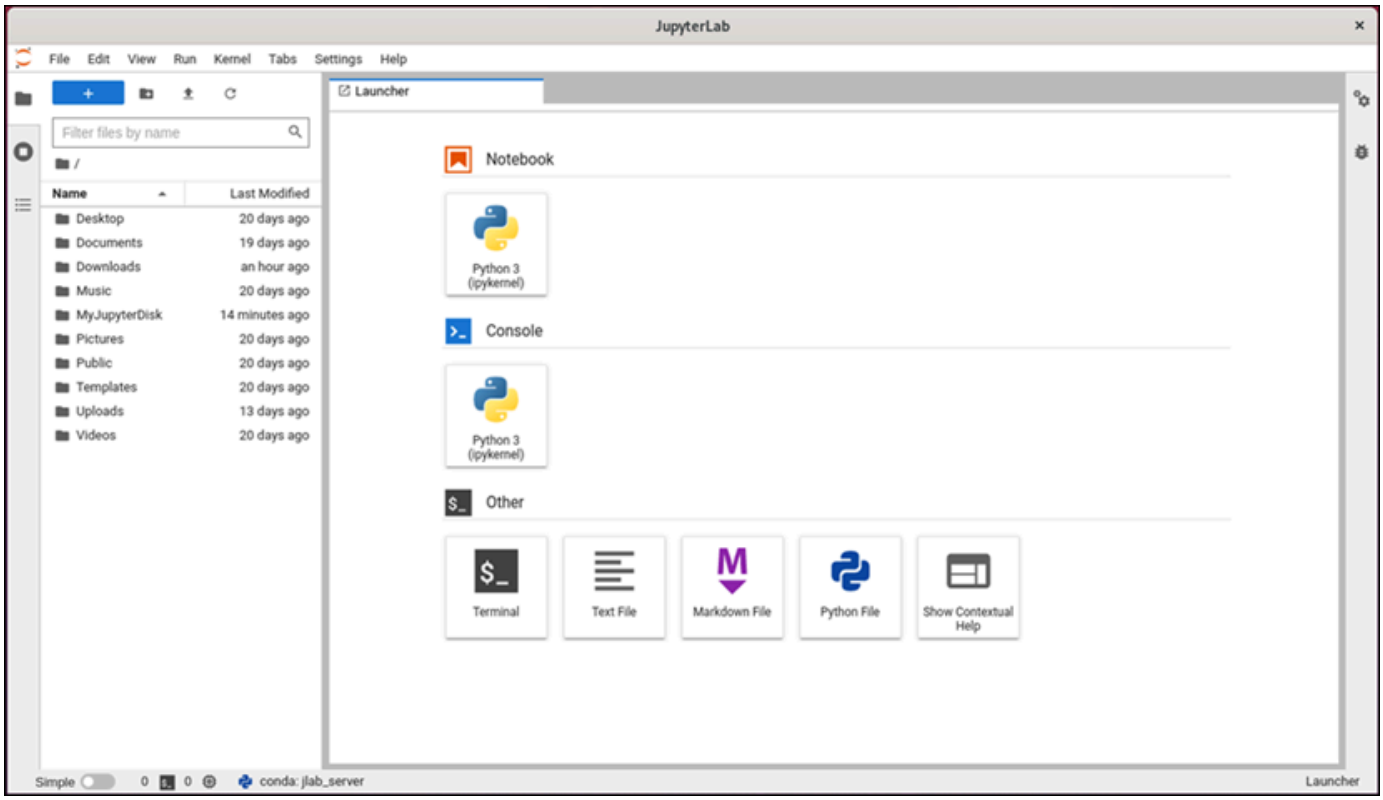
   b. Seleccione el menú desplegable del equipo y, a continuación, seleccione Acceso al sistema operativo para acceder al escritorio del equipo virtual.



Lightsail for Research ejecuta algunos comandos para iniciar la conexión del protocolo de pantalla remota. Tras unos instantes, se abre una nueva ventana de pestañas del navegador con una conexión de escritorio virtual establecida con su equipo virtual. Si eligió la opción Iniciar aplicación, continúe con el siguiente paso de este procedimiento para abrir un archivo en la JupyterLab aplicación. Si ha elegido la opción Acceso al sistema operativo, puede abrir otras aplicaciones a través del escritorio de Ubuntu.

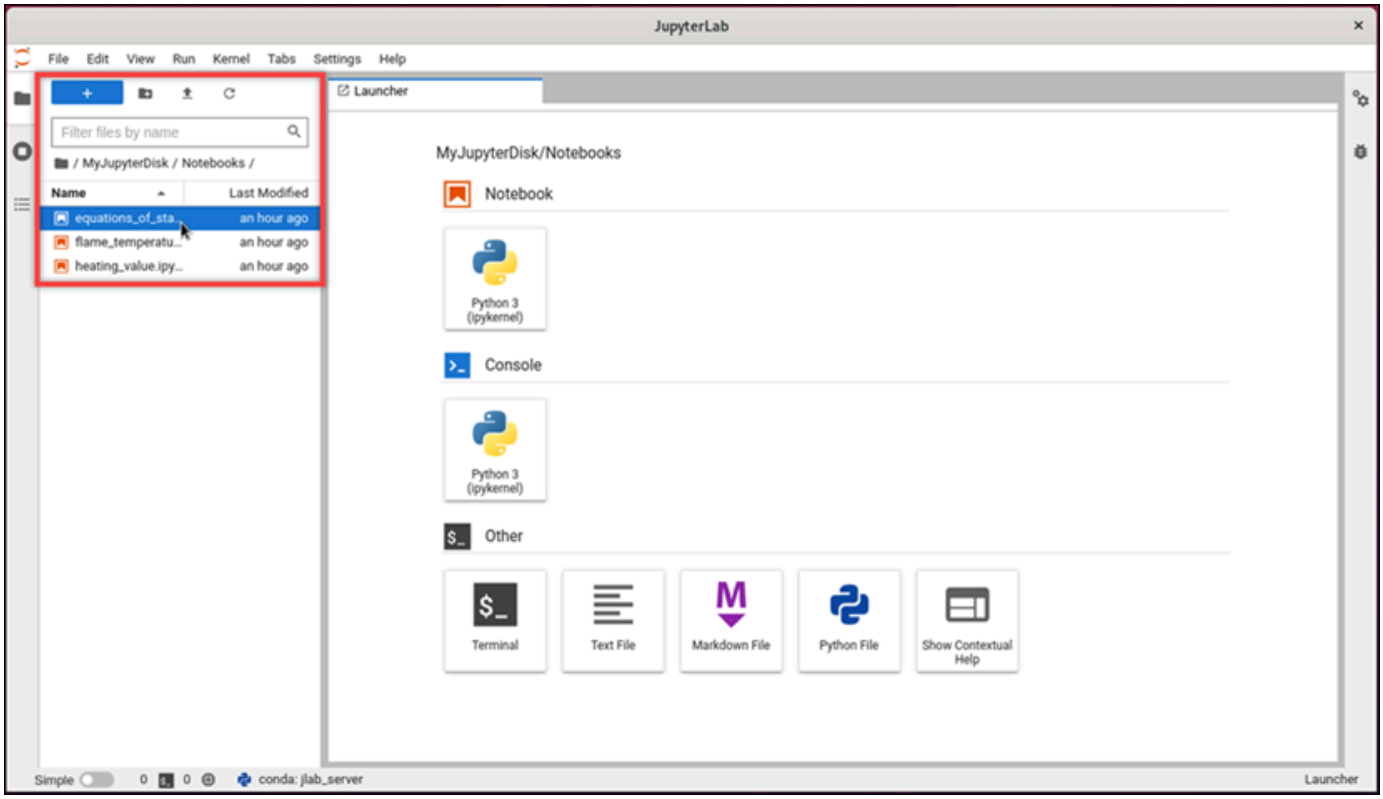
> **Note**
>
> Es posible que su navegador le pida que autorice el uso compartido del portapapeles. Si lo permite, podrá copiar y pegar entre el equipo local y el equipo virtual.
> Es posible que Ubuntu también le pida una configuración inicial. Siga las instrucciones hasta que complete la configuración y pueda usar el sistema operativo.

4. Se abre JupyterLab la aplicación. En el menú del lanzador, puede crear un nuevo cuaderno, lanzar la consola, lanzar el terminal y crear varios archivos.

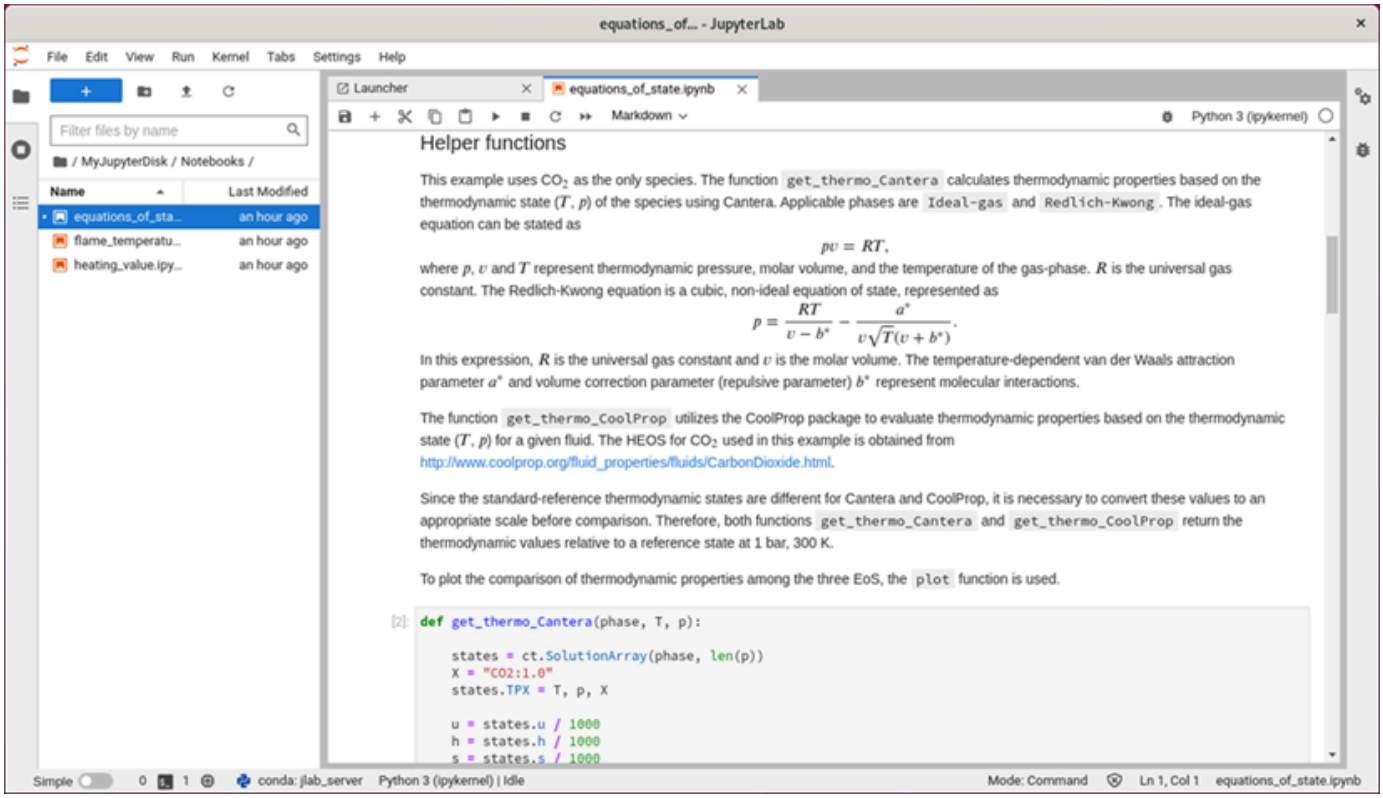


5. Para abrir un archivo JupyterLab, en el panel del explorador de archivos, elija el directorio o la carpeta donde se almacenan los archivos del proyecto. A continuación, elija el archivo para abrirlo.

   Si ha cargado los archivos del proyecto en un disco adjunto, busque el directorio en el que está montado el disco. De forma predeterminada, Lightsail for Research monta los discos en el directorio. `/home/lightsail-user/<disk-name>` `<disk-name>`es el nombre que le dio al disco. En el siguiente ejemplo, el directorio `MyJupyterDisk` representa el disco montado y el subdirectorio `Notebooks` contiene los archivos de nuestro cuaderno de Jupyter.



En el siguiente ejemplo, hemos abierto el archivo del cuaderno de Jupyter `equations_of_state.ipynb`.



Para obtener información sobre cómo comenzar, continúe con la sección Paso 5: Lea la JupyterLab documentación de este tutorial.

Paso 5: Lea la JupyterLab documentación

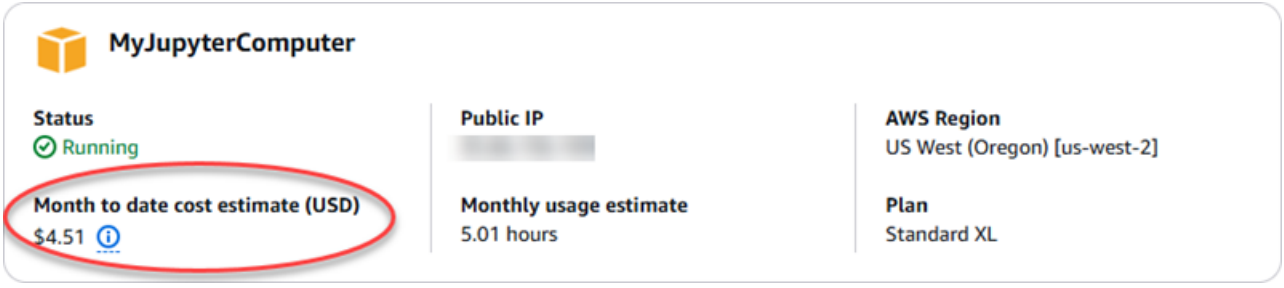
Si no está familiarizado con ellos JupyterLab, le recomendamos que lea su documentación oficial. Están disponibles los siguientes recursos JupyterLab en línea:

- Documentación de JupyterLab
- Jupyter Discourse Forum
- JupyterLab en StackOverflow
- JupyterLab en GitHub

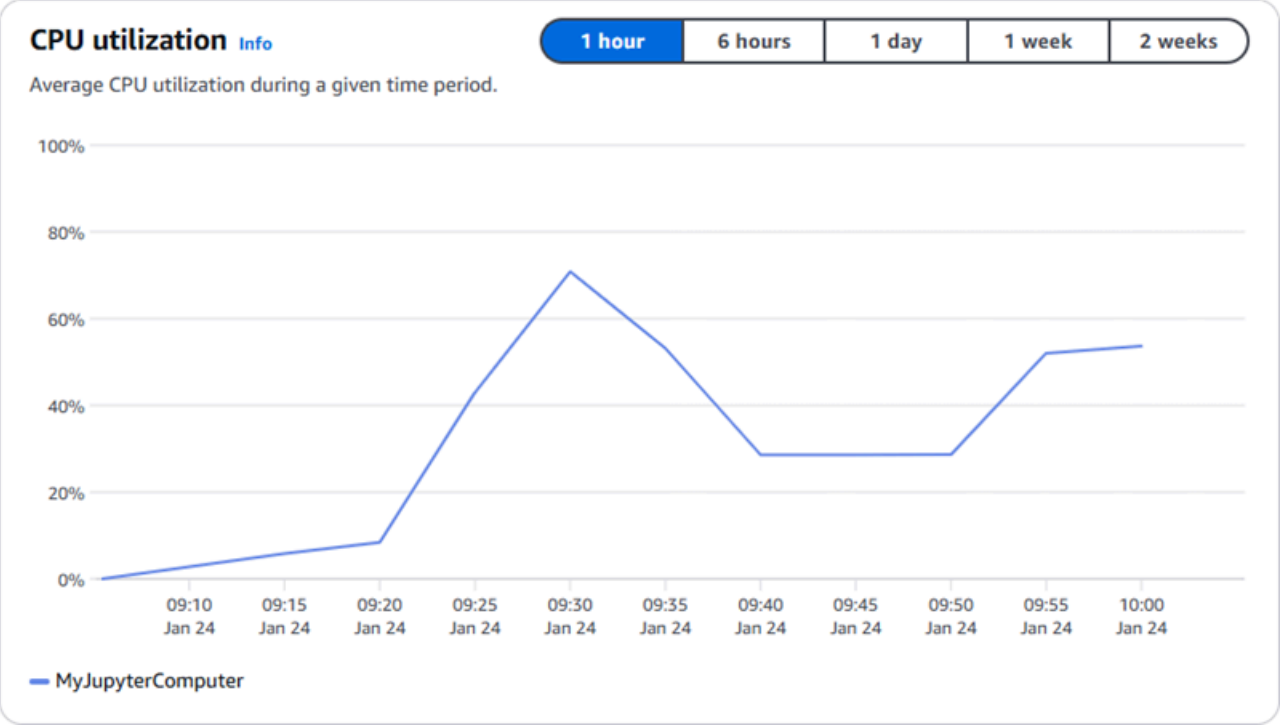
Paso 6: (opcional) supervisar el uso y los costos

Las estimaciones de coste y uso mensuales de sus recursos de Lightsail for Research se muestran en las siguientes áreas de la consola de Lightsail for Research.

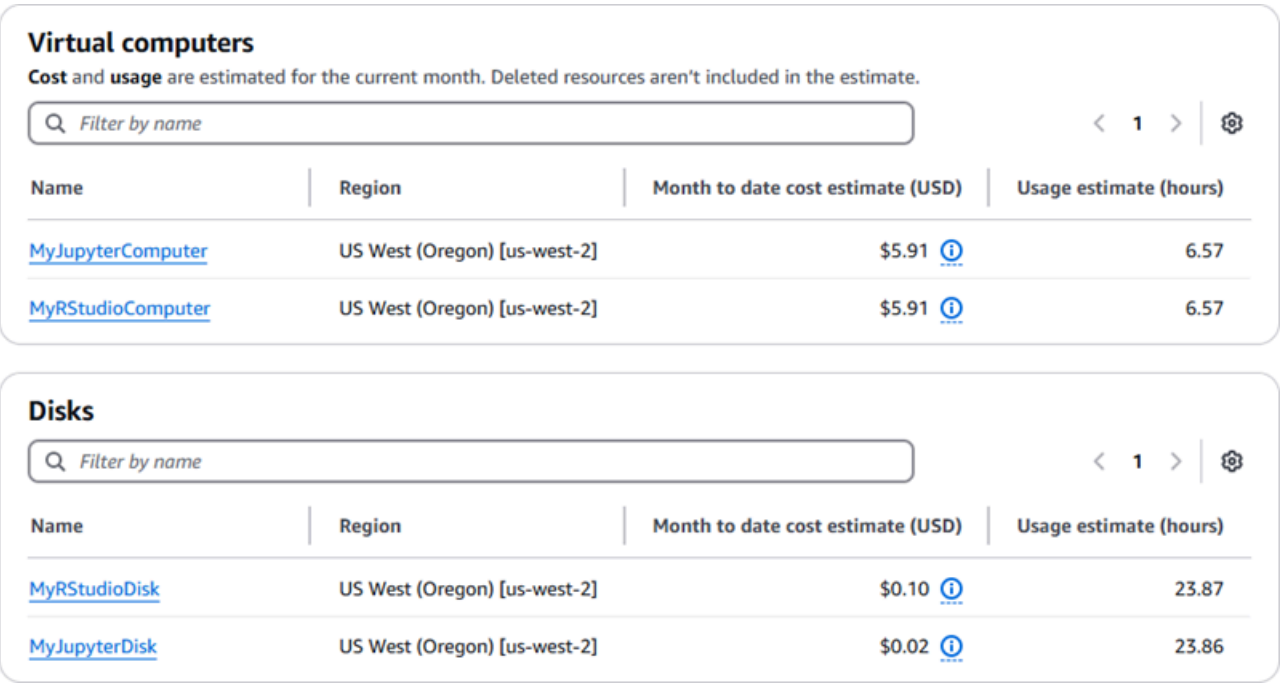
1. Seleccione Ordenadores virtuales en el panel de navegación de la consola de Lightsail for Research. La estimación del costo mensual de sus equipos virtuales hasta la fecha aparece debajo de cada equipo virtual en ejecución.



2. Para ver el uso de la CPU de un equipo virtual, elija el nombre del equipo virtual y, a continuación, elija la pestaña Panel.



3. Para ver las estimaciones de costo y uso del mes hasta la fecha de todos sus recursos de Lightsail for Research, seleccione Uso en el panel de navegación.



Paso 7: (opcional) crear una regla de control de costos

Administre el uso y el costo de sus equipos virtuales mediante la creación de reglas de control de costos. Puede crear una regla Detener el equipo virtual inactivo que detenga un equipo en ejecución cuando alcance un porcentaje específico de uso de la CPU durante un periodo determinado. Por ejemplo, una regla puede detener automáticamente un equipo específico cuando el uso de la CPU es igual o inferior al 5 % durante un periodo de 30 minutos. Esto puede significar que el equipo está inactivo y Lightsail for Research lo detiene para que no se le cobre por un recurso inactivo.

> **Important**
>
> Antes de crear una regla para detener el equipo virtual inactivo, le recomendamos que supervise el uso de la CPU durante unos días. Tome nota del uso de la CPU mientras el equipo virtual esté sometido a diferentes cargas. Por ejemplo, cuando compila código, procesa una operación y está inactivo. Esto lo ayudará a determinar un umbral preciso para la regla. Para obtener más información, consulte la sección Paso 6: (opcional) supervisar el uso y los costos de este tutorial.
>
> Si crea una regla con un umbral de uso de la CPU superior a su carga de trabajo, la regla puede detener el equipo virtual de forma consecutiva. Por ejemplo, si inicia el equipo virtual inmediatamente después de que una regla lo detenga, la regla se reactiva y el equipo se detiene de nuevo.

Las instrucciones detalladas para crear y administrar las reglas de control de costos se encuentran en las siguientes guías:

- Gestione las reglas de control de costes en Lightsail for Research
- Cree reglas de control de costes para sus ordenadores virtuales Lightsail for Research
- Elimine las reglas de control de costes de sus ordenadores virtuales Lightsail for Research

Paso 8: (opcional) crear una instantánea

Las instantáneas son una point-in-time copia de sus datos. Puede crear instantáneas de sus equipos virtuales y utilizarlas como puntos de referencia para crear nuevos equipos o para realizar copias de seguridad de los datos. Una instantánea contiene todos los datos necesarios para restaurar el equipo (desde el momento en que se hizo la instantánea).

Las instrucciones detalladas para crear y administrar las instantáneas se encuentran en las siguientes guías:

- Cree instantáneas de ordenadores o discos virtuales de Lightsail for Research
- Vea y gestione instantáneas de ordenadores y discos virtuales en Lightsail for Research
- Creación de un equipo virtual o un disco a partir de una instantánea
- Eliminar una instantánea en la consola de Lightsail for Research

Paso 9: (opcional) detener o eliminar el equipo virtual

Cuando haya acabado con el equipo virtual que creó para este tutorial, puede eliminarlo. Así dejará de incurrir en cargos por el equipo virtual si no lo necesita.

Al eliminar un equipo virtual, no se eliminan las instantáneas ni los discos adjuntos asociados. Si ha creado instantáneas y discos, debe eliminarlos manualmente para que no se le cobre nada por ellos.

Si quiere guardar el equipo virtual para más adelante, pero evitar incurrir en cargos con los precios por hora estándar, puede detener el equipo virtual en lugar de eliminarlo. A continuación, podrá volver a iniciarlo más adelante. Para obtener más información, consulte Ver detalles de la computadora virtual de Lightsail for Research. Para obtener más información sobre los precios, consulte los precios de Lightsail for Research.

> **Important**
>
> Eliminar un recurso de Lightsail for Research es una acción permanente. Los datos eliminados no se pueden recuperar. Si necesita los datos más adelante, cree una instantánea del equipo virtual antes de eliminarlo. Para obtener más información, consulte Create a snapshot.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Equipos virtuales.
3. Elija el equipo virtual que desea eliminar.
4. Seleccione Acciones y, a continuación, elija Eliminar equipo virtual.
5. Escriba confirmar en el bloque de texto. A continuación, elija Eliminar equipo virtual.

Lanzamiento y uso RStudio en Lightsail for Research

En este tutorial, le mostramos cómo empezar a gestionar y utilizar su ordenador RStudio virtual en Amazon Lightsail for Research.

> **Note**
>
> Se ha publicado un tutorial detallado para empezar a utilizar Lightsail for Research RStudio en el blog AWS del sector público. Para obtener más información, consulte Introducción a Amazon Lightsail for Research: un tutorial sobre el uso. RStudio

Temas

Paso 1: completar los requisitos previos

Cree un ordenador virtual con la RStudio aplicación si aún no lo ha hecho. Para obtener más información, consulte Cree un ordenador virtual Lightsail for Research.

Paso 2: (opcional) agregar espacio de almacenamiento

El equipo virtual viene con un disco del sistema. Sin embargo, a medida que cambien sus necesidades de almacenamiento, puede adjuntar discos adicionales al equipo virtual para aumentar su espacio de almacenamiento.

También puede almacenar los archivos de trabajo en un disco adjunto. A continuación, puede separar el disco y adjuntarlo a un equipo virtual diferente para mover rápidamente los archivos de un equipo a otro.

Como alternativa, puede crear una instantánea de un disco adjunto que contenga los archivos de trabajo y, a continuación, crear un disco duplicado a partir de la instantánea. A continuación, puede adjuntar el nuevo disco duplicado a otro equipo para duplicar su trabajo en distintos equipos virtuales. Para obtener más información, consulte Cree un disco de almacenamiento en la consola de Lightsail for Research y Añada almacenamiento a un ordenador virtual en Lightsail for Research.

> **Note**
>
> Al conectar un disco a su ordenador virtual mediante la consola, Lightsail for Research formatea y monta automáticamente el disco. Este proceso tarda unos minutos, por lo que debe confirmar que el disco ha alcanzado el estado de montaje Montado antes de empezar a usarlo. De forma predeterminada, Lightsail for Research monta los discos en `/home/lightsail-user/<disk-name>` el `<disk-name>` directorio con el nombre que le dio al disco.

Paso 3: cargar y descargar archivos

Puede cargar archivos en su ordenador RStudio virtual y descargarlos desde él. Para ello, debe completar los siguientes pasos:

1. Obtenga un key pair de Amazon Lightsail. Para obtener más información, consulte Obtenga un par de claves para un ordenador virtual Lightsail for Research.
2. Una vez que tenga el par de claves, puede usarlo para establecer una conexión mediante la utilidad Secure Copy (SCP). SCP le permite cargar y descargar archivos mediante el símbolo del sistema o el terminal. Para obtener más información, consulte Transfiera archivos a ordenadores virtuales de Lightsail for Research mediante Secure Copy.
3. (Opcional) También puede usar el par de claves para conectarse a su equipo virtual mediante SSH. Para obtener más información, consulte Connect a un ordenador virtual de Lightsail for Research mediante Secure Shell.

> **Note**
>
> También puede acceder a la interfaz de línea de comandos de su ordenador virtual y transferir archivos mediante el cliente Amazon DCV basado en navegador. Amazon DCV está disponible en la consola Lightsail for Research. Para obtener más información, consulte Acceda a una aplicación informática virtual de Lightsail for Research y Acceda al sistema operativo de su ordenador virtual Lightsail for Research.

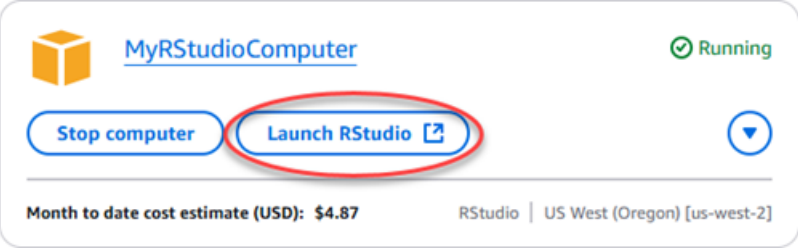
Paso 4: Inicie la aplicación RStudio

Complete el siguiente procedimiento para iniciar la RStudio aplicación en su nueva computadora virtual.

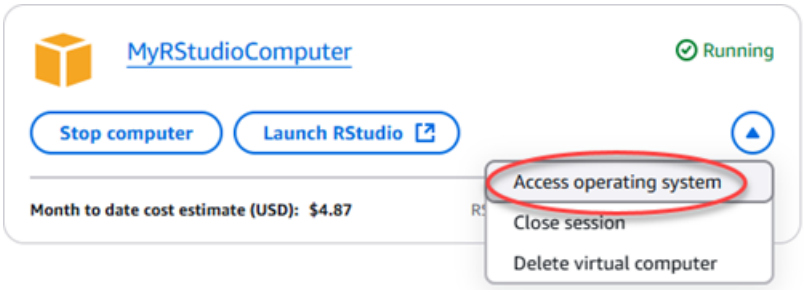
> **Important**
>
> No actualice el sistema operativo ni la RStudio aplicación aunque se le pida que lo haga. En su lugar, elija la opción de cerrar o ignorar esas indicaciones. Además, no modifique ninguno de los archivos que se encuentran en el directorio /home/lightsail-admin/. Estas acciones pueden inutilizar el equipo virtual.

1. Inicie sesión en la consola de Lightsail for Research.
2. Elija Equipos virtuales en el panel de navegación para ver los equipos virtuales que están disponibles en la cuenta.
3. En la página Equipos virtuales, busque su equipo virtual y elija una de las siguientes opciones para conectarse a él:

   a. (Recomendado) Elija Launch RStudio para iniciar la RStudio aplicación en modo enfocado. Si no se ha conectado a su ordenador virtual recientemente, puede que tenga que esperar unos minutos mientras Lightsail for Research prepara la sesión.



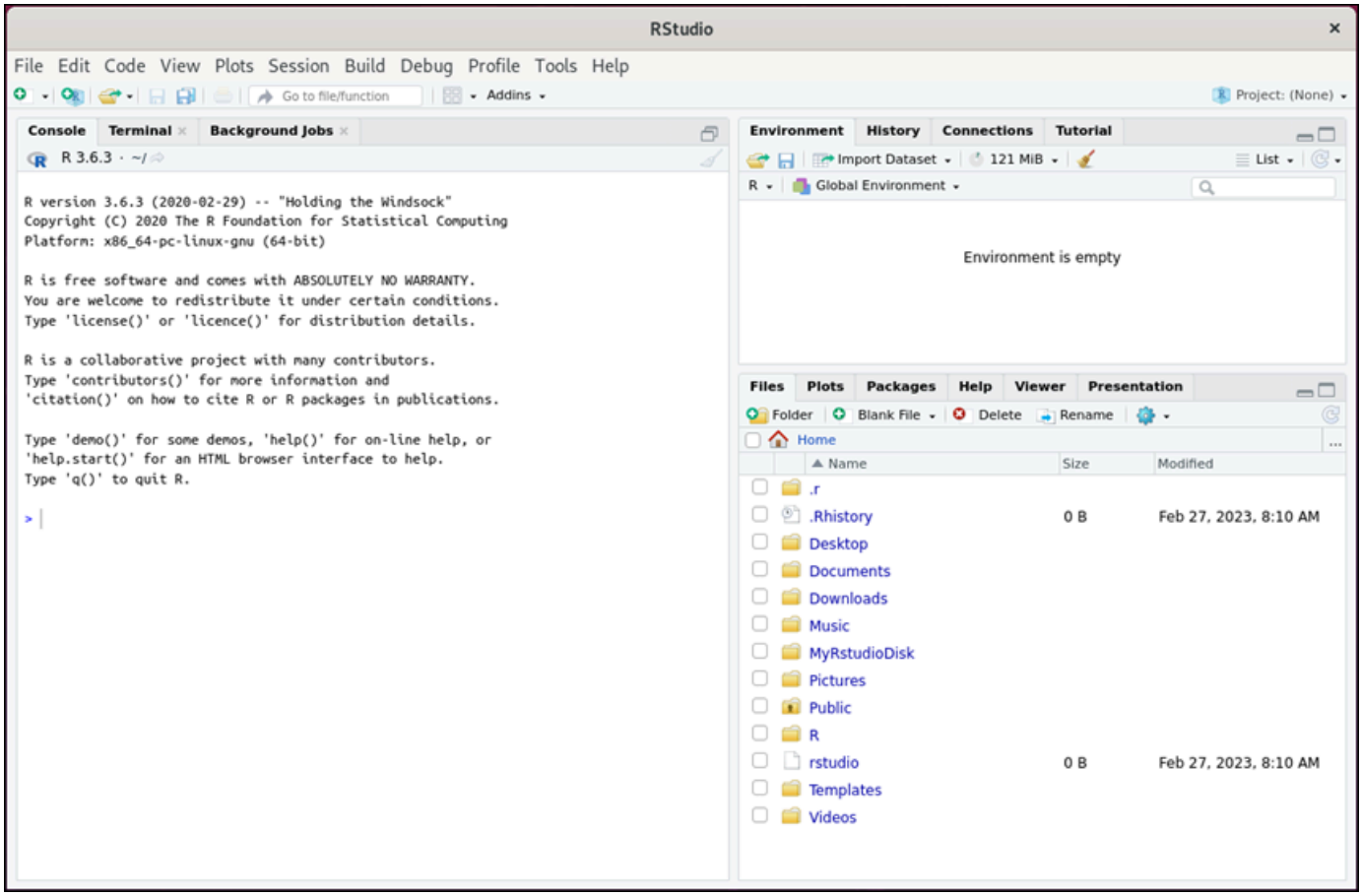
b. Seleccione el menú desplegable del equipo y, a continuación, seleccione Acceso al sistema operativo para acceder al escritorio del equipo virtual. Haga esto si desea instalar una aplicación diferente en el sistema operativo.



Lightsail for Research ejecuta algunos comandos para iniciar la conexión del protocolo de pantalla remota. Tras unos instantes, se abre una nueva ventana de pestañas del navegador con una conexión de escritorio virtual establecida con su equipo virtual. Si eligió la opción Iniciar aplicación, continúe con el siguiente paso de este procedimiento para abrir un archivo en la RStudio aplicación. Si ha elegido la opción Acceso al sistema operativo, puede abrir otras aplicaciones a través del escritorio de Ubuntu.

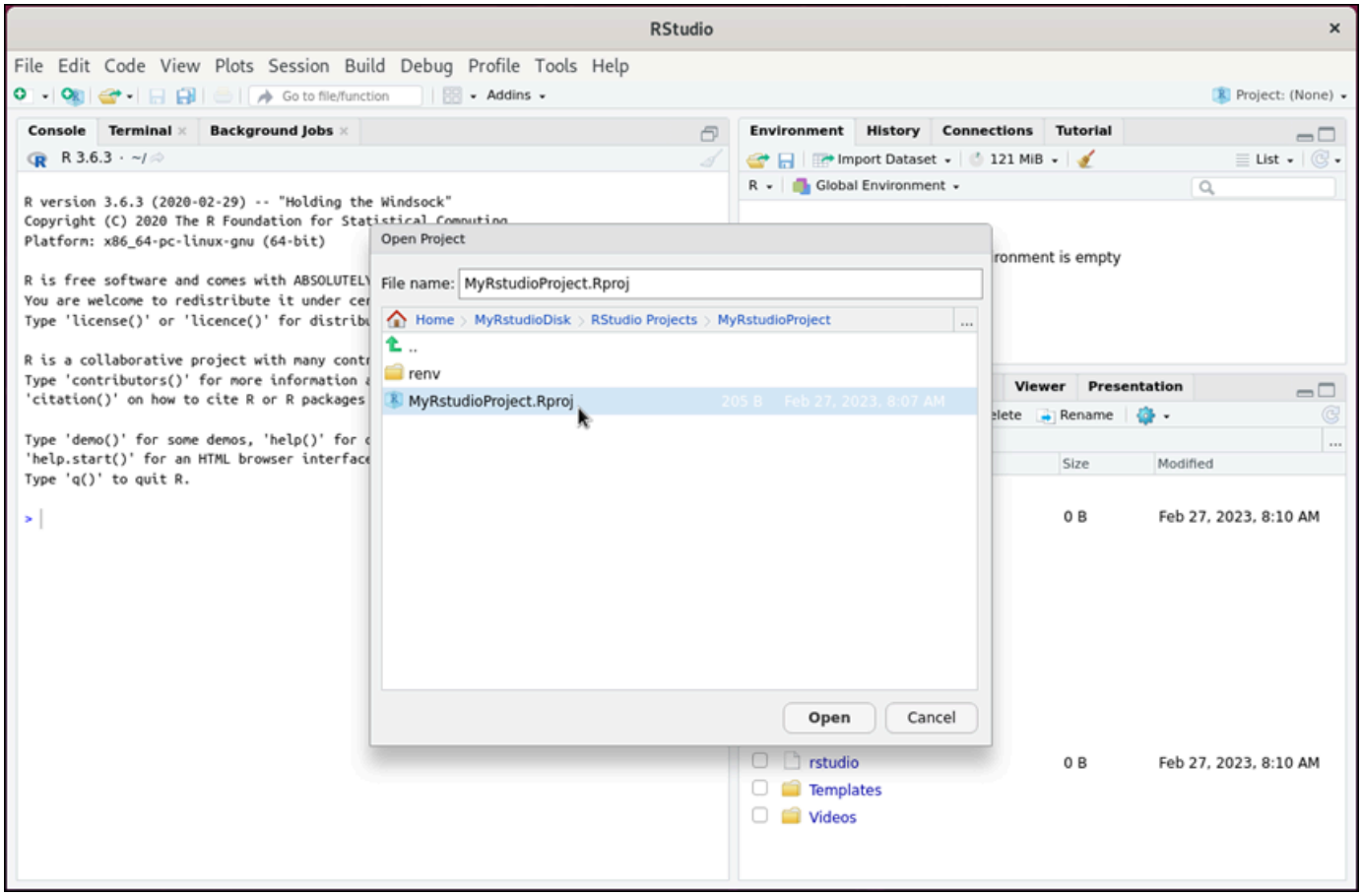
> **Note**
>
> Es posible que su navegador le pida que autorice el uso compartido del portapapeles. Si lo permite, podrá copiar y pegar entre el equipo local y el equipo virtual.
> Es posible que Ubuntu también le pida una configuración inicial. Siga las instrucciones hasta que complete la configuración y pueda usar el sistema operativo.

4. Se abre RStudio la aplicación.

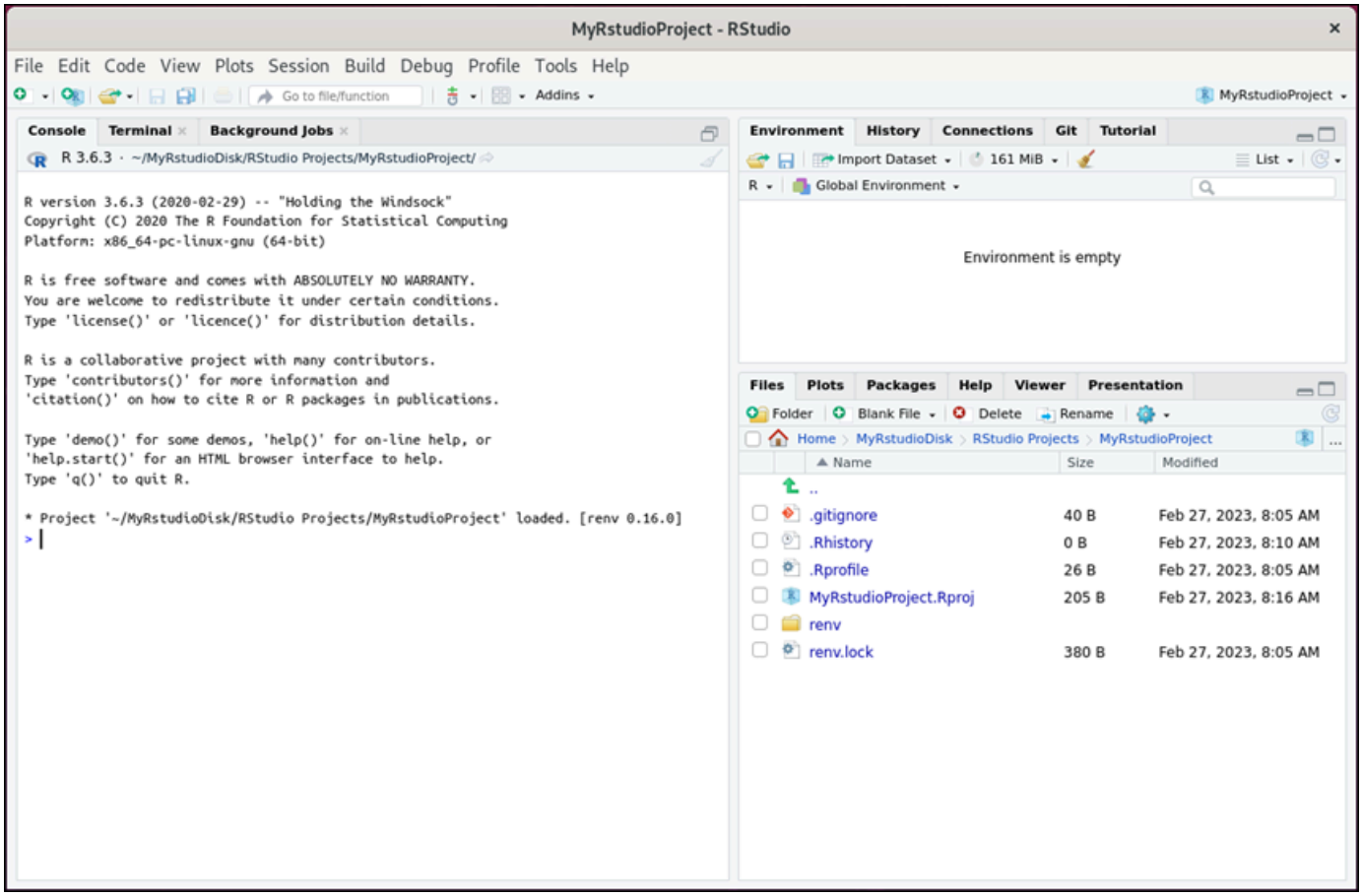


5. Para abrir un proyecto RStudio, seleccione el menú Archivo y, a continuación, elija Abrir proyecto. Navegue hasta el directorio o la carpeta donde están almacenados los archivos del proyecto. A continuación, elija el archivo para abrirlo.

   Si ha cargado los archivos del proyecto en un disco adjunto, busque el directorio en el que está montado el disco. De forma predeterminada, Lightsail for Research monta los discos en el directorio. `/home/lightsail-user/<disk-name>` `<disk-name>`es el nombre que le dio al disco. En el siguiente ejemplo, el `MyRstudioDisk` directorio representa el disco montado y el `Projects` subdirectorio contiene los archivos de nuestro RStudio proyecto.



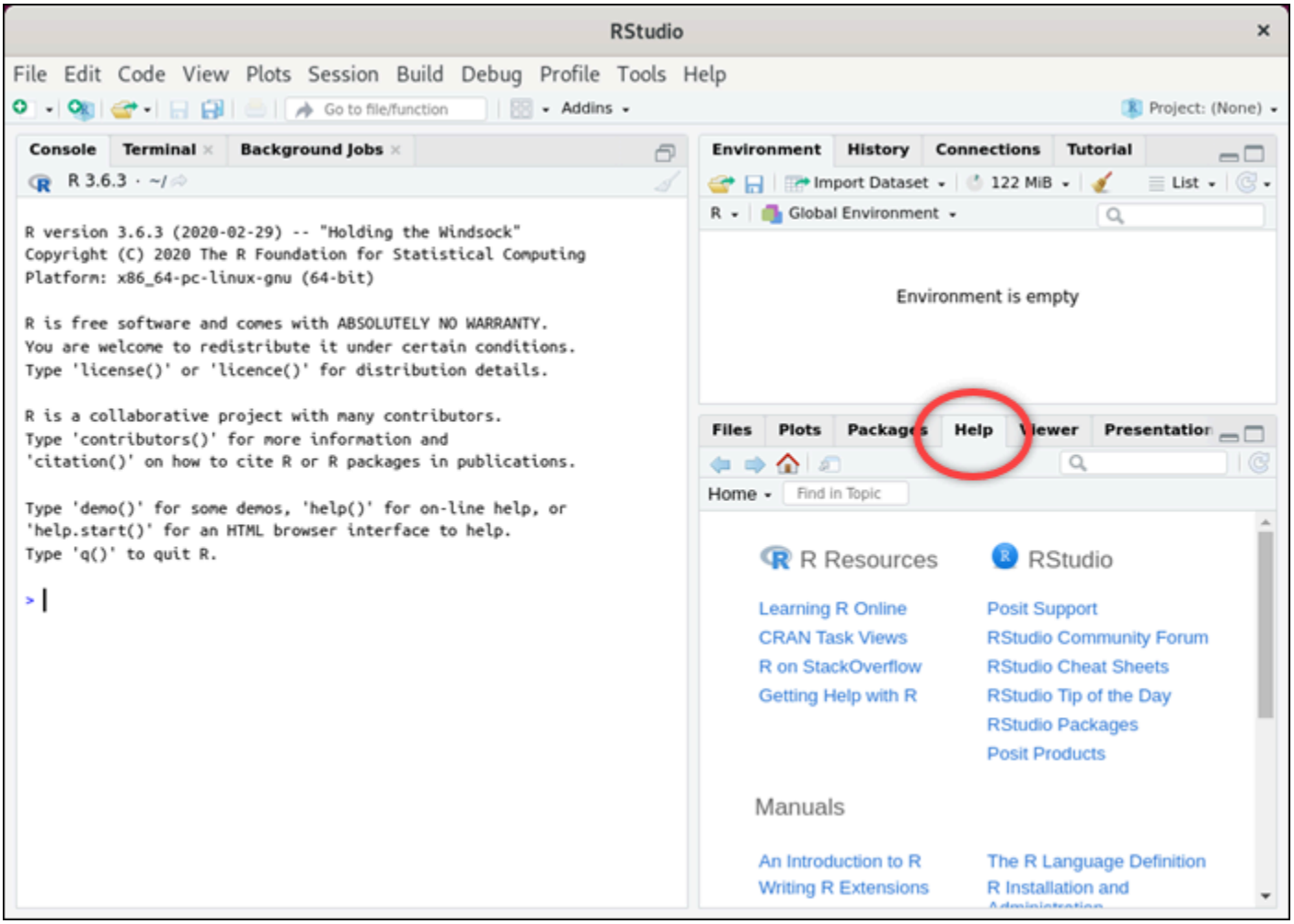
En el siguiente ejemplo, hemos abierto el archivo del proyecto `MyRstudioProject.Rproj`.



Para obtener información sobre cómo empezar RStudio, continúa con la Paso 5: Lea la RStudio documentación sección de este tutorial.

Paso 5: Lea la RStudio documentación

La RStudio aplicación viene con un paquete de documentación completo. Para empezar a aprender RStudio, le recomendamos que acceda a la pestaña Ayuda RStudio como se muestra en el siguiente ejemplo.



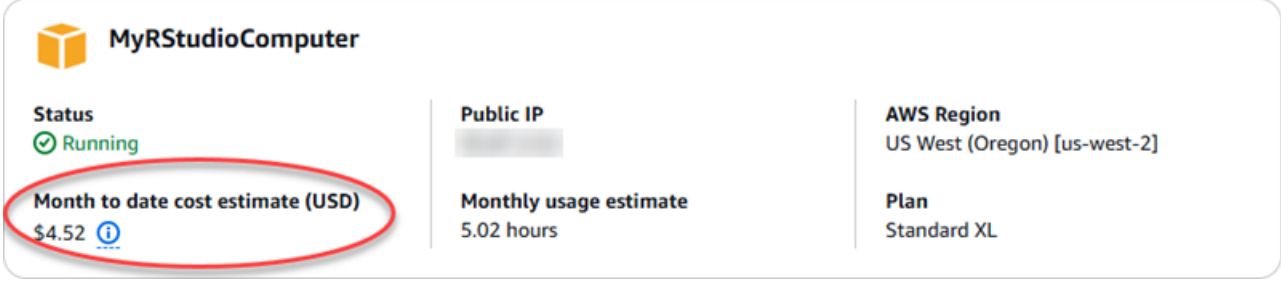
También están disponibles los siguientes recursos en RStudio línea:

- Aprendizaje de R en línea
- R encendido StackOverflow
- Getting Help with R
- Posit Support
- RStudioForo comunitario
- RStudio Hojas de trucos
- RStudio Consejo del día (Twitter)
- RStudioPaquetes

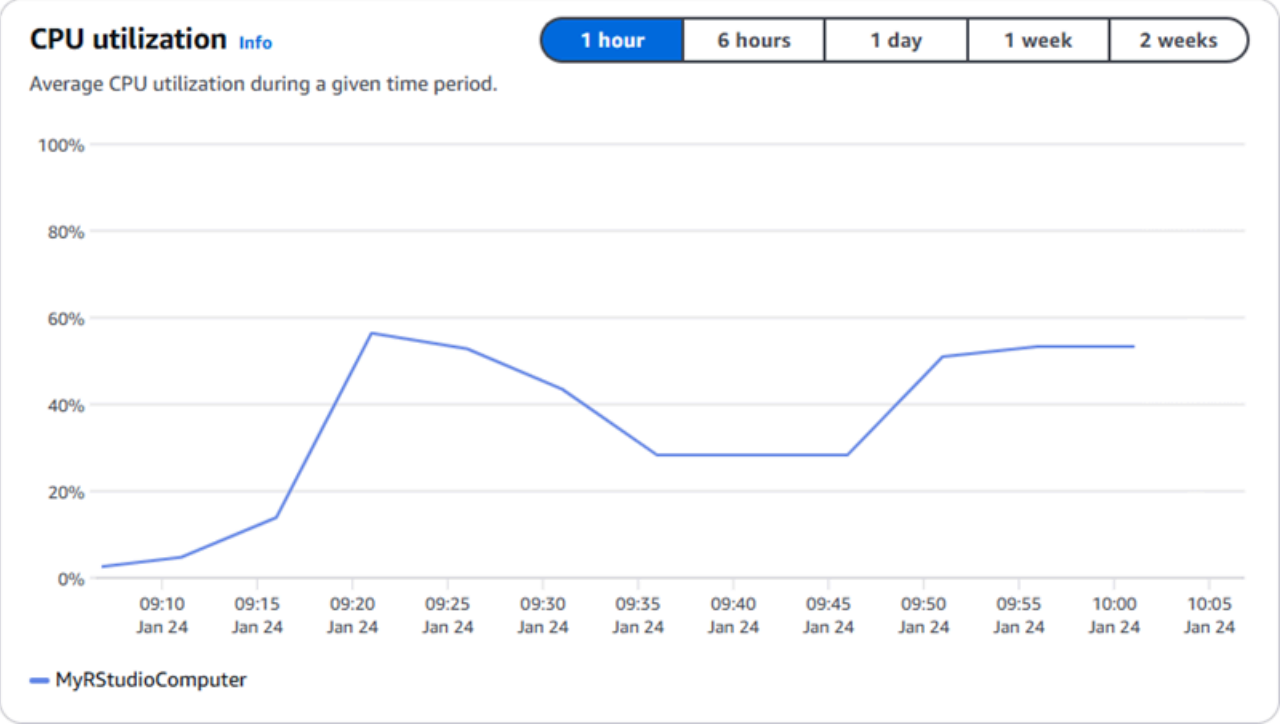
Paso 6: (opcional) supervisar el uso y los costos

Las estimaciones de coste y uso mensuales de sus recursos de Lightsail for Research se muestran en las siguientes áreas de la consola de Lightsail for Research.

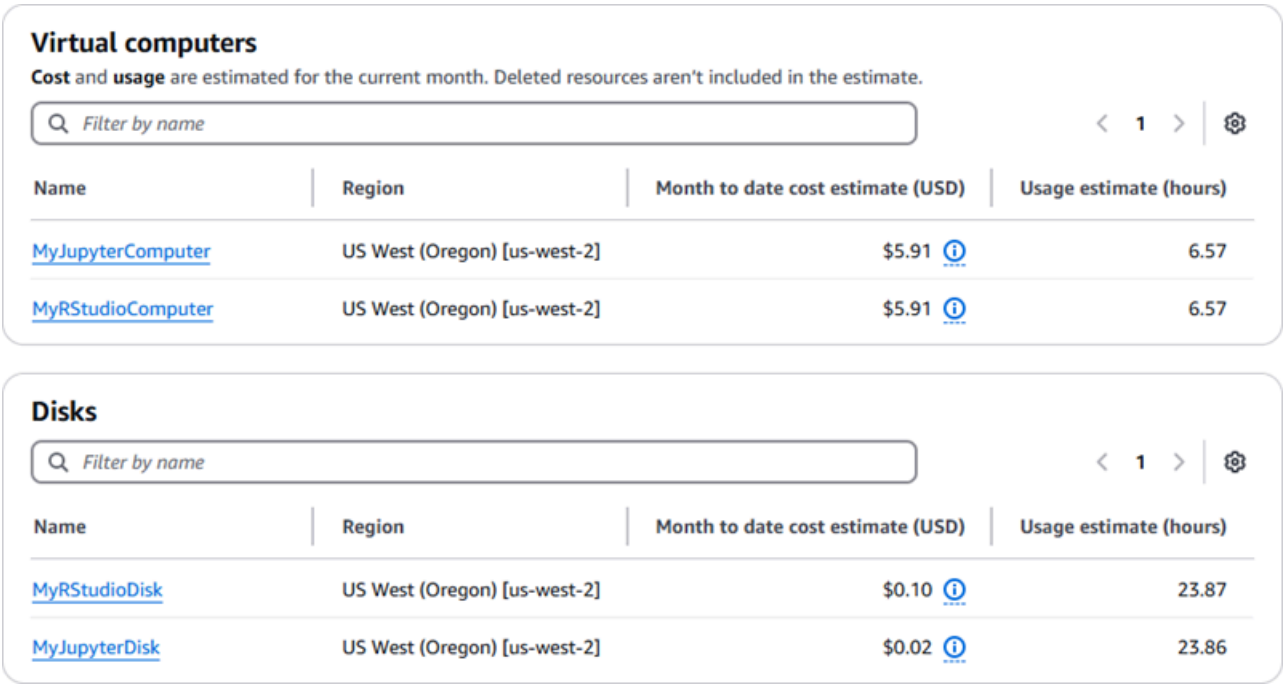
1. Seleccione Ordenadores virtuales en el panel de navegación de la consola de Lightsail for Research. La estimación del costo mensual de sus equipos virtuales hasta la fecha aparece debajo de cada equipo virtual en ejecución.



2. Para ver el uso de la CPU de un equipo virtual, elija el nombre del equipo virtual y, a continuación, elija la pestaña Panel.



3. Para ver las estimaciones de costo y uso del mes hasta la fecha de todos sus recursos de Lightsail for Research, seleccione Uso en el panel de navegación.



Paso 7: (opcional) crear una regla de control de costos

Administre el uso y el costo de sus equipos virtuales mediante la creación de reglas de control de costos. Puede crear una regla Detener el equipo virtual inactivo que detenga un equipo en ejecución cuando alcance un porcentaje específico de uso de la CPU durante un periodo determinado. Por ejemplo, una regla puede detener automáticamente un equipo específico cuando el uso de la CPU es igual o inferior al 5 % durante un periodo de 30 minutos. Esto puede significar que el equipo está inactivo y Lightsail for Research lo detiene para que no se le cobre por un recurso inactivo.

> **Important**
>
> Antes de crear una regla para detener el equipo virtual inactivo, le recomendamos que supervise el uso de la CPU durante unos días. Tome nota del uso de la CPU mientras el equipo virtual esté sometido a diferentes cargas. Por ejemplo, cuando compila código, procesa una operación y está inactivo. Esto lo ayudará a determinar un umbral preciso para la regla. Para obtener más información, consulte la sección Paso 6: (opcional) supervisar el uso y los costos de este tutorial.
>
> Si crea una regla con un umbral de uso de la CPU superior a su carga de trabajo, la regla puede detener el equipo virtual de forma consecutiva. Por ejemplo, si inicia el equipo virtual

inmediatamente después de que una regla lo detenga, la regla se reactiva y el equipo se detiene de nuevo.

Las instrucciones detalladas para crear y administrar las reglas de control de costos se encuentran en las siguientes guías:

- Gestione las reglas de control de costes en Lightsail for Research
- Cree reglas de control de costes para sus ordenadores virtuales Lightsail for Research
- Elimine las reglas de control de costes de sus ordenadores virtuales Lightsail for Research

Paso 8: (opcional) crear una instantánea

Las instantáneas son una point-in-time copia de sus datos. Puede crear instantáneas de sus equipos virtuales y utilizarlas como puntos de referencia para crear nuevos equipos o para realizar copias de seguridad de los datos. Una instantánea contiene todos los datos necesarios para restaurar el equipo (desde el momento en que se hizo la instantánea).

Las instrucciones detalladas para crear y administrar las instantáneas se encuentran en las siguientes guías:

- Cree instantáneas de ordenadores o discos virtuales de Lightsail for Research
- Vea y gestione instantáneas de ordenadores y discos virtuales en Lightsail for Research
- Creación de un equipo virtual o un disco a partir de una instantánea
- Eliminar una instantánea en la consola de Lightsail for Research

Paso 9: (opcional) detener o eliminar el equipo virtual

Cuando haya acabado con el equipo virtual que creó para este tutorial, puede eliminarlo. Así dejará de incurrir en cargos por el equipo virtual si no lo necesita.

Al eliminar un equipo virtual, no se eliminan las instantáneas ni los discos adjuntos asociados. Si ha creado instantáneas y discos, debe eliminarlos manualmente para que no se le cobre nada por ellos.

Si quiere guardar el equipo virtual para más adelante, pero evitar incurrir en cargos con los precios por hora estándar, puede detener el equipo virtual en lugar de eliminarlo. A continuación, podrá volver a iniciarlo más adelante. Para obtener más información, consulte Ver detalles de la

computadora virtual de Lightsail for Research. Para obtener más información sobre los precios, consulte los precios de Lightsail for Research.

> **Important**
>
> Eliminar un recurso de Lightsail for Research es una acción permanente. Los datos eliminados no se pueden recuperar. Si necesita los datos más adelante, cree una instantánea del equipo virtual antes de eliminarlo. Para obtener más información, consulte Create a snapshot.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Equipos virtuales.
3. Elija el equipo virtual que desea eliminar.
4. Seleccione Acciones y, a continuación, elija Eliminar equipo virtual.
5. Escriba confirmar en el bloque de texto. A continuación, elija Eliminar equipo virtual.

Cree y gestione ordenadores virtuales en Lightsail for Research

Con Amazon Lightsail for Research, puede crear ordenadores virtuales en. Nube de AWS

Cuando crea un equipo virtual, elige una aplicación y un plan de hardware para usarlos. Puede establecer un límite de gasto para su equipo virtual y elegir qué ocurrirá cuando el equipo virtual alcance ese límite. Por ejemplo, puede optar por detener automáticamente el equipo virtual para que no se le cobre más del presupuesto configurado.

> **Important**
>
> A partir del 22 de marzo de 2024, los ordenadores virtuales Lightsail for Research se activarán IMDSv2 de forma predeterminada.

Temas

Elija imágenes de aplicaciones y planes de hardware para Lightsail for Research

Cuando crea un ordenador virtual Amazon Lightsail for Research, selecciona una aplicación y un plan de hardware (plan) para él.

Una aplicación proporciona una configuración de software (por ejemplo, una aplicación y un sistema operativo). Un plan proporciona el hardware de la computadora virtual, como el número de v, la memoriaCPUs, el espacio de almacenamiento y la asignación mensual de transferencia de datos. En conjunto, la aplicación y el plan conforman la configuración del equipo virtual.

> **Note**
>
> No puede cambiar la aplicación ni el plan del equipo virtual después de crearlo. Sin embargo, puede crear una instantánea del equipo virtual y, a continuación, elegir un plan nuevo al crear un nuevo equipo virtual a partir de la instantánea. Para obtener más información acerca de las instantáneas, consulte Backup de ordenadores y discos virtuales con instantáneas de Lightsail for Research.

Temas

Aplicaciones

Amazon Lightsail for Research proporciona y administra imágenes de máquinas que contienen la aplicación y el sistema operativo necesarios para lanzar un ordenador virtual. Puede elegir entre una lista de aplicaciones al crear un ordenador virtual en Lightsail for Research. Todas las imágenes de la aplicación Lightsail for Research utilizan el sistema operativo Ubuntu (Linux).

Las siguientes aplicaciones están disponibles en Lightsail for Research:

- JupyterLab— JupyterLab es un entorno de desarrollo integrado (IDE) basado en la web para cuadernos, código y datos. Con su interfaz flexible, puede configurar y organizar los flujos de trabajo en ciencia de datos, computación científica, periodismo computacional y machine learning. Para obtener más información, consulte Jupyter Project Documentation.
- RStudio— RStudio es un entorno de desarrollo integrado (IDE) de código abierto para R, un lenguaje de programación para computación estadística y gráficos, y Python. Combina un editor de código fuente, herramientas de automatización de compilaciones y un depurador, así como herramientas para el trazado y la administración del espacio de trabajo. Para obtener más información, consulte el RStudioIDE.

- VSCodium— VSCodium es una distribución binaria del editor VS Code de Microsoft, impulsada por la comunidad. Para obtener más información, consulte VSCodium.
- Scilab: Scilab es un paquete computacional numérico de código abierto y un lenguaje de programación de alto nivel orientado numéricamente. Para obtener más información, consulte Scilab.
- LTS de Ubuntu 20.04: Ubuntu es una distribución de Linux de código abierto basada en Debian. Ubuntu Server, un servicio reducido, rápido y eficaz, ofrece servicios de forma fiable, predecible y económica. Es una excelente base sobre la que crear sus equipos virtuales. Para obtener más información, consulte Ubuntu releases.

¿Planes

Un plan proporciona las especificaciones de hardware y determina el precio de su ordenador virtual Lightsail for Research. El plan incluye una cantidad fija de memoria (RAM), cómputo (vCPUs), espacio de volumen de almacenamiento (disco) basado en SSD y una asignación mensual de transferencia de datos. Los planes se cobran por hora y bajo demanda, por lo que solo paga por el tiempo que su equipo virtual esté funcionando.

El plan que elija puede depender de los recursos que necesite la carga de trabajo. Lightsail for Research ofrece los siguientes tipos de planes:

- Estándar: los planes estándar son aplicaciones optimizadas para la computación e ideales para las aplicaciones relacionadas con la computación que disponen de procesadores de alto rendimiento.
- GPU: los planes de GPU proporcionan una plataforma rentable y de alto rendimiento para la computación de GPU de uso general. Puede utilizar estos planes para acelerar aplicaciones y cargas de trabajo científicas, de ingeniería y de representación.

Planes estándar

Las siguientes son las especificaciones de hardware de los planes estándar disponibles en Lightsail for Research.

Nombre del plan	v CPUs	Memoria	Espacio de almacenamiento	Asignación mensual de transferencia de datos

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

Planes de GPU

A continuación se muestran las especificaciones de hardware de los planes de GPU disponibles en Lightsail for Research.

Nombre del plan	v CPUs	Memoria	Espacio de almacenamiento	Asignación mensual de transferencia de datos
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

Cree un ordenador virtual Lightsail for Research

Complete los siguientes pasos para crear un ordenador virtual de Lightsail for Research que ejecute una aplicación.

1. Inicie sesión en la consola de Lightsail for Research.
2. En la página de inicio, seleccione Crear equipo virtual.
3. Seleccione una Región de AWS para su computadora virtual que esté cerca de su ubicación física.
4. Elija una aplicación y un plan de hardware. Para obtener más información, consulte Elija imágenes de aplicaciones y planes de hardware para Lightsail for Research.
5. Escriba un nombre para el equipo virtual. Los caracteres válidos son caracteres alfanuméricos, números, puntos, guiones y guiones bajos.

Los nombres de los equipos virtuales también deben cumplir los siguientes requisitos:

- Sea único en cada uno de ellos Región de AWS en su cuenta de Lightsail for Research.
- Contener entre 2 y 255 caracteres.
- Comenzar y terminar por un carácter alfanumérico o un número.

6. Seleccione Crear equipo virtual en el panel Resumen.

En cuestión de minutos, su ordenador virtual Lightsail for Research estará listo y podrá conectarse a él mediante una sesión de interfaz gráfica de usuario (GUI). Para obtener más información sobre cómo conectarse a su ordenador virtual Lightsail for Research, consulte. Acceda a una aplicación informática virtual de Lightsail for Research

> **Important**
>
> Los equipos virtuales recién creados tienen un conjunto de puertos de firewall abiertos de forma predeterminada. Para obtener más información sobre estos puertos, consulte Administre los puertos de firewall para los ordenadores virtuales Lightsail for Research.

Ver detalles de la computadora virtual de Lightsail for Research

Complete los siguientes pasos para ver una lista de ordenadores virtuales y sus detalles en su cuenta de Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research.
2. Elija Equipos virtuales en el panel de navegación para ver una lista de los equipos virtuales de la cuenta.

Elija el nombre de un equipo virtual para ir a su página de administración. A continuación se muestra la información que se proporciona en la página de administración:

- Nombre del equipo virtual: nombre del equipo virtual.
- Estado: el equipo virtual puede tener uno de los siguientes códigos de estado:
  - Creación
  - Ejecutar

  - Detención
  - Stopped
  - Desconocido
- Región de AWS— El lugar en el que se creó Región de AWS su ordenador virtual.
- Aplicación y hardware: aplicación y plan de hardware del equipo virtual.
- Estimación de uso mensual: uso estimado por hora de este equipo virtual durante el ciclo de facturación actual.
- Cálculo del costo mensual hasta la fecha: costo estimado (en USD) del equipo virtual para este ciclo de facturación.
- Panel: desde la pestaña Panel, puede iniciar una sesión para acceder a la aplicación del equipo virtual. También puede ver el uso de la CPU. El uso de la CPU identifica la potencia de procesamiento que utilizan las aplicaciones del equipo virtual. Cada punto de datos que se muestra en el gráfico representa el promedio de uso de la CPU durante un periodo de tiempo.
- Reglas de control de costos: reglas que define para ayudar a administrar el uso y los costos de su equipo virtual.
- Uso de equipos virtuales: estimación del costo y el uso para un ciclo de facturación determinado. Puede filtrar por fecha y hora.
- Almacenamiento: cree, adjunte y desasocie discos de equipos virtuales desde la pestaña Almacenamiento. Un disco es un volumen de almacenamiento que se puede adjuntar a un equipo virtual y montar como disco duro.
- Etiquetas: administre las etiquetas de su equipo virtual desde la pestaña de etiquetas. Una etiqueta es una etiqueta que se asigna a un AWS recurso. Cada etiqueta consta de una clave y un valor opcional. Puede usar etiquetas para buscar y filtrar sus recursos o realizar un seguimiento de sus AWS costos.

Acceda a una aplicación informática virtual de Lightsail for Research

Complete los siguientes pasos para iniciar la aplicación que se ejecuta en su ordenador virtual Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Equipos virtuales.

3. Busque el nombre del equipo virtual desde el que desea lanzar la aplicación.

> **Note**
>
> Si el equipo virtual está detenido, primero pulse el botón Iniciar equipo para activarlo.

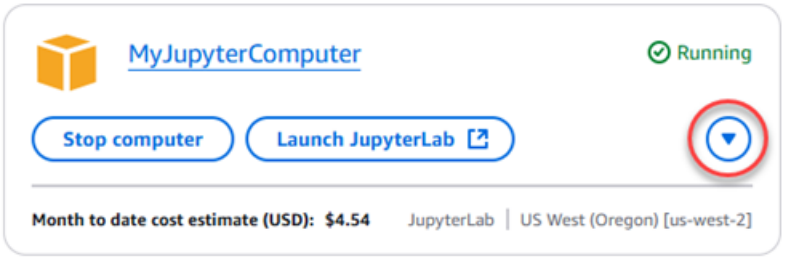
4. Seleccione Lanzar aplicación. Por ejemplo, Launch. JupyterLab Se abrirá una sesión de aplicación en una nueva ventana del navegador web.

> **Important**
>
> Si el navegador web tiene instalado un bloqueador de ventanas emergentes, puede que tenga que permitir las ventanas emergentes del dominio aws.amazon.com antes de abrir la sesión.

Acceda al sistema operativo de su ordenador virtual Lightsail for Research

Complete los siguientes pasos para acceder al sistema operativo de su ordenador virtual Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Equipos virtuales.
3. Busque el nombre de su equipo virtual y, a continuación, selecciona el botón desplegable de acciones situado debajo del estado del equipo.



> **Note**
>
> Si el equipo virtual está detenido, primero pulse el botón Iniciar para activarlo.

4. Seleccione Acceso al sistema operativo. Se abrirá una sesión del sistema operativo en una nueva ventana del navegador.

> **Important**
>
> Si el navegador web tiene instalado un bloqueador de ventanas emergentes, puede que tenga que permitir las ventanas emergentes del dominio aws.amazon.com antes de abrir la sesión.

Administre los puertos de firewall para los ordenadores virtuales Lightsail for Research

Un firewall en Amazon Lightsail for Research controla el tráfico permitido para conectarse a su ordenador virtual. Agrega reglas al firewall de su computadora virtual que especifican el protocolo, los puertos y la fuente IPv4 o IPv6 las direcciones que pueden conectarse a ella. Las reglas del firewall siempre son permisivas; no se pueden crear reglas que denieguen el acceso. Agregue reglas al firewall del equipo virtual para permitir que el tráfico llegue a su equipo virtual. Cada equipo virtual tiene dos firewalls: uno para las IPv4 direcciones y otro para IPv6 las direcciones. Ambos firewalls son independientes entre sí y contienen un conjunto preconfigurado de reglas que filtran el tráfico que entra en la instancia.

Protocolos

Un protocolo es el formato en el que se transmiten los datos entre dos equipos. Puede especificar los siguientes protocolos en una regla de firewall:

- El protocolo de control de transmisión (TCP) se utiliza principalmente para establecer y mantener una conexión entre los clientes y la aplicación que se ejecuta en el equipo virtual. Es un protocolo ampliamente utilizado y que a menudo puede especificar en sus reglas de firewall.
- El protocolo de datagramas de usuario (UDP) se utiliza principalmente para establecer conexiones de baja latencia y con tolerancia a pérdidas entre los clientes y la aplicación que se ejecuta en el equipo virtual. Su uso ideal es para aplicaciones de red en las que la latencia percibida es crítica, como comunicaciones de video, voz y juegos.
- El protocolo de mensajes de control de Internet (ICMP) se utiliza principalmente para diagnosticar problemas de comunicación de red, como por ejemplo determinar si los datos están llegando a su destino previsto de manera oportuna. El uso ideal sería para la utilidad Ping, que puede utilizar

para probar la velocidad de la conexión entre su equipo local y su equipo virtual. Informa de cuánto tiempo tardan los datos en llegar a su equipo virtual y volver a su equipo local.

- Todo se utiliza para permitir que todo el tráfico de protocolo pase por su equipo virtual. Especifique este protocolo cuando no esté seguro de qué protocolo debe especificar. Esto incluye todos los protocolos de Internet, no solo los especificados anteriormente. Para obtener más información, consulte Números de protocolo en el sitio web de la Autoridad de Números Asignados en Internet.

Puertos

Al igual que los puertos físicos del equipo, que permiten al equipo comunicarse con periféricos como el teclado y el puntero, los puertos de red sirven como puntos de conexión de comunicaciones de Internet para su equipo virtual. Cuando un cliente busca conectarse con su equipo virtual, expondrá un puerto para establecer la comunicación.

Los puertos que puede especificar en una regla de firewall pueden oscilar entre 0 y 65535. Al crear una regla de firewall para permitir a un cliente establecer una conexión con el equipo virtual, se especifica el protocolo que se va a utilizar. También debe especificar los números de puerto a través de los cuales se puede establecer la conexión y las direcciones IP que pueden establecer una conexión.

Los siguientes puertos están abiertos de forma predeterminada para los equipos virtuales recién creados.

- TCP
  - 22: se utiliza para Secure Shell (SSH).
  - 80: se utiliza para el protocolo de transferencia de hipertexto (HTTP).
  - 443: se utiliza para el protocolo seguro de transferencia de hipertexto (HTTPS).
  - 8443: se utiliza para el protocolo seguro de transferencia de hipertexto (HTTPS).

¿Por qué abrir y cerrar puertos?

Al abrir los puertos, permite que un cliente establezca una conexión con su equipo virtual. Al cerrar los puertos, bloquea las conexiones con el equipo virtual. Por ejemplo, para permitir que un cliente de SSH se conecte a su equipo virtual, configure una regla de firewall que permita el protocolo TCP a través del puerto 22 únicamente desde la dirección IP del equipo que necesita establecer una conexión. En este caso, no desea permitir que ninguna dirección IP establezca una conexión

SSH con el equipo virtual. Hacerlo podría suponer un riesgo de seguridad. Si esta regla ya está configurada en el firewall de la instancia, puede eliminarla para impedir que el cliente de SSH se conecte a su equipo virtual.

Los siguientes procedimientos le muestran cómo obtener los puertos que están abiertos actualmente en su equipo virtual, abrir puertos nuevos y cerrar puertos.

Temas

Cumplimiento de los requisitos previos de

Complete los siguientes requisitos previos antes de comenzar.

- Cree un ordenador virtual en Lightsail for Research. Para obtener más información, consulte Cree un ordenador virtual Lightsail for Research.
- Descargue e instale el AWS Command Line Interface ()AWS CLI. Para obtener más información, consulte Instalar o actualizar la última versión de la AWS CLI en la Guía del usuario de AWS Command Line Interface de la versión 2.
- Configure el AWS CLI para acceder a su Cuenta de AWS. Para obtener más información, consulte Fundamentos de configuración en la Guía del usuario de AWS Command Line Interface de la versión 2.

Obtención de los estados de los puertos de un equipo virtual

Complete el siguiente procedimiento para obtener los estados de los puertos de un equipo virtual. Este procedimiento utiliza el `get-instance-port-states` AWS CLI comando para obtener los estados de los puertos del firewall de un equipo virtual Lightsail for Research específico, las direcciones IP que pueden conectarse al equipo virtual a través de los puertos y el protocolo. Para obtener más información, consulte get-instance-port-states en la Referencia de comandos de la AWS CLI .

1. Este paso se establece en función del sistema operativo del equipo local.

   - Si el equipo local utiliza un sistema operativo Windows, abra una ventana del símbolo del sistema.
   - Si el equipo local utiliza un sistema operativo Linux o basado en Unix (incluido macOS), abra una ventana del terminal.

2. Ingrese el siguiente comando para obtener los estados de los puertos del firewall y las direcciones IP y los protocolos permitidos. En el comando, sustituya *REGION* por el código de la región de AWS en la que se creó el equipo virtual (por ejemplo, `us-east-2`). Sustituya *NAME* por el nombre de su equipo virtual.

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

   Ejemplo

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

   En la respuesta se mostrarán los protocolos y los puertos abiertos y los rangos de IP de CIDR que pueden conectarse a su equipo virtual.

   ```
   % 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
   ```

   Para obtener información sobre cómo abrir puertos, continúe con la siguiente sección.

Apertura de los puertos de un equipo virtual

Complete el siguiente procedimiento para abrir los puertos de un equipo virtual. Este procedimiento utiliza el `open-instance-public-ports` AWS CLI comando. Abra los puertos del firewall para permitir que se establezcan conexiones desde una dirección IP de confianza o un rango de direcciones IP. Por ejemplo, para permitir la dirección IP `192.0.2.44`, especifique `192.0.2.44` o `192.0.2.44/32`. Para permitir las direcciones IP `192.0.2.0` en `192.0.2.255`, especifique

`192.0.2.0/24`. Para obtener más información, consulte open-instance-public-ports en la Referencia de comandos de la AWS CLI .

1. Este paso se establece en función del sistema operativo del equipo local.
   - Si el equipo local utiliza un sistema operativo Windows, abra una ventana del símbolo del sistema.
   - Si el equipo local utiliza un sistema operativo Linux o basado en Unix (incluido macOS), abra una ventana del terminal.
2. Ingrese el siguiente comando para abrir puertos.

   En el comando, sustituya los siguientes elementos:

   - *REGION*Sustitúyalo por el código de la AWS región en la que se creó el equipo virtual, por ejemplo`us-east-2`.
   - Sustituya *NAME* por el nombre de su equipo virtual.
   - Sustituya *FROM-PORT* por el primer puerto de un rango de puertos que desea abrir.
   - Sustituya *PROTOCOL* por el nombre del protocolo de IP. Por ejemplo, TCP.
   - Sustituya *TO-PORT* por el último puerto de un rango de puertos que desea abrir.
   - Sustituya *IP* por la dirección IP o el rango de direcciones IP que desea permitir que se conecten a su equipo virtual.

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

   Ejemplo

   ```
   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
   ```

   En la respuesta se mostrarán los protocolos y los puertos agregados recientemente y los rangos de IP de CIDR que pueden conectarse a su equipo virtual.

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

Para obtener información sobre cómo cerrar puertos, continúe con la siguiente sección.

Cierre de los puertos de un equipo virtual

Complete el siguiente procedimiento para cerrar los puertos de un equipo virtual. Este procedimiento utiliza el `close-instance-public-ports` AWS CLI comando. Para obtener más información, consulte close-instance-public-ports en la Referencia de comandos de la AWS CLI .

1. Este paso se establece en función del sistema operativo del equipo local.
   - Si el equipo local utiliza un sistema operativo Windows, abra una ventana del símbolo del sistema.
   - Si el equipo local utiliza un sistema operativo Linux o basado en Unix (incluido macOS), abra una ventana del terminal.
2. Ingrese el siguiente comando para cerrar puertos.

   En el comando, sustituya los siguientes elementos:

   - *REGION*Sustitúyalo por el código de la AWS región en la que se creó el equipo virtual, por ejemplo`us-east-2`.
   - Sustituya *NAME* por el nombre de su equipo virtual.
   - Sustituya *FROM-PORT* por el primer puerto de un rango de puertos que desea cerrar.
   - Sustituya *PROTOCOL* por el nombre del protocolo de IP. Por ejemplo, TCP.
   - Sustituya *TO-PORT* por el último puerto de un rango de puertos que desea cerrar.
   - Sustituya *IP* por la dirección IP o el rango de direcciones IP que desea eliminar.

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

Ejemplo

```
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
```

En la respuesta se mostrarán los puertos, los protocolos y los rangos de IP de CIDR que se han cerrado y que no pueden conectarse a su equipo virtual.

Continúe con los pasos siguientes.

Puede completar los siguientes pasos adicionales una vez que haya administrado correctamente los puertos del firewall de su equipo virtual:

- Obtenga el par de claves de su equipo virtual. Con el par de claves, puede establecer una conexión mediante numerosos clientes de SSH, como OpenSSH, PuTTY y el Subsistema de Windows para Linux. Para obtener más información, consulte Obtenga un par de claves para un ordenador virtual Lightsail for Research.
- Conéctese a su equipo virtual mediante SSH para administrarlo mediante la línea de comandos. Para obtener más información, consulte Transfiera archivos a ordenadores virtuales de Lightsail for Research mediante Secure Copy.

- Conéctese a su equipo virtual mediante SCP para transferir archivos de forma segura. Para obtener más información, consulte Transfiera archivos a ordenadores virtuales de Lightsail for Research mediante Secure Copy.

Obtenga un par de claves para un ordenador virtual Lightsail for Research

Un par de claves, compuesto por una clave pública y una clave privada, es un conjunto de credenciales de seguridad que se utilizan para demostrar su identidad al conectarse a un ordenador virtual Amazon Lightsail for Research. La clave pública se guarda en cada ordenador virtual de Lightsail for Research y usted guarda la clave privada en el equipo local. La clave privada le permite establecer de forma segura un protocolo Secure Shell (SSH) con su equipo virtual. Cualquier persona que tenga la clave privada puede conectarse a su equipo virtual, por lo que es importante que almacene su clave privada en un lugar seguro.

La primera vez que se crea una instancia de Lightsail o un ordenador virtual de Lightsail for Research, se crea automáticamente un par de claves predeterminado de Amazon Lightsail (DKP). El DKP es específico de cada AWS región en la que cree una instancia o un ordenador virtual. Por ejemplo, el DKP de Lightsail para la región EE.UU. Este (Ohio) (us-east-2) se aplica a todos los ordenadores que cree en EE.UU. Este (Ohio) en Lightsail y Lightsail for Research que estaban configurados para usar el DKP cuando se crearon. Lightsail for Research almacena automáticamente la clave pública del DKP en los ordenadores virtuales que cree. Puede descargar la clave privada del DKP en cualquier momento realizando una llamada a la API del servicio Lightsail.

En este documento, le mostramos cómo obtener el DKP de un equipo virtual. Cuando tenga el DKP, puede establecer una conexión mediante numerosos clientes de SSH, como OpenSSH, PuTTY y el Subsistema de Windows para Linux. También puede utilizar Secure Copy (SCP) para transferir archivos de forma segura desde el equipo local al equipo virtual.

> **Note**
>
> También puede establecer una conexión de protocolo de pantalla remota a su ordenador virtual mediante el cliente Amazon DCV basado en navegador. Amazon DCV está disponible en la consola Lightsail for Research. Ese cliente de RDP no requiere que obtenga un par de claves para su equipo. Para obtener más información, consulte Acceda a una aplicación

informática virtual de Lightsail for Research y Acceda al sistema operativo de su ordenador virtual Lightsail for Research.

Temas

- Cumplimiento de los requisitos previos de
- Obtención de un par de claves para un equipo virtual
- Continúe con los pasos siguientes.

Cumplimiento de los requisitos previos de

Complete los siguientes requisitos previos antes de comenzar.

- Cree un ordenador virtual en Lightsail for Research. Para obtener más información, consulte Cree un ordenador virtual Lightsail for Research.
- Descargue e instale el AWS Command Line Interface ()AWS CLI. Para obtener más información, consulte Instalar o actualizar la última versión de la AWS CLI en la Guía del usuario de AWS Command Line Interface de la versión 2.
- Configure el AWS CLI para acceder a su Cuenta de AWS. Para obtener más información, consulte Fundamentos de configuración en la Guía del usuario de AWS Command Line Interface de la versión 2.
- Descargue e instale jq. Es un procesador de JSON de línea de comandos ligero y flexible que se utiliza en los siguientes procedimientos para extraer detalles de los pares de claves de las salidas JSON de AWS CLI. Para obtener más información sobre la descarga e instalación de jq, consulte Download jq en el sitio web de jq.

Obtención de un par de claves para un equipo virtual

Complete uno de los siguientes procedimientos para obtener el DKP de Lightsail para un ordenador virtual en Lightsail for Research.

Obtención de un par de claves para un equipo virtual mediante un equipo local con Windows

Este procedimiento se aplica a su caso si su equipo local utiliza un sistema operativo Windows. Este procedimiento utiliza el `download-default-key-pair` AWS CLI comando para obtener el DKP de

Lightsail para una región. AWS Para obtener más información, consulte download-default-key-pair en la Referencia de comandos de la AWS CLI .

1. Abra una ventana del símbolo del sistema.
2. Ingresa el siguiente comando para obtener el DKP de Lightsail para una región específica. AWS Este comando guarda la información en un archivo `dkp-details.json`. En el comando, *`region-code`* sustitúyalo por el código de la AWS región en la que se creó la computadora virtual, por ejemplo. `us-east-2`

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

   Ejemplo

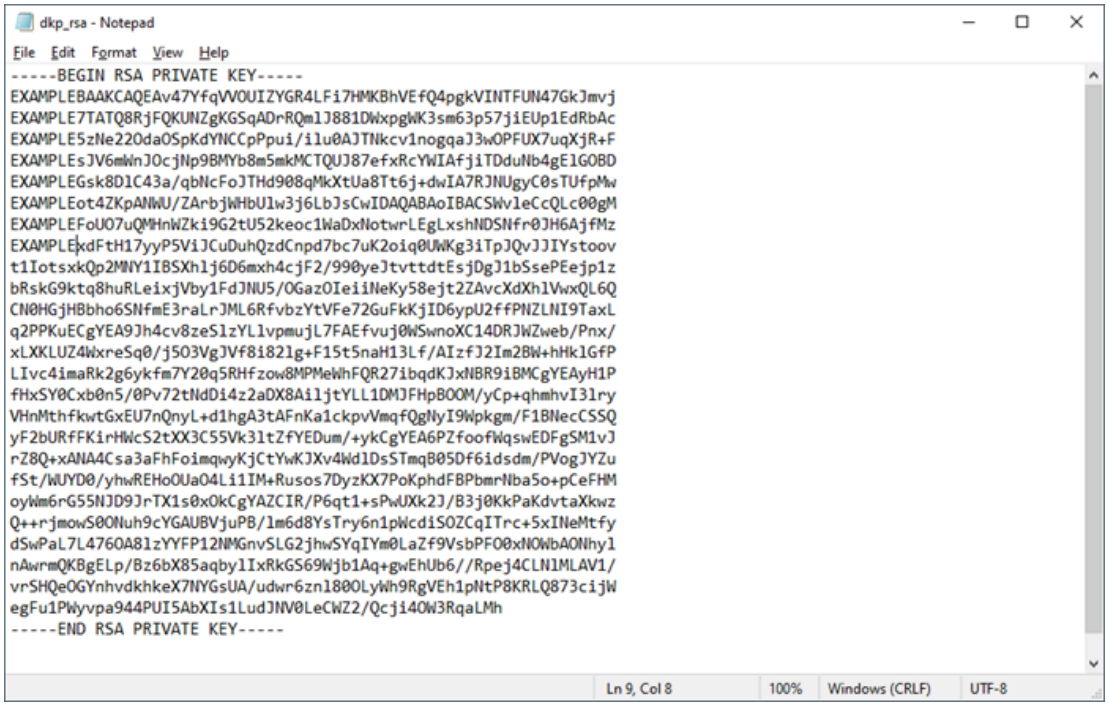
   ```
   aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
   ```

   No hay respuesta al comando. Puede confirmar si el comando se ha realizado correctamente abriendo el `dkp-details.json` archivo y comprobando si se ha guardado la información del DKP de Lightsail. El contenido del archivo `dkp-details.json` debe ser similar al siguiente ejemplo. El comando ha fallado si el archivo está en blanco.

3. Ingrese el siguiente comando para extraer la información de la clave privada del archivo `dkp-details.json` y agregarla a un nuevo archivo de clave privada `dkp_rsa`.

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

No hay respuesta al comando. Para confirmar si el comando se ejecutó correctamente, puede abrir los archivos `dkp_rsa` y comprobar si tienen información. El contenido del archivo `dkp_rsa` debe ser similar al siguiente ejemplo. El comando ha fallado si el archivo está en blanco.



Ahora tiene la clave privada necesaria para establecer una conexión SSH o SCP con su equipo virtual. Continúe con la siguiente sección para consultar los siguientes pasos adicionales.

Obtención de un par de claves para un equipo virtual mediante un equipo local con Linux, Unix o macOS

Este procedimiento se aplica a su caso si su equipo local utiliza un sistema operativo Linux, Unix o macOS. Este procedimiento utiliza el `download-default-key-pair` AWS CLI comando para obtener el DKP de Lightsail para una región. AWS Para obtener más información, consulte download-default-key-pair en la Referencia de comandos de la AWS CLI .

1. Abra una ventana de terminal.
2. Ingresa el siguiente comando para obtener el DKP de Lightsail para una región específica. AWS Este comando guarda la información en un archivo `dkp-details.json`. En el comando,

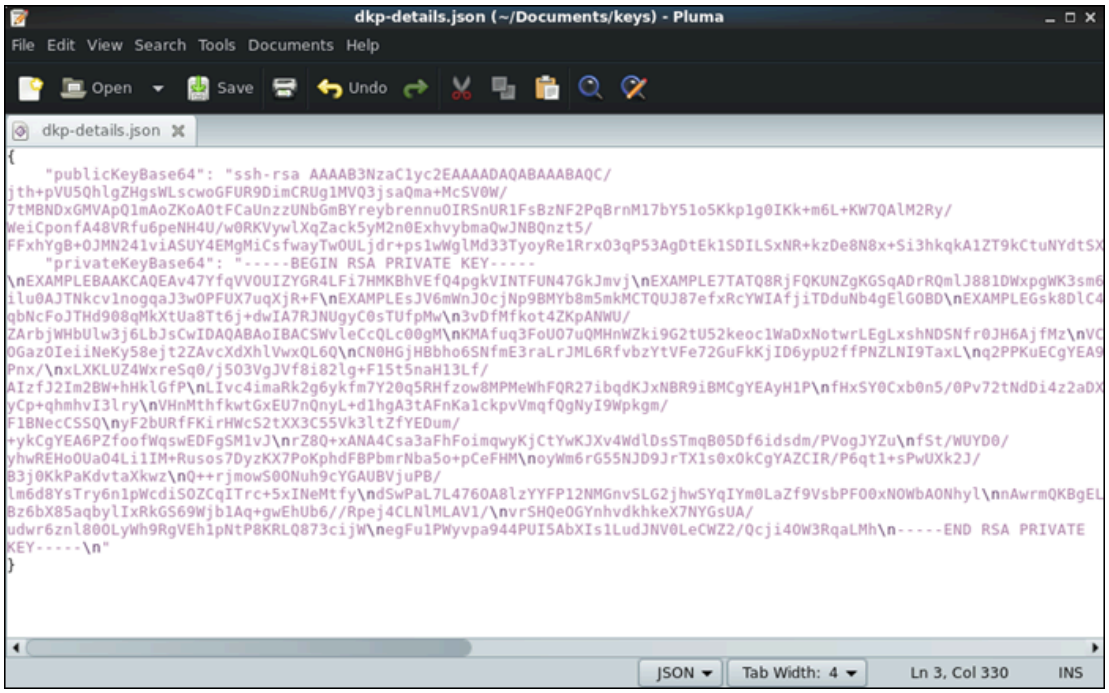
region-code sustitúyalo por el código de la AWS región en la que se creó la computadora virtual, por ejemplo. us-east-2

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

Ejemplo

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

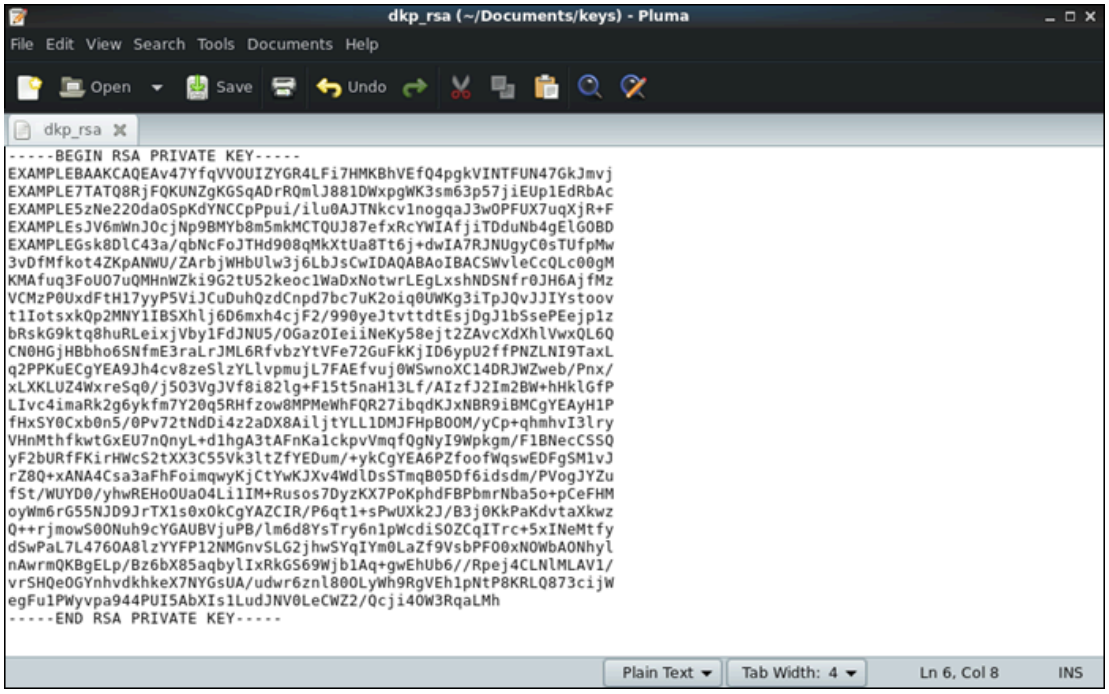
No hay respuesta al comando. Puede confirmar si el comando se ha realizado correctamente abriendo el dkp-details.json archivo y comprobando si se ha guardado la información del DKP de Lightsail. El contenido del archivo dkp-details.json debe ser similar al siguiente ejemplo. El comando ha fallado si el archivo está en blanco.



3. Ingrese el siguiente comando para extraer la información de la clave privada del archivo dkp-details.json y agregarla a un nuevo archivo de clave privada dkp_rsa.

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

No hay respuesta al comando. Para confirmar si el comando se ejecutó correctamente, puede abrir los archivos dkp_rsa y comprobar si tienen información. El contenido del archivo dkp_rsa debe ser similar al siguiente ejemplo. El comando ha fallado si el archivo está en blanco.



4. Ingrese el siguiente comando para establecer permisos para el archivo `dkp_rsa`.

```
chmod 600 dkp_rsa
```

Ahora tiene la clave privada necesaria para establecer una conexión SSH o SCP con su equipo virtual. Continúe con la siguiente sección para consultar los siguientes pasos adicionales.

Continúe con los pasos siguientes.

Puede completar los siguientes pasos adicionales una vez que haya obtenido correctamente los pares de claves de su equipo virtual:

- Conéctese a su equipo virtual mediante SSH para administrarlo mediante la línea de comandos. Para obtener más información, consulte Connect a un ordenador virtual de Lightsail for Research mediante Secure Shell.
- Conéctese a su equipo virtual mediante SCP para transferir archivos de forma segura. Para obtener más información, consulte Transfiera archivos a ordenadores virtuales de Lightsail for Research mediante Secure Copy.

Connect a un ordenador virtual de Lightsail for Research mediante Secure Shell

Puede conectarse a un ordenador virtual en Amazon Lightsail for Research mediante el protocolo Secure Shell (SSH). Puede usar SSH para administrar su equipo virtual de forma remota, de modo que pueda iniciar sesión en este a través de Internet y ejecutar comandos.

> **Note**
>
> También puede establecer una conexión de protocolo de pantalla remota a su ordenador virtual mediante el cliente Amazon DCV basado en navegador. Amazon DCV está disponible en la consola Lightsail for Research. Para obtener más información, consulte Acceda al sistema operativo de su ordenador virtual Lightsail for Research.

Temas

Cumplimiento de los requisitos previos de

Complete los siguientes requisitos previos antes de comenzar.

- Cree un ordenador virtual en Lightsail for Research. Para obtener más información, consulte Cree un ordenador virtual Lightsail for Research.
- Asegúrese de que el equipo virtual al que desea conectarse se encuentra en estado de ejecución. Además, anote el nombre de la computadora virtual y la AWS región en la que se creó. Necesitará esta información más adelante en este proceso. Para obtener más información, consulte Ver detalles de la computadora virtual de Lightsail for Research.
- Asegúrese de que el puerto 22 está abierto en el equipo virtual al que desea conectarse. Este es el puerto predeterminado que se utiliza para SSH. Está abierto de forma predeterminada. Sin embargo, si lo ha cerrado, debe volver a abrirlo antes de continuar. Para obtener más información, consulte Administre los puertos de firewall para los ordenadores virtuales Lightsail for Research.

- Obtenga el key pair predeterminado de Lightsail (DKP) para su ordenador virtual. Para obtener más información, consulte Obtención de un par de claves para un equipo virtual.

> **Tip**
>
> Si planea usarlo para conectarse AWS CloudShell a su computadora virtual, consulte la siguiente Conéctese a un ordenador virtual mediante AWS CloudShell sección. Para obtener más información, consulte Qué es AWS CloudShell. De lo contrario, continúe con el siguiente requisito previo.

- Descargue e instale el AWS Command Line Interface (AWS CLI). Para obtener más información, consulte Instalar o actualizar la última versión de la AWS CLI en la Guía del usuario de AWS Command Line Interface de la versión 2.
- Configure el AWS CLI para acceder a su Cuenta de AWS. Para obtener más información, consulte Fundamentos de configuración en la Guía del usuario de AWS Command Line Interface de la versión 2.
- Descargue e instale jq. Es un procesador de JSON de línea de comandos ligero y flexible que se utiliza en los siguientes procedimientos para extraer detalles de los pares de claves. Para obtener más información sobre la descarga e instalación de jq, consulte Download jq en el sitio web de jq.

Conexión a un equipo virtual mediante SSH

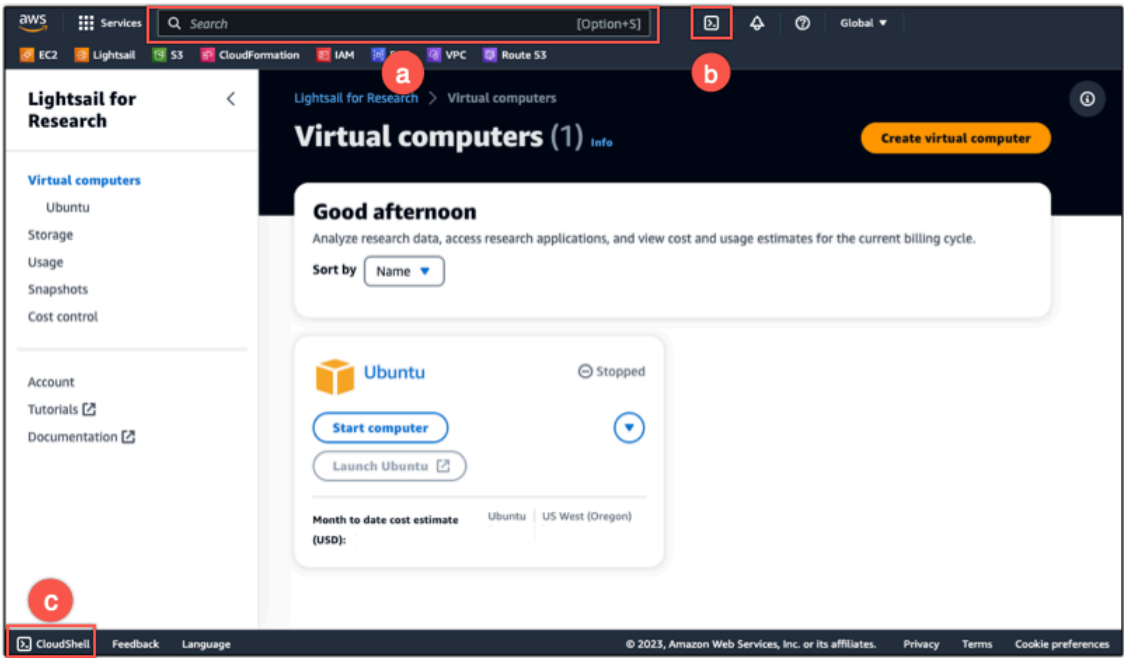
Realice uno de los siguientes procedimientos para establecer una conexión SSH con su ordenador virtual en Lightsail for Research.

Conéctese a un ordenador virtual mediante AWS CloudShell

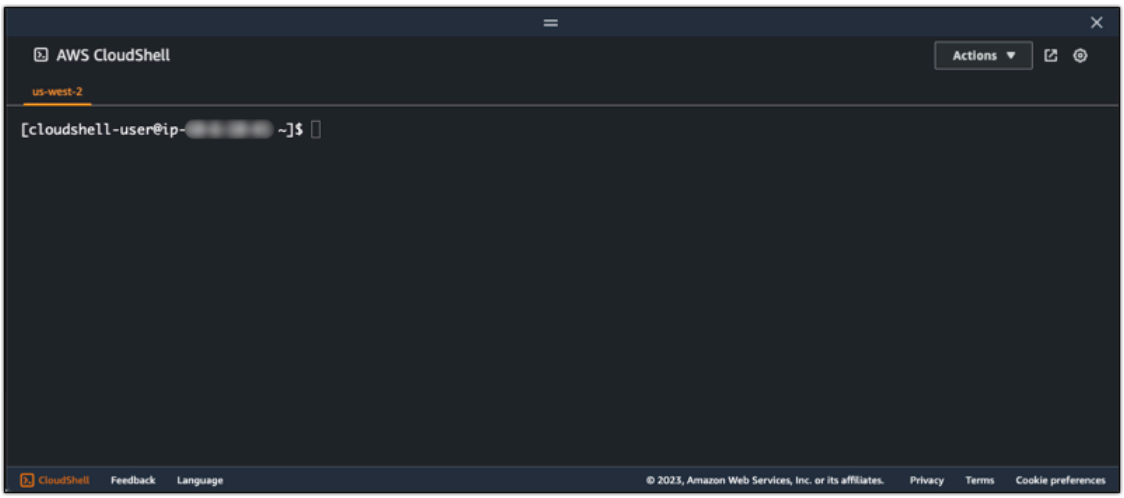
Este procedimiento se aplica si prefiere una configuración mínima para conectarse al equipo virtual. AWS CloudShell utiliza un shell preautenticado y basado en un navegador que puede iniciar directamente desde. Consola de administración de AWS Puede ejecutar AWS CLI comandos con el shell que prefiera, como el shell Bash o el shell Z. PowerShell Puede hacerlo sin necesidad de descargar ni instalar herramientas de línea de comandos. Para obtener más información, consulte el Cómo empezar a usar AWS CloudShell en la Guía del usuario de AWS CloudShell .

> **Important**
>
> Antes de empezar, asegúrese de obtener el key pair predeterminado de Lightsail (DKP) para el ordenador virtual al que se va a conectar. Para obtener más información, consulte Obtenga un par de claves para un ordenador virtual Lightsail for Research.

1. Desde la consola Lightsail for Research, CloudShell ejecútelo seleccionando una de las siguientes opciones:
   a. En el cuadro de búsqueda, escriba "CloudShell«y, a continuación, elija. CloudShell
   b. En la barra de navegación, elija el icono CloudShell.
   c. Seleccione CloudShellen la barra de herramientas de la consola, en la parte inferior izquierda de la consola.



Cuando aparece el símbolo del sistema, el shell está listo para la interacción.



2. Elija una carcasa preinstalada con la que trabajar. Para cambiar el shell predeterminado, introduzca uno de los siguientes nombres de programa en la línea de comandos. Bashes el shell predeterminado que se ejecuta cuando se inicia AWS CloudShell.

   Bash

   ```
   bash
   ```

   Si cambia a Bash, el símbolo de la línea de comandos se actualizará a $.

   PowerShell

   ```
   pwsh
   ```

   Si cambias a PowerShell, el símbolo de la línea de comandos se actualizará aPS>.

   Z shell

   ```
   zsh
   ```

   Si cambia a Z shell, el símbolo de la línea de comandos se actualizará a %.

3. Para conectarse a un ordenador virtual desde la ventana del CloudShell terminal, consulteConexión a un equipo virtual mediante SSH en un equipo local con Linux, Unix o macOS.

Para obtener información sobre el software preinstalado en el CloudShell entorno, consulte el entorno AWS CloudShell informático en la Guía del AWS CloudShell usuario.

Conexión a un equipo virtual mediante SSH en un equipo local con Windows

Este procedimiento se aplica si el equipo local utiliza un sistema operativo Windows. Este procedimiento utiliza el `get-instance` AWS CLI comando para obtener el nombre de usuario y la dirección IP pública de la instancia a la que desea conectarse. Para obtener más información, consulte get-instance en la Referencia de comandos de la AWS CLI .

> **Important**
>
> Asegúrese de obtener el key pair (DKP) predeterminado de Lightsail para el ordenador virtual al que intenta conectarse antes de iniciar este procedimiento. Para obtener más información, consulte Obtenga un par de claves para un ordenador virtual Lightsail for Research. Este procedimiento envía la clave privada del Lightsail DKP a `dkp_rsa` un archivo que se utiliza en uno de los siguientes comandos.

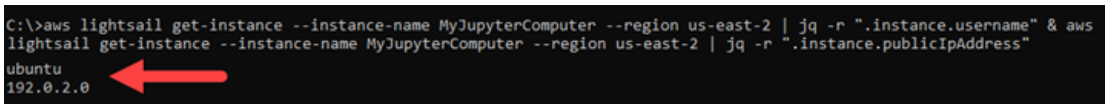
1. Abra una ventana del símbolo del sistema.
2. Ingrese el siguiente comando para mostrar la dirección IP pública y el nombre de usuario de su equipo virtual. En el comando, *`region-code`* sustitúyala por el código Región de AWS en el que se creó la computadora virtual, por ejemplo. `us-east-2` Sustituya *`computer-name`* por el nombre del equipo virtual al que desea conectarse.

   ```
   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"
   ```

   Ejemplo

   ```
   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"
   ```

   En la respuesta se mostrará el nombre de usuario y la dirección IP pública del equipo virtual, como se indica en el siguiente ejemplo. Anote estos valores, ya que los necesitará en el siguiente paso de este procedimiento.

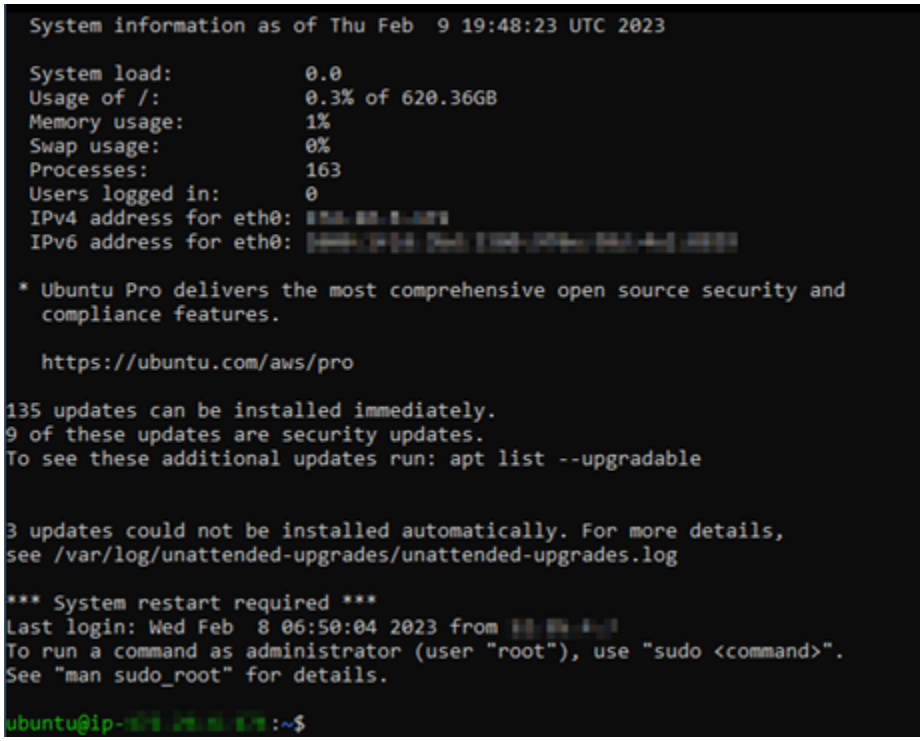
3. Ingrese el siguiente comando para establecer una conexión SSH con su equipo virtual. En el comando, sustituya *user-name* por el nombre de usuario de inicio de sesión y sustituya *public-ip-address* por la dirección IP pública de su equipo virtual.

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

Ejemplo

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

Debería ver una respuesta similar a la del siguiente ejemplo, que muestra una conexión SSH establecida con un ordenador virtual Ubuntu en Lightsail for Research.



Ahora que ha establecido correctamente una conexión SSH con su equipo virtual, continúe con la siguiente sección para consultar los siguientes pasos adicionales.

Conexión a un equipo virtual mediante SSH en un equipo local con Linux, Unix o macOS

Este procedimiento se aplica si el equipo local utiliza un sistema operativo Linux, Unix o macOS. Este procedimiento utiliza el `get-instance` AWS CLI comando para obtener el nombre de usuario

y la dirección IP pública de la instancia a la que desea conectarse. Para obtener más información, consulte get-instance en la Referencia de comandos de la AWS CLI .

> **Important**
>
> Asegúrese de obtener el key pair (DKP) predeterminado de Lightsail para el ordenador virtual al que intenta conectarse antes de iniciar este procedimiento. Para obtener más información, consulte Obtenga un par de claves para un ordenador virtual Lightsail for Research. Este procedimiento envía la clave privada del Lightsail DKP a `dkp_rsa` un archivo que se utiliza en uno de los siguientes comandos.

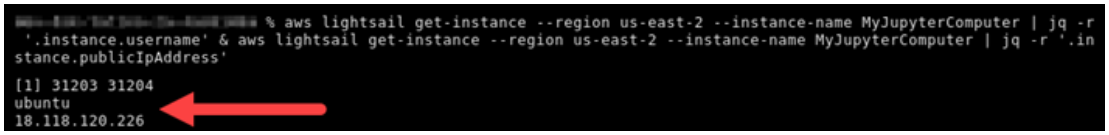
1. Abra una ventana de terminal.
2. Ingrese el siguiente comando para mostrar la dirección IP pública y el nombre de usuario de su equipo virtual. En el comando, *`region-code`* sustitúyalo por el código de la AWS región en la que se creó la computadora virtual, por ejemplo. `us-east-2` Sustituya *`computer-name`* por el nombre del equipo virtual al que desea conectarse.

   ```
   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'
   ```

   Ejemplo

   ```
   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'
   ```

   En la respuesta se mostrará el nombre de usuario y la dirección IP pública del equipo virtual, como se indica en el siguiente ejemplo. Anote estos valores, ya que los necesitará en el siguiente paso de este procedimiento.

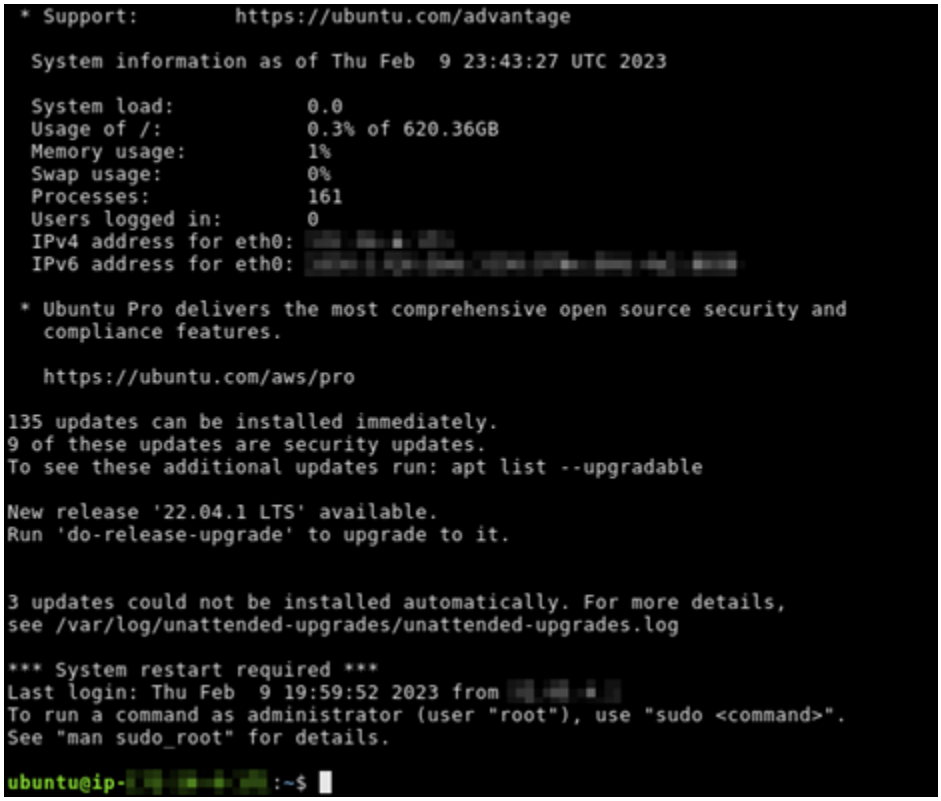
3. Ingrese el siguiente comando para establecer una conexión SSH con su equipo virtual. En el comando, sustituya *`user-name`* por el nombre de usuario de inicio de sesión y sustituya *`public-ip-address`* por la dirección IP pública de su equipo virtual.

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

Ejemplo

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

Debería ver una respuesta similar a la del siguiente ejemplo, que muestra una conexión SSH establecida con un ordenador virtual Ubuntu en Lightsail for Research.



Ahora que ha establecido correctamente una conexión SSH con su equipo virtual, continúe con la siguiente sección para consultar los siguientes pasos adicionales.

Continúe con los pasos siguientes.

Puede completar los siguientes pasos adicionales una vez que haya establecido correctamente una conexión SSH con su equipo virtual:

- Conéctese a su equipo virtual mediante SCP para transferir archivos de forma segura. Para obtener más información, consulte Transfiera archivos a ordenadores virtuales de Lightsail for Research mediante Secure Copy.

Transfiera archivos a ordenadores virtuales de Lightsail for Research mediante Secure Copy

Puede transferir archivos desde su ordenador local a un ordenador virtual en Amazon Lightsail for Research mediante Secure Copy (SCP). Con este proceso, puede transferir varios archivos, o directorios completos, a la vez.

> **Note**
>
> También puede establecer una conexión de protocolo de pantalla remota a su ordenador virtual mediante el cliente Amazon DCV basado en navegador disponible en la consola de Lightsail for Research. Con el cliente Amazon DCV, puede transferir rápidamente archivos individuales. Para obtener más información, consulte Acceda al sistema operativo de su ordenador virtual Lightsail for Research.

Temas

Cumplimiento de los requisitos previos de

Complete los siguientes requisitos previos antes de comenzar.

- Cree un ordenador virtual en Lightsail for Research. Para obtener más información, consulte Cree un ordenador virtual Lightsail for Research.
- Asegúrese de que el equipo virtual al que desea conectarse se encuentra en estado de ejecución. Además, anote el nombre del equipo virtual y la región de AWS en la que se creó. Necesitará esta información más adelante en este mismo proceso. Para obtener más información, consulte Ver detalles de la computadora virtual de Lightsail for Research.

- Descargue e instale el AWS Command Line Interface ()AWS CLI. Para obtener más información, consulte Instalar o actualizar la última versión de la AWS CLI en la Guía del usuario de AWS Command Line Interface de la versión 2.
- Configure el AWS CLI para acceder a su Cuenta de AWS. Para obtener más información, consulte Fundamentos de configuración en la Guía del usuario de AWS Command Line Interface de la versión 2.
- Descargue e instale jq. Es un procesador de JSON de línea de comandos ligero y flexible que se utiliza en los siguientes procedimientos para extraer detalles de los pares de claves. Para obtener más información sobre la descarga e instalación de jq, consulte Download jq en el sitio web de jq.
- Asegúrese de que el puerto 22 está abierto en el equipo virtual al que desea conectarse. Este es el puerto predeterminado que se utiliza para SSH. Está abierto de forma predeterminada. Sin embargo, si lo ha cerrado, debe volver a abrirlo antes de continuar. Para obtener más información, consulte Administre los puertos de firewall para los ordenadores virtuales Lightsail for Research.
- Obtenga el key pair predeterminado de Lightsail (DKP) para su ordenador virtual. Para obtener más información, consulte Cree un ordenador virtual Lightsail for Research.

Conexión a un equipo virtual mediante SCP

Realice uno de los siguientes procedimientos para conectarse a su ordenador virtual en Lightsail for Research mediante SCP.

Conexión a un equipo virtual mediante SCP en un equipo local con Windows

Este procedimiento se aplica a su caso si su equipo local utiliza un sistema operativo Windows. Este procedimiento utiliza el `get-instance` AWS CLI comando para obtener el nombre de usuario y la dirección IP pública de la instancia a la que desea conectarse. Para obtener más información, consulte get-instance en la Referencia de comandos de la AWS CLI .

> **Important**
>
> Asegúrese de obtener el key pair (DKP) predeterminado de Lightsail para el ordenador virtual al que intenta conectarse antes de iniciar este procedimiento. Para obtener más información, consulte Obtenga un par de claves para un ordenador virtual Lightsail for Research. Este procedimiento envía la clave privada del Lightsail DKP a `dkp_rsa` un archivo que se utiliza en uno de los siguientes comandos.

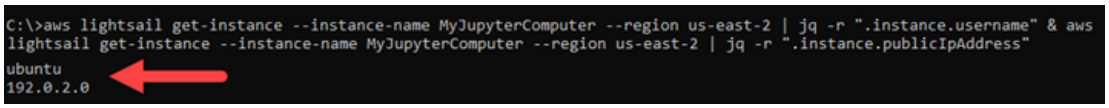
1. Abra una ventana del símbolo del sistema.
2. Ingrese el siguiente comando para mostrar la dirección IP pública y el nombre de usuario de su equipo virtual. En el comando, *region-code* sustitúyalo por el código de la AWS región en la que se creó la computadora virtual, por ejemplo. `us-east-2` Sustituya *computer-name* por el nombre del equipo virtual al que desea conectarse.

```
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"
```

   Ejemplo

```
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"
```

   En la respuesta se mostrará el nombre de usuario y la dirección IP pública del equipo virtual, como se indica en el siguiente ejemplo. Anote estos valores, ya que los necesitará en el siguiente paso de este procedimiento.



3. Ingrese el siguiente comando para establecer una conexión SCP con su equipo virtual y transferir archivos a este.

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

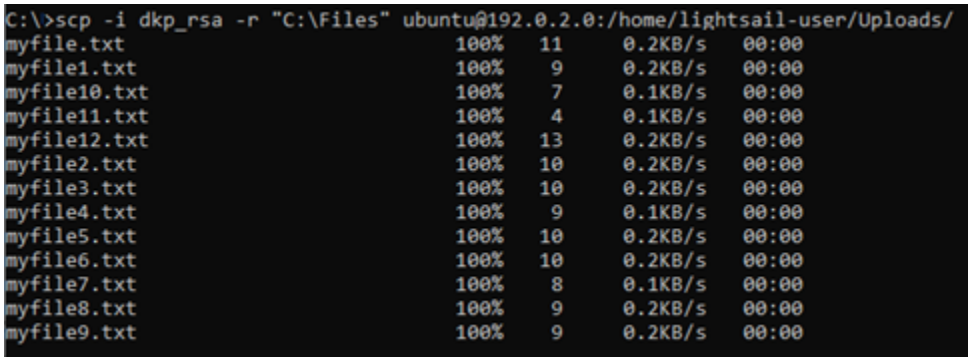
   En el comando, sustituya:

   - *source-folder* con la carpeta del equipo local que contiene los archivos que desea transferir.
   - *user-name* con el nombre de usuario del paso anterior de este procedimiento (por ejemplo, `ubuntu`).
   - *public-ip-address* con la dirección IP pública del equipo virtual del paso anterior de este procedimiento.
   - *destination-directory* con la ruta del directorio del equipo virtual en el que desea copiar los archivos.

El siguiente ejemplo copia todos los archivos de la carpeta `C:\Files` del equipo local al directorio `/home/lightsail-user/Uploads/` del equipo virtual remoto.

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

Debería ver una respuesta similar a la del siguiente ejemplo. Muestra todos los archivos que se han transferido de la carpeta de origen al directorio de destino. Ahora debería poder acceder a esos archivos en su equipo virtual.



Conexión a un equipo virtual mediante SCP en un equipo local con Linux, Unix o macOS

Este procedimiento se aplica a su caso si su equipo local utiliza un sistema operativo Linux, Unix o macOS. Este procedimiento utiliza el `get-instance` AWS CLI comando para obtener el nombre de usuario y la dirección IP pública de la instancia a la que desea conectarse. Para obtener más información, consulte get-instance en la Referencia de comandos de la AWS CLI .

> **Important**
>
> Asegúrese de obtener el key pair (DKP) predeterminado de Lightsail para el ordenador virtual al que intenta conectarse antes de iniciar este procedimiento. Para obtener más información, consulte Obtenga un par de claves para un ordenador virtual Lightsail for Research. Este procedimiento envía la clave privada del Lightsail DKP a `dkp_rsa` un archivo que se utiliza en uno de los siguientes comandos.

1. Abra una ventana de terminal.
2. Ingrese el siguiente comando para mostrar la dirección IP pública y el nombre de usuario de su equipo virtual. En el comando, *`region-code`* sustitúyalo por el código de la AWS región en la

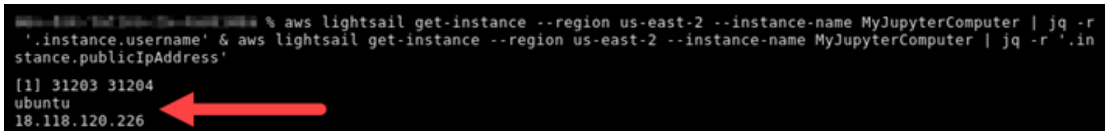
que se creó la computadora virtual, por ejemplo. `us-east-2` Sustituya *`computer-name`* por el nombre del equipo virtual al que desea conectarse.

```
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'
```

Ejemplo

```
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'
```

En la respuesta se mostrará el nombre de usuario y la dirección IP pública del equipo virtual, como se indica en el siguiente ejemplo. Anote estos valores, ya que los necesitará en el siguiente paso de este procedimiento.



3. Ingrese el siguiente comando para establecer una conexión SCP con su equipo virtual y transferir archivos a este.

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

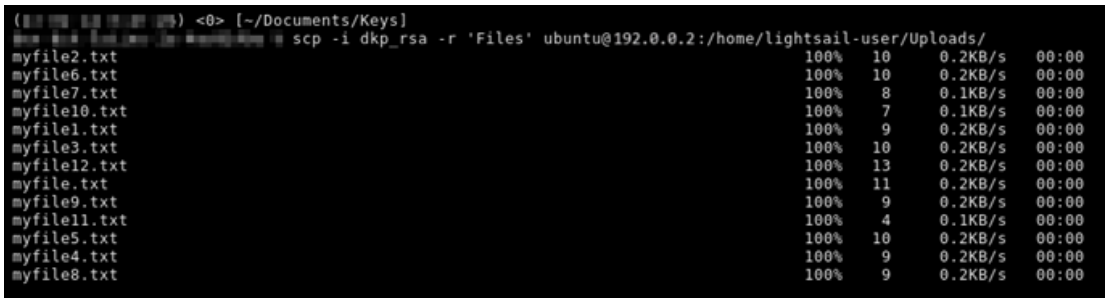
En el comando, sustituya:

- *`source-folder`* con la carpeta del equipo local que contiene los archivos que desea transferir.
- *`user-name`* con el nombre de usuario del paso anterior de este procedimiento (por ejemplo, `ubuntu`).
- *`public-ip-address`* con la dirección IP pública del equipo virtual del paso anterior de este procedimiento.
- *`destination-directory`* con la ruta del directorio del equipo virtual en el que desea copiar los archivos.

El siguiente ejemplo copia todos los archivos de la carpeta `C:\Files` del equipo local al directorio `/home/lightsail-user/Uploads/` del equipo virtual remoto.

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

Debería ver una respuesta similar a la del siguiente ejemplo. Muestra todos los archivos que se han transferido de la carpeta de origen al directorio de destino. Ahora debería poder acceder a esos archivos en su equipo virtual.



Eliminar un ordenador virtual de Lightsail for Research

Complete los siguientes pasos para eliminar su ordenador virtual Lightsail for Research cuando ya no lo necesite. Dejarán de acumularse cargos por el equipo virtual en cuanto lo elimine. Los recursos adjuntos al equipo eliminado, como, por ejemplo, instantáneas, seguirán acumulando cargos hasta que se eliminen.

> **Important**
>
> Eliminar un equipo virtual es una acción permanente y el equipo no se puede recuperar. Si necesita los datos más adelante, cree una instantánea del equipo virtual antes de eliminarlo. Para obtener más información, consulte Create a snapshot.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Equipos virtuales.
3. Elija el equipo virtual que desea eliminar.
4. Seleccione Acciones y, a continuación, elija Eliminar equipo virtual.
5. Escriba confirmar en el bloque de texto. A continuación, elija Eliminar equipo virtual.

Proteja y almacene los datos con Lightsail for Research

Amazon Lightsail for Research proporciona volúmenes de almacenamiento a nivel de bloques (discos) que puede conectar a un ordenador virtual de Lightsail for Research en ejecución. Puede utilizar un disco como dispositivo de almacenamiento principal para los datos que requieran actualizaciones frecuentes y detalladas. Por ejemplo, los discos son la opción de almacenamiento recomendada cuando se ejecuta una base de datos en un ordenador virtual Lightsail for Research.

Un disco se comporta como un dispositivo de bloques externo sin formatear que puede adjuntar a un único equipo virtual. El volumen persiste, independientemente de la vida de ejecución de una instancia. Después de adjuntar un disco a un equipo, puede usarlo como cualquier otro disco duro físico.

Puede adjuntar varios discos a un equipo. También puede desasociar un disco de un equipo y adjuntarlo a otro equipo.

Para mantener una copia de seguridad de los datos, cree una instantánea del disco. Puede crear un nuevo disco a partir de una instantánea y adjuntarlo a otro equipo.

Temas

Cree un disco de almacenamiento en la consola de Lightsail for Research

Complete los siguientes pasos para crear un disco para su ordenador virtual Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Almacenamiento.
3. Elija Crear disco.

4. Escriba un nombre para el disco. Los caracteres válidos son caracteres alfanuméricos, números, puntos, guiones y guiones bajos.

   Los nombres de los discos deben cumplir con los siguientes requisitos:

   - Sea único en cada uno de ellos Región de AWS en su cuenta de Lightsail for Research.
   - Contener entre 2 y 255 caracteres.
   - Comenzar y terminar por un carácter alfanumérico o un número.
5. Elija una Región de AWS para su disco.

   El disco debe estar en la misma región que el equipo virtual al que desea adjuntarlo.
6. Elija el tamaño del disco en GB.
7. Continúe hasta la sección Adjuntar un disco para obtener información sobre cómo adjuntar discos a su equipo virtual.

Vea los detalles del disco de almacenamiento en la consola de Lightsail for Research

Complete los siguientes pasos para ver los discos de su cuenta de Lightsail for Research y sus detalles.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Almacenamiento.

   La página Almacenamiento proporciona una vista completa de los discos de su cuenta de Lightsail for Research.

   En dicha página se muestra la siguiente información:

   - Nombre: nombre del disco de almacenamiento.
   - Tamaño: tamaño del disco (en GB).
   - Región de AWS: Región de AWS en la que se creó el disco.
   - Conectado a: el ordenador Lightsail al que está conectado el disco.
   - Fecha de creación: fecha en que se creó el disco.

Añada almacenamiento a un ordenador virtual en Lightsail for Research

Complete los siguientes pasos para conectar un disco a un ordenador virtual en Lightsail for Research. Puede adjuntar hasta 15 discos a un equipo virtual. Al conectar un disco a su ordenador virtual mediante la consola Lightsail for Research, el servicio lo formateará y montará automáticamente. Este proceso tarda unos minutos, por lo que debe confirmar que el disco ha alcanzado el estado de montaje Montado antes de empezar a usarlo. De forma predeterminada, Lightsail for Research monta los discos en `/home/lightsail-user/<disk-name>` el directorio, `<disk-name>` donde es el nombre que le dio al disco.

> **Important**
>
> Para poder adjuntar un disco a un equipo virtual, el equipo virtual debe encontrarse en estado En ejecución. Si adjunta un disco a un equipo virtual mientras se encuentra en estado Detenido, el disco se adjuntará pero no se podrá montar. Si el estado de montaje del disco es Error, debe desasociar el disco y volver a adjuntarlo cuando el equipo virtual se encuentre en estado En ejecución.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Equipos virtuales.
3. Elija el equipo al que desee adjuntar el disco.
4. Elija la pestaña Almacenamiento.
5. Elija Adjuntar disco.
6. Seleccione el nombre del disco que desee adjuntar al equipo.
7. Elija Adjuntar.

Separe un disco de un ordenador virtual en Lightsail for Research

Complete los siguientes pasos para desasociar un disco de un equipo.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Almacenamiento.

3. Busque el disco que desea desasociar. En la columna Adjuntado a, elija el nombre del equipo al que se ha adjuntado el disco.
4. Elija Detener para detener el equipo. Debe detener el equipo para poder desasociar el disco.
5. Confirme que desea detener el equipo y, a continuación, seleccione Detener equipo.
6. Elija la pestaña Almacenamiento.
7. Seleccione el disco que desee desasociar y, a continuación, elija Desasociar.
8. Confirme que desea desasociar el disco del equipo y, a continuación, seleccione Desasociar.

Elimine los discos de almacenamiento no utilizados en Lightsail for Research

Complete los siguientes pasos para eliminar un disco de almacenamiento cuando ya no lo necesite. Dejan de aplicarse cargos por el disco tan pronto como se elimina.

Si el disco se ha adjuntado a un equipo, primero debe desasociarlo para poder eliminarlo. Para obtener más información, consulte Separe un disco de un ordenador virtual en Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Almacenamiento.
3. Busque y seleccione el disco que desee eliminar.
4. Elija Eliminar disco.
5. Confirme que desea eliminar el disco. A continuación, elija Eliminar.

Backup de ordenadores y discos virtuales con instantáneas de Lightsail for Research

Las instantáneas son una point-in-time copia de sus datos. Puede crear instantáneas de sus ordenadores virtuales y discos de almacenamiento de Amazon Lightsail for Research y utilizarlos como líneas base para crear nuevos ordenadores o para realizar copias de seguridad de datos.

Una instantánea contiene todos los datos necesarios para restaurar el equipo (desde el momento en que se hizo la instantánea). Cuando se crea un equipo virtual nuevo a partir de una instantánea, comienza como una réplica exacta del equipo original utilizado para crear la instantánea.

Como sus recursos pueden fallar en cualquier momento, le recomendamos crear instantáneas frecuentes para evitar la pérdida permanente de datos.

Temas

Cree instantáneas de ordenadores o discos virtuales de Lightsail for Research

Complete los siguientes pasos para crear una instantánea de su ordenador o disco virtual de Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research.
2. Elija Snapshots (Instantáneas) en el panel de navegación.
3. Complete uno de los pasos siguientes:

    - En Instantáneas de equipos virtuales, busque el nombre del equipo del que desee tomar una instantánea y seleccione Crear instantánea.
    - En Instantáneas de disco, busque el nombre del disco del que desee tomar una instantánea y seleccione Crear instantánea.

4. Escriba un nombre para la instantánea. Los caracteres válidos son caracteres alfanuméricos, números, puntos, guiones y guiones bajos.

   Los nombres de las instantáneas deben cumplir con los siguientes requisitos:

   - Sea único en cada uno de ellos Región de AWS en su cuenta de Lightsail for Research.
   - Contener entre 2 y 255 caracteres.
   - Comenzar y terminar por un carácter alfanumérico o un número.
5. Seleccione Create snapshot (Crear instantánea).

Vea y gestione instantáneas de ordenadores y discos virtuales en Lightsail for Research

Complete los siguientes pasos para ver las instantáneas de sus equipos virtuales y discos.

1. Inicie sesión en la consola de Lightsail for Research.
2. Elija Snapshots (Instantáneas) en el panel de navegación.

   En la página Instantáneas se muestran las instantáneas de los equipos virtuales y los discos que haya creado.

   Las instantáneas archivadas también se encuentran en esta página. Las instantáneas archivadas son instantáneas de los recursos que se han eliminado de su cuenta.

Creación de un equipo virtual o un disco a partir de una instantánea

Complete los siguientes pasos para crear un nuevo ordenador virtual o disco de Lightsail for Research a partir de una instantánea.

Al crear un equipo virtual a partir de una instantánea, utilice un plan del mismo tamaño o más grande que el utilizado para el equipo original. No puede usar un plan más pequeño que el equipo virtual original.

Cuando cree un disco a partir de una instantánea, elija un tamaño de disco mayor que el disco original. No puede usar un disco más pequeño que el original.

1. Inicie sesión en la consola de Lightsail for Research.

2. Elija Snapshots (Instantáneas) en el panel de navegación.
3. En la página Instantáneas, busque el nombre de la instantánea del equipo o disco que utilizará para crear el nuevo equipo o disco. Selecciona el menú desplegable Instantáneas para ver una lista de las instantáneas disponibles para ese recurso.
4. Seleccione la instantánea que desee utilizar para crear el equipo virtual.
5. Elija el menú desplegable Acciones. A continuación, elija Crear equipo virtual o Crear disco.

Eliminar una instantánea en la consola de Lightsail for Research

Complete los siguientes pasos para eliminar una instantánea.

1. Inicie sesión en la consola de Lightsail for Research.
2. Elija Snapshots (Instantáneas) en el panel de navegación.
3. En la página Instantáneas, busque el nombre de la instantánea del equipo o disco que desee eliminar. Selecciona el menú desplegable Instantáneas para ver una lista de las instantáneas disponibles para ese recurso.
4. Seleccione la instantánea que desee eliminar.
5. Elija el menú desplegable Acciones. A continuación, elija Eliminar instantánea.
6. Verifique que el nombre de la instantánea sea correcto. A continuación, elija Eliminar instantánea.

Estimaciones de costos y uso en Lightsail for Research

Amazon Lightsail for Research ofrece estimaciones de costos y uso de sus recursos. AWS Puede utilizar estas estimaciones para planificar sus gastos, encontrar oportunidades de ahorro de costes y tomar decisiones informadas cuando utilice Lightsail for Research.

Al crear un disco o un equipo virtual, se muestran las estimaciones de costos y uso de ese recurso. Se comienza a hacer un seguimiento de una estimación de costo y uso tan pronto como se crea un recurso y se encuentra en estado Disponible o En ejecución. La estimación aparecerá en la Consola de administración de AWS 15 minutos después de crear el recurso. Los recursos que se han eliminado no se incluyen en una estimación.

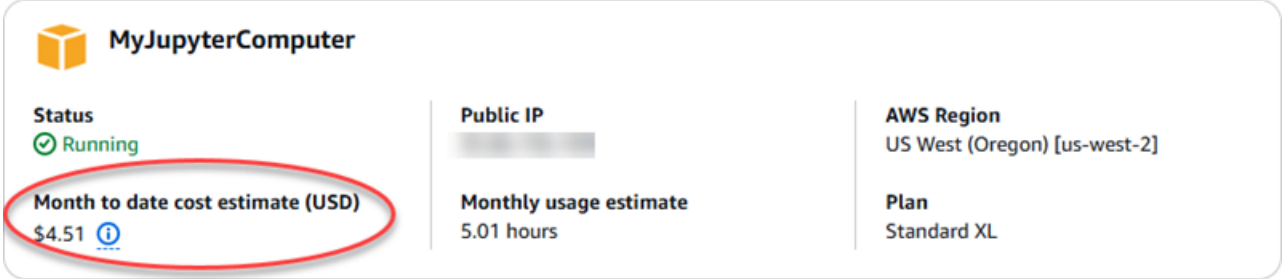
> **Important**
>
> Una estimación es un costo estimado que se basa en el uso del recurso. El coste real se basará en el uso real de los recursos, no en la estimación que se muestra en la consola de Lightsail for Research. Los costos reales se muestran en su estado de AWS Billing cuenta. Inicie sesión en Consola de administración de AWS y abra la Administración de facturación y costos de AWS consola en https://console.aws.amazon.com/costmanagement/.

Temas

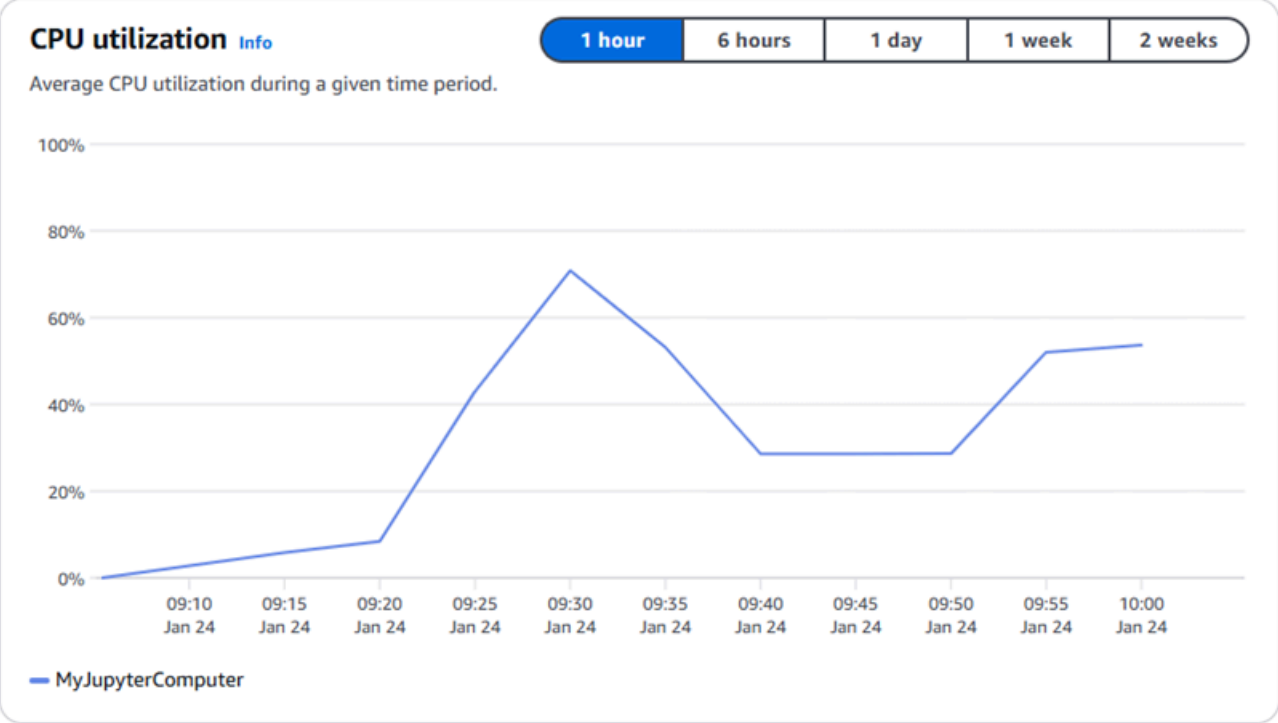
Consulte las estimaciones de costo y uso de sus recursos en Lightsail for Research

Las estimaciones de coste y uso mensuales de sus recursos de Lightsail for Research se muestran en las siguientes áreas de la consola de Lightsail for Research.

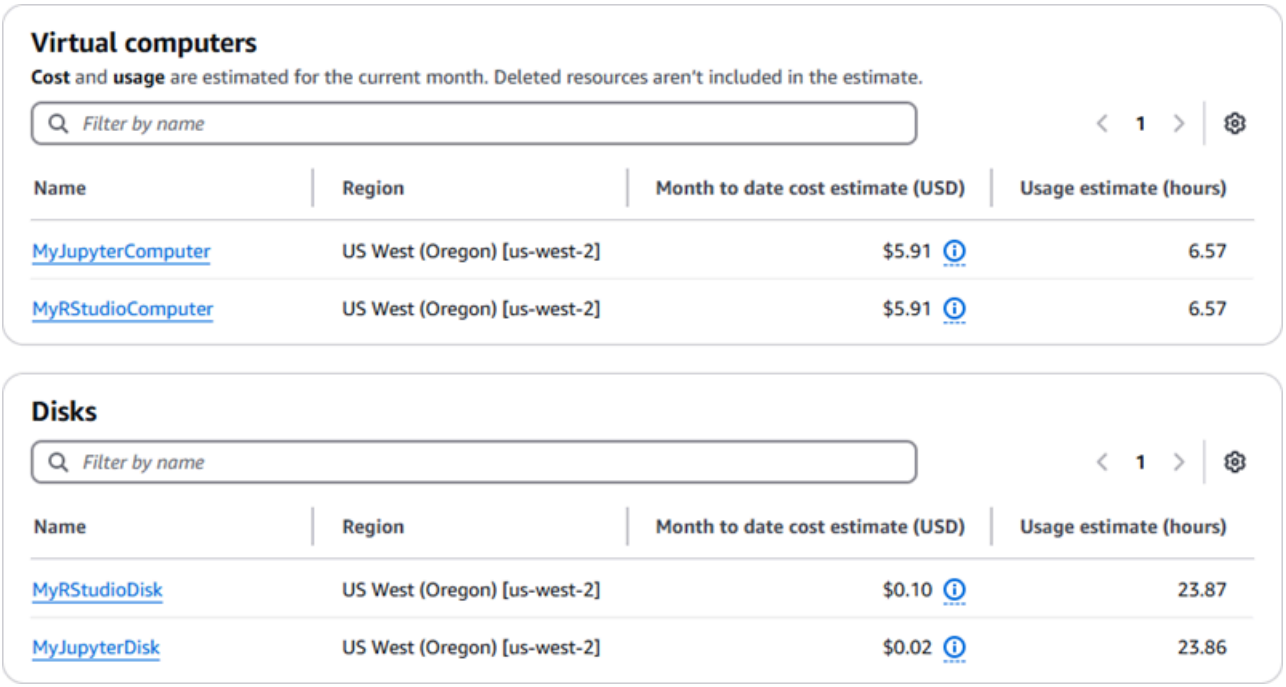
1. Seleccione Ordenadores virtuales en el panel de navegación de la consola de Lightsail for Research. La estimación del costo mensual de sus equipos virtuales hasta la fecha aparece debajo de cada equipo virtual en ejecución.



2. Para ver el uso de la CPU de un equipo virtual, elija el nombre del equipo virtual y, a continuación, elija la pestaña Panel.



3. Para ver las estimaciones de costo y uso del mes hasta la fecha de todos sus recursos de Lightsail for Research, seleccione Uso en el panel de navegación.



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 West (Oregon) [us-west-2]	$5.91	6.57
MyRStudioComputer	US West (Oregon) [us-west-2]	$5.91	6.57

Disks

Filter by name

1

Name	Region	Month to date cost estimate (USD)	Usage estimate (hours)
MyRStudioDisk	US West (Oregon) [us-west-2]	$0.10	23.87
MyJupyterDisk	US West (Oregon) [us-west-2]	$0.02	23.86

Gestione las reglas de control de costes en Lightsail for Research

El control de costos usa reglas que usted define para ayudar a administrar el uso y el costo de sus ordenadores virtuales Lightsail for Research.

Puede crear una regla Detener el equipo virtual inactivo que detenga un equipo en ejecución cuando alcance un porcentaje específico de uso de la CPU durante un periodo determinado. Por ejemplo, una regla puede detener automáticamente un equipo específico cuando el uso de la CPU es igual o inferior al 5 % durante un periodo de 30 minutos. Esto significa que el equipo está inactivo y Lightsail for Research lo detiene. Dejará de incurrir en los cargos por hora estándar una vez que se detenga el equipo virtual.

Temas

Cree reglas de control de costes para sus ordenadores virtuales Lightsail for Research

Complete los siguientes pasos para crear una regla para su ordenador virtual Lightsail for Research.

> **Note**
>
> La única acción de regla admitida en este momento es la detención de un equipo virtual. El uso de la CPU es la única métrica que actualmente supervisan las reglas y la única operación admitida es menor o igual que.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Control de costos.
3. Seleccione Creación de regla.
4. Seleccione el recurso al que desee aplicar la regla.

5. Especifique el porcentaje de uso de la CPU y el periodo de tiempo en el que debe ejecutarse la regla.

   Por ejemplo, puede especificar el 5 por ciento y 30 minutos. Lightsail for Research detiene automáticamente el ordenador cuando el uso de la CPU es inferior o igual al 5 por ciento durante un período de 30 minutos.
6. Seleccione Creación de regla.
7. Confirme que la información de la nueva regla es correcta y, a continuación, seleccione Confirmar.

Elimine las reglas de control de costes de sus ordenadores virtuales Lightsail for Research

Complete los siguientes pasos para eliminar una regla de su ordenador virtual Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research.
2. En el panel de navegación, elija Control de costos.
3. Seleccione la regla que desea eliminar.
4. Elija Eliminar.
5. Verifique que desea eliminar la regla y elija Eliminar.

Organice los recursos de Lightsail for Research con etiquetas

Con Amazon Lightsail for Research, puede asignar etiquetas a sus recursos. Cada etiqueta es una marca que consta de una clave y un valor opcional que puede hacer que sea eficiente administrar sus recursos. Una clave sin un valor se denomina etiqueta de solo clave y una clave con un valor se denomina etiqueta de clave-valor. Aunque no hay tipos inherentes de etiquetas, le permiten clasificar los recursos según su finalidad, propietario, entorno u otro criterio. Esto es útil cuando se tienen muchos recursos del mismo tipo. Puede identificar rápidamente un recurso específico según las etiquetas que le haya asignado. Por ejemplo, puede definir un conjunto de etiquetas que lo ayude a realizar un seguimiento del proyecto de cada uno de los recursos o de la prioridad.

Los siguientes recursos se pueden etiquetar en la consola de Amazon Lightsail for Research:

- Equipos virtuales
- Discos de almacenamiento
- Instantáneas

Se aplican las siguientes restricciones a las etiquetas:

- El número máximo de etiquetas por recurso es 50.
- Para cada recurso, cada clave de etiqueta debe ser única. Cada clave de etiqueta solo puede tener un valor.
- La longitud máxima de la clave es de 128 caracteres Unicode en UTF-8.
- La longitud máxima del valor es de 256 caracteres Unicode en UTF-8.
- Si se utiliza su esquema de etiquetado en múltiples servicios y recursos de , recuerde que otros servicios podrían tener otras restricciones sobre caracteres permitidos. En general, los caracteres permitidos son letras, números, espacios y los siguientes caracteres: `+ - = . _ : / @`
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- No utilice el prefijo `aws:` para claves ni valores. Ese prefijo está reservado para su uso. AWS

Temas

- Etiqueta Lightsail para recursos de investigación

Etiqueta Lightsail para recursos de investigación

Complete los siguientes pasos para crear una etiqueta para su ordenador virtual Lightsail for Research. Los pasos son similares para los discos e instantáneas de Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research en la consola de Lightsail for Research.
2. En el panel de navegación, elija Equipos virtuales.
3. Elija el equipo virtual para el que desea crear una etiqueta.
4. Elija la pestaña Etiquetas.
5. Elija Manage tags (Administrar etiquetas).
6. Elija Add new tag (Agregar nueva etiqueta).
7. Escriba un nombre de clave en el campo Clave. Por ejemplo, Proyecto.
8. (Opcional) Escriba un nombre de valor en el campo Valor. Por ejemplo, Blog.
9. Seleccione Guardar cambios para guardar la clave en su equipo virtual.

Eliminar etiquetas de los recursos de Lightsail for Research

Complete los siguientes pasos para eliminar una etiqueta de su ordenador virtual Lightsail for Research. Los pasos son similares para los discos e instantáneas de Lightsail for Research.

1. Inicie sesión en la consola de Lightsail for Research en la consola de Lightsail for Research.
2. En el panel de navegación, elija Equipos virtuales.
3. Elija el equipo virtual del que desea eliminar la etiqueta.
4. Elija la pestaña Etiquetas.
5. Elija Administrar etiquetas.
6. Elija Eliminar para eliminar la etiqueta del recurso.

> **Note**
>
> Si solo quiere eliminar el valor de la etiqueta, localice el valor y, a continuación, seleccione el ícono X que está junto a él.

7. Elija Guardar cambios.

La seguridad en Amazon Lightsail for Research

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener información sobre los programas de conformidad que se aplican a Amazon Lightsail for Research, AWS consulte Servicios incluidos en el ámbito de aplicación por programa de conformidad Servicios en el ámbito de aplicación por AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Lightsail for Research. En los temas siguientes se muestra cómo configurar Lightsail for Research para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Lightsail for Research.

Temas

Protección de datos en Amazon Lightsail for Research

El modelo de se aplica a protección de datos en Amazon Lightsail for Research. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los. Nube de AWS Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados que contienen Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Lightsail for Research u Servicios de AWS otro dispositivo mediante la consola, la API AWS CLI o. AWS SDKs Cualquier dato que introduzca

en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Identity and Access Management para Amazon Lightsail for Research

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda a un administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de Lightsail for Research. Puede utilizar el IAM Servicio de AWS sin coste adicional.

> **Note**
>
> Amazon Lightsail y Lightsail for Research comparten los mismos parámetros de política de IAM. Los cambios realizados en las políticas de Lightsail for Research también afectarán a las políticas de Lightsail. Por ejemplo, si un usuario tiene permiso para crear un disco en Lightsail for Research, ese mismo usuario también puede crear un disco en Lightsail.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según su función:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Solución de problemas de identidad y acceso a Amazon Lightsail for Research).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Cómo funciona Amazon Lightsail for Research con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Ejemplos de políticas basadas en identidad para Amazon Lightsail for Research).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en la Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un Rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuario federado, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración del acceso con políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Los ejemplos incluyen las Políticas de confianza de roles de IAM y las Políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política basada en recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .

- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Amazon Lightsail for Research con IAM

Antes de usar IAM para administrar el acceso a Lightsail for Research, averigüe qué funciones de IAM están disponibles para usar con Lightsail for Research.

Funciones de IAM que puede utilizar con Amazon Lightsail for Research

Característica de IAM	Soporte de Lightsail for Research
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí

Característica de IAM	Soporte de Lightsail for Research
Permisos de entidades principales	No
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una visión general de cómo funcionan Lightsail for Research y AWS otros servicios con la mayoría de las funciones de IAM, AWS consulte los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para Lightsail for Research

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para Lightsail for Research

Para ver ejemplos de políticas basadas en la identidad de Lightsail for Research, consulte. Ejemplos de políticas basadas en identidad para Amazon Lightsail for Research

Políticas basadas en recursos en Lightsail for Research

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las

políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para Lightsail for Research

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Lightsail for Research, consulte Acciones definidas por Amazon Lightsail for Research en la Referencia de autorización de servicio.

Las acciones políticas de Lightsail for Research utilizan el siguiente prefijo antes de la acción:

```
lightsail
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas basadas en la identidad de Lightsail for Research, consulte. Ejemplos de políticas basadas en identidad para Amazon Lightsail for Research

Recursos de políticas para Lightsail for Research

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Lightsail for Research y ARNs sus respectivos tipos, consulte Recursos definidos por Amazon Lightsail for Research en la Referencia de autorización de servicio. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por Amazon Lightsail for Research.

Para ver ejemplos de políticas basadas en la identidad de Lightsail for Research, consulte. Ejemplos de políticas basadas en identidad para Amazon Lightsail for Research

Condiciones clave de la política de Lightsail for Research

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de claves de estado de Lightsail for Research, consulte Claves de estado de Amazon Lightsail for Research en la Referencia de autorización de servicio. Para saber con qué

acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por Amazon Lightsail for Research.

Para ver ejemplos de políticas basadas en la identidad de Lightsail for Research, consulte. Ejemplos de políticas basadas en identidad para Amazon Lightsail for Research

ACLs en Lightsail for Research

Soportes ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Lightsail para la investigación

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director coincida con la etiqueta del recurso.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Lightsail for Research

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para

obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Permisos principales de servicios cruzados para Lightsail for Research

Compatibilidad con sesiones de acceso directo (FAS): no

Las sesiones de acceso directo (FAS) utilizan los permisos del principal que llama y los que solicitan Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Funciones de servicio de Lightsail for Research

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Lightsail for Research. Edite las funciones de servicio solo cuando Lightsail for Research proporcione instrucciones para hacerlo.

Funciones vinculadas al servicio para Lightsail for Research

Compatibilidad con roles vinculados al servicio: no

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidad para Amazon Lightsail for Research

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de Lightsail for Research. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Lightsail for Research, incluido el formato de cada uno de ARNs los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon Lightsail for Research en la Referencia de autorización de servicio.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de Lightsail for Research de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se

pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola Lightsail for Research

Para acceder a la consola de Amazon Lightsail for Research, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Lightsail for Research en su. Cuenta de AWS Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No necesita conceder permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS misma. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de Lightsail for Research, adjunte también Lightsail for *ConsoleAccess* Research o la política gestionada a las entidades. *ReadOnly* AWS Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

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

```
    ]
}
```

Solución de problemas de identidad y acceso a Amazon Lightsail for Research

Utilice la siguiente información para ayudarle a diagnosticar y solucionar los problemas habituales que pueden surgir al trabajar con Lightsail for Research e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en Lightsail for Research
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Lightsail for Research

No estoy autorizado a realizar ninguna acción en Lightsail for Research

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `lightsail:`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `lightsail:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Lightsail for Research

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para

que asuma el rol. En el caso de los servicios que respaldan las políticas basadas en recursos o las listas de control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Lightsail for Research admite estas funciones, consulte. Cómo funciona Amazon Lightsail for Research con IAM
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de conformidad para Amazon Lightsail for Research

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte AWS la documentación de seguridad.

La resiliencia en Amazon Lightsail para la investigación

La infraestructura AWS global se basa Regiones de AWS en distintas zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, Lightsail for Research ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos. Para obtener más información, consulte Backup de ordenadores y discos virtuales con instantáneas de Lightsail for Research y Cree instantáneas de ordenadores o discos virtuales de Lightsail for Research.

Seguridad de infraestructura en Amazon Lightsail for Research

Como servicio gestionado, Amazon Lightsail for Research está protegido por la seguridad de AWS la red global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a Lightsail for Research a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Análisis de configuración y vulnerabilidad en Amazon Lightsail for Research

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Mejores prácticas de seguridad para Amazon Lightsail for Research

Lightsail for Research proporciona una serie de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Para evitar posibles problemas de seguridad asociados al uso de Lightsail for Research, siga estas prácticas recomendadas:

- Acceda a la consola de Lightsail for Research autenticándose en la primera. Consola de administración de AWS No comparta las credenciales de su consola personal. Cualquier usuario de Internet puede navegar hasta la consola, pero no puede iniciar sesión a menos que tenga credenciales válidas para acceder a la consola.

Historial de documentos de la Guía del usuario de Lightsail for Research

En la siguiente tabla se describen las versiones de documentación de Lightsail for Research.

Cambio	Descripción	Fecha
Versión inicial	Versión inicial de la Guía del usuario de Lightsail for Research.	28 de febrero de 2023

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.