aws

Guía del usuario

Amazon Lightsail para la investigación

Amazon Lightsail para la investigación: Guía del usuario

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 equipos virtuales vienen con aplicaciones de investigación preinstaladas, como RStudio y 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. Para estos procedimientos de configuración, utiliza el servicio AWS Identity and Access Management (IAM). Para obtener información completa sobre IAM, consulte la Guía del usuario de IAM.

Temas

Inscríbase en AWS

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

Para suscribirse a una Cuenta de AWS

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

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

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. 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.

Creación un usuario de IAM

Para crear un usuario administrador, elija una de las siguientes opciones.

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
En IAM Identity Center (recomendado)	Usar credenciales a corto plazo para acceder a AWS. Esto se ajusta a las prácticas recomendadas de seguridad. Para obtener información sobre las prácticas recomendadas, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.	Siga las instrucciones en Introducción en la Guía del usuario de AWS IAM Identity Center .	Configure el acceso programático configurando el AWS CLI que se utilizará AWS IAM Identity Center en la Guía del AWS Command Line Interface usuario.
En IAM (no recomendado)	Usar credenciales a largo plazo para acceder a AWS.	Siga las instrucciones en Creación del primer grupo de usuarios y usuario de administrador de IAM en la Guía del usuario de IAM.	Configurar el acceso programático mediante Administración de las claves de acceso de los usuarios de IAM en la Guía del usuario de IAM.

Tutorial: empezar a utilizar equipos virtuales de Lightsail para la investigación

Use este tutorial para empezar a utilizar equipos virtuales de Amazon Lightsail para la investigación. Obtendrá información sobre cómo crear y usar un equipo virtual, además de cómo conectarse. En Lightsail para la investigación, un equipo virtual es una estación de trabajo de investigación que se crea y administra en la nube de AWS. Los equipos virtuales se basan en instancias de Lightsail con el sistema operativo Ubuntu. En su equipo virtual, puede configurar previamente una aplicación de investigación como JupyterLab, RStudio o Scilab, entre otras.

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 acerca de los precios, consulte Precios de Lightsail.

Temas

Paso 1: completar los requisitos previos

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

Paso 2: crear un equipo virtual

Puede crear un equipo virtual mediante la consola de Lightsail para la investigación, tal como se describe en el procedimiento siguiente. 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 Aplicaciones y planes de hardware y Creación de un equipo virtual.

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

   Elija la región que se encuentre más cerca de su ubicación física para mejorar la latencia.
4. Elija una aplicación, también conocida como esquema 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 para la investigación ofrece planes estándar y planes de GPU para equipos 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 Equipos virtuales en el panel de navegación de la consola de Lightsail para la investigación.
2. Busque el nombre del equipo virtual que creó en el paso 1 y elija Lanzar aplicación. Por ejemplo, Lanzar 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 NICE DCV basado en navegador que está disponible en la consola de Lightsail para la investigación. Con NICE DCV, puede utilizar una interfaz gráfica de usuario (GUI) para interactuar con su aplicación de investigación y el sistema operativo de su equipo virtual.
- 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.

> **Note**
>
> También puede acceder a la interfaz de línea de comandos de su equipo virtual y transferir archivos mediante el cliente NICE DCV basado en navegador.

Debe proporcionar el par de claves de su equipo virtual para conectarse a este mediante SSH o para transferir archivos mediante SCP. Un par de claves es un conjunto de credenciales de seguridad que se usa para demostrar la identidad al conectarse a un equipo virtual de Lightsail para la investigación. 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:
  - Lanzamiento de la aplicación de un equipo virtual
  - Acceso al sistema operativo de un equipo virtual
- Establezca una conexión SSH o transfiera archivos mediante SCP:
  - Obtención de un par de claves para un equipo virtual
  - Conexión a un equipo virtual mediante Secure Shell
  - Transferencia de archivos a un equipo virtual 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 para la investigación ofrece volúmenes de almacenamiento de nivel de bloque (discos) que se pueden adjuntar a un equipo 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.

Cuando adjunta un disco al equipo virtual mediante la consola, Lightsail para la investigación formatea y monta el disco automáticamente 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:

- Crear un disco
- Visualización de discos
- Adjuntar un disco a un equipo virtual
- Desasociar un disco de un equipo virtual
- Eliminar un disco

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 copia en un momento dado de los 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:

- Crear una instantánea
- Visualización de instantáneas
- Creación de un equipo virtual o un disco a partir de una instantánea
- Eliminar una instantánea

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 Visualización de los detalles de un equipo virtual. Para obtener más información acerca de los precios, consulte Precios de Lightsail.

> **Important**
>
> Eliminar un recurso de Lightsail para la investigación 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 para la investigación.
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.

Tutoriales de introducción a Amazon 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**
>
> En el blog del sector público se ha publicado un tutorial detallado para empezar a utilizar Lightsail for Research y RStudio. AWS Para obtener más información, consulte Introducción a Amazon Lightsail for Research: tutorial sobre el uso de RStudio.

Comience con JupyterLab

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 Creación de un equipo virtual.

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 Crear un disco y Adjuntar un disco a un equipo virtual.

> **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 Obtención de un par de claves para un equipo virtual.

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 Transferencia de archivos a un equipo virtual 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 Conexión a un equipo virtual mediante Secure Shell.

> **Note**
>
> También puede acceder a la interfaz de línea de comandos de su equipo virtual y transferir archivos mediante el cliente NICE DCV basado en navegador. El NICE DCV está disponible en la consola Lightsail for Research. Para obtener más información, consulte Lanzamiento de la aplicación de un equipo virtual y Acceso al sistema operativo de un equipo virtual.

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

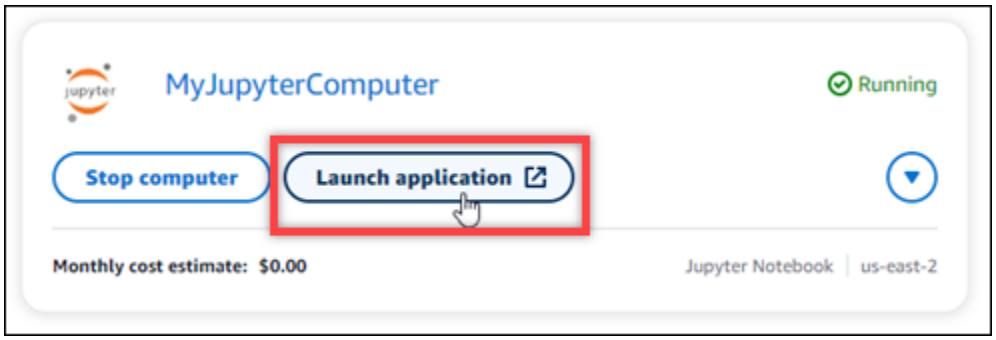
Complete el siguiente procedimiento para iniciar la JupyterLab aplicación en su nueva computadora virtual.

> **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.

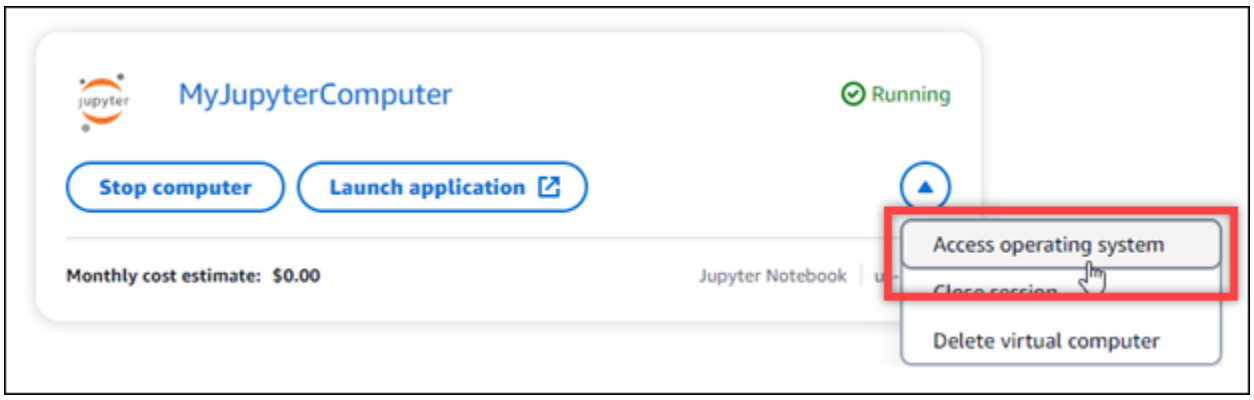
1. Inicie sesión en la consola de Lightsail for Research.

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



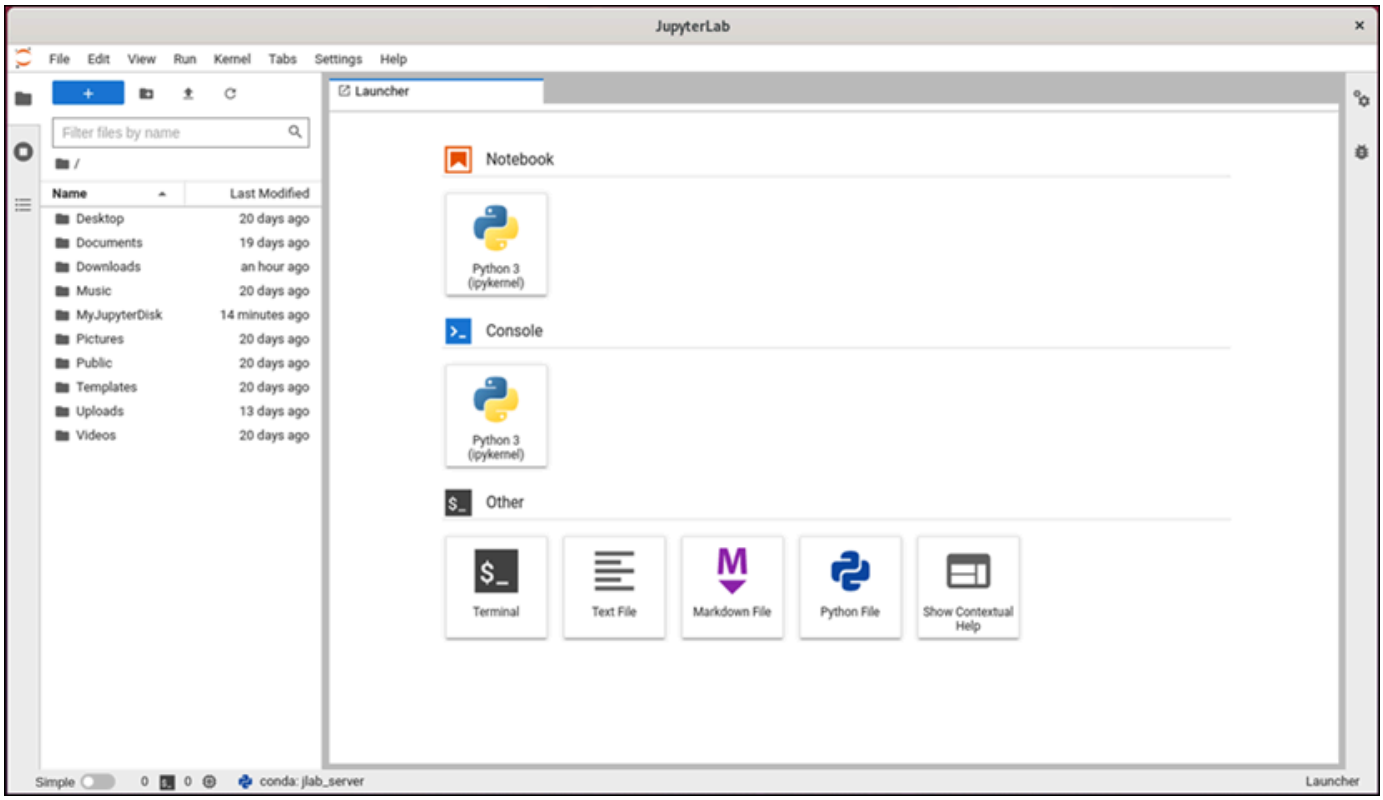
   b. Seleccione el menú desplegable del equipo y, a continuación, seleccione Acceso al sistema operativo para acceder al escritorio del equipo virtual.



   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.

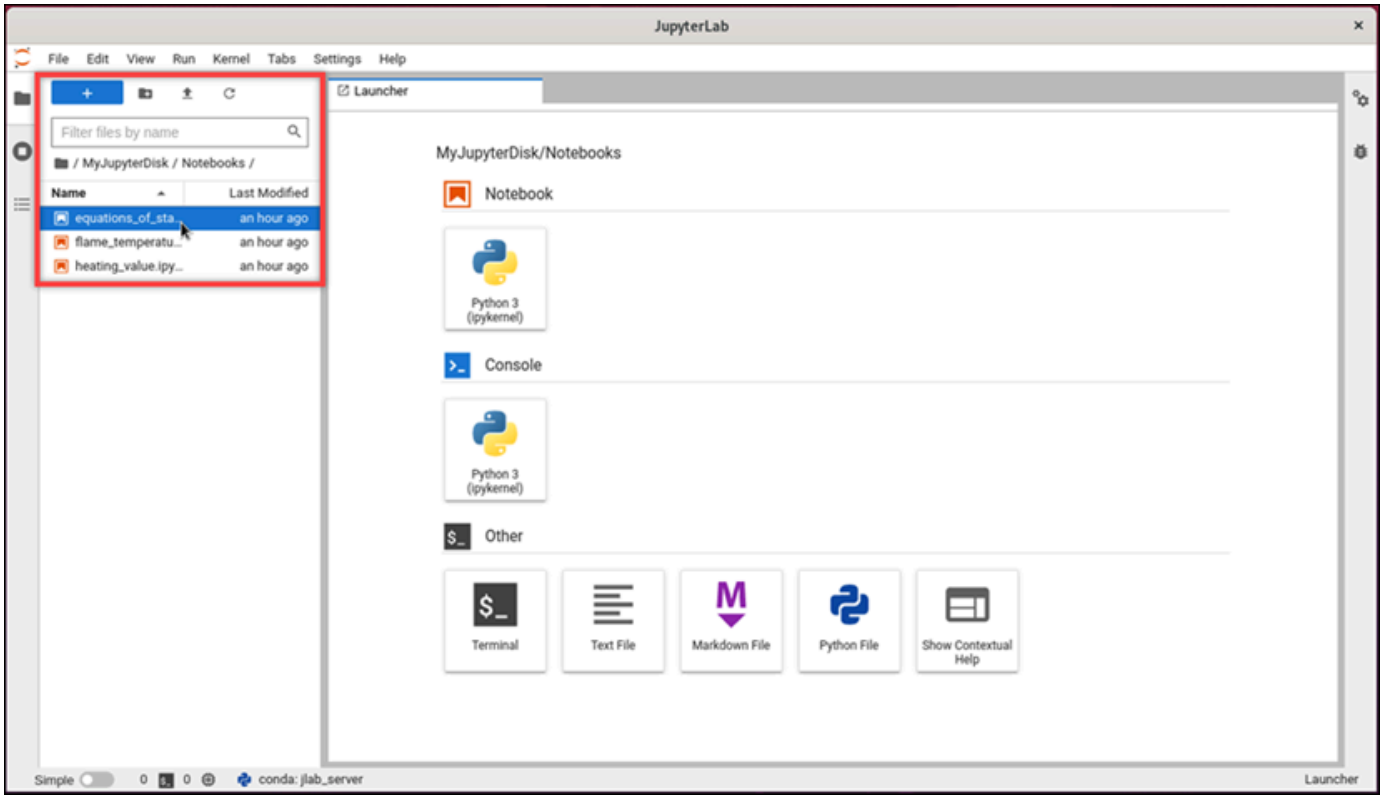
> **Note**
>
> Es posible que su navegador le pida que autorice el uso compartido del portapapeles. Si lo permite, podrá copiar y pegar entre el equipo local y el equipo virtual.
> Es posible que Ubuntu también le pida una configuración inicial. Siga las instrucciones hasta que complete la configuración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

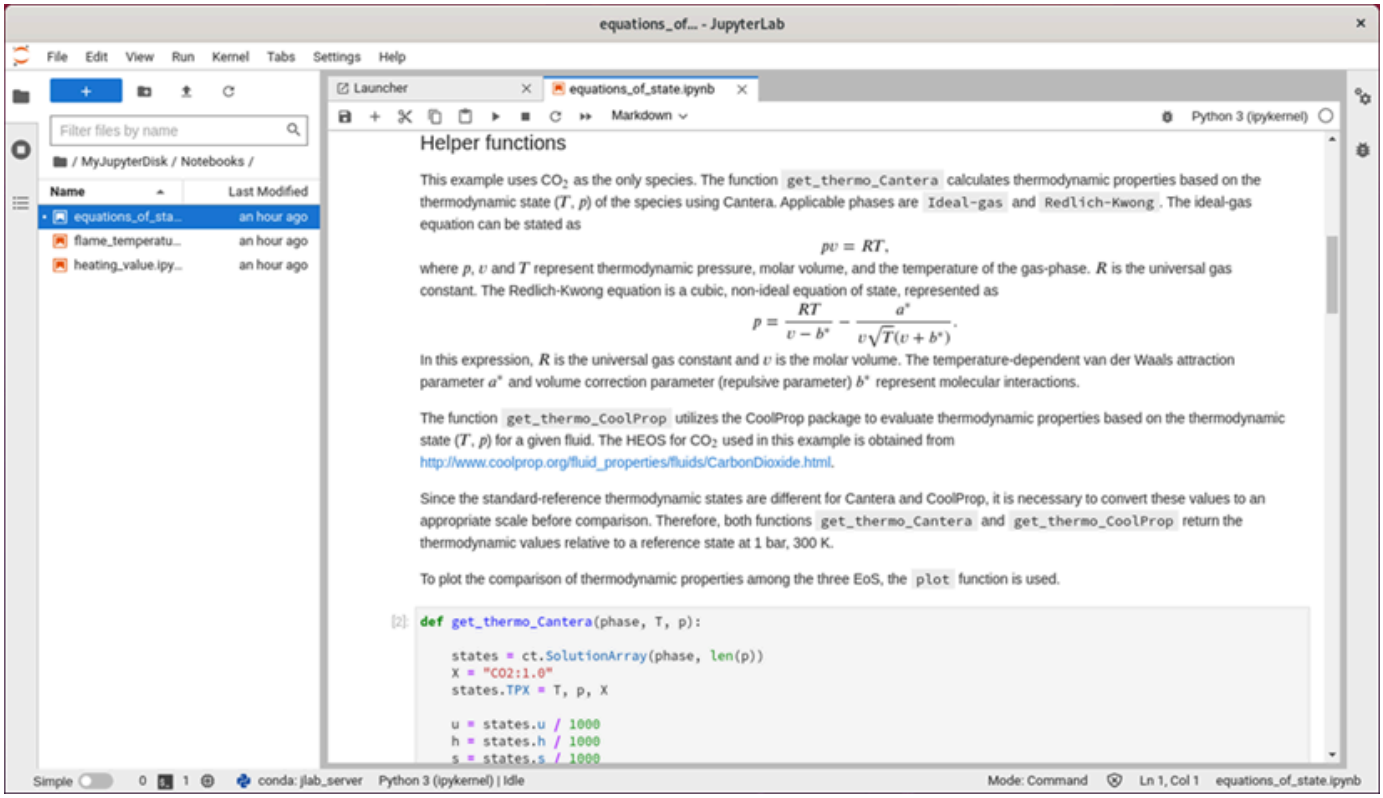


5. Para abrir un archivo JupyterLab, en el panel del explorador de archivos, elija el directorio o la carpeta donde se almacenan los archivos del proyecto. A continuación, elija el archivo para abrirlo.

   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

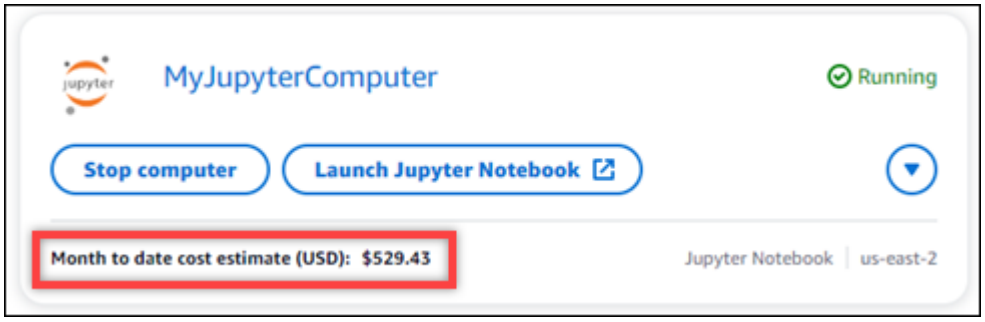
Si no está familiarizado con ellos JupyterLab, le recomendamos que lea su documentación oficial. Están disponibles los siguientes recursos JupyterLab en línea:

- JupyterLabDocumentación
- Jupyter Discourse Forum
- JupyterLab en StackOverflow
- JupyterLab en GitHub

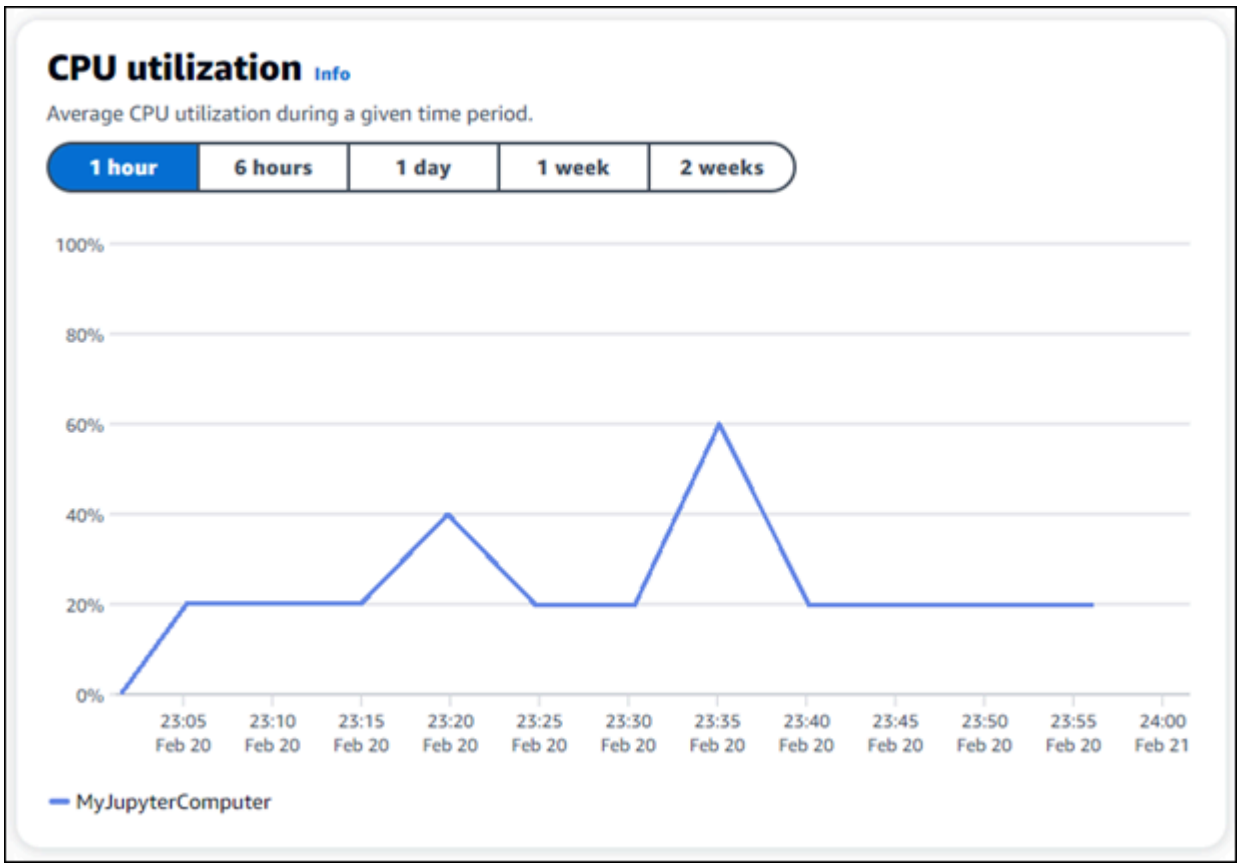
Paso 6: (opcional) supervisar el uso y los costos

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.

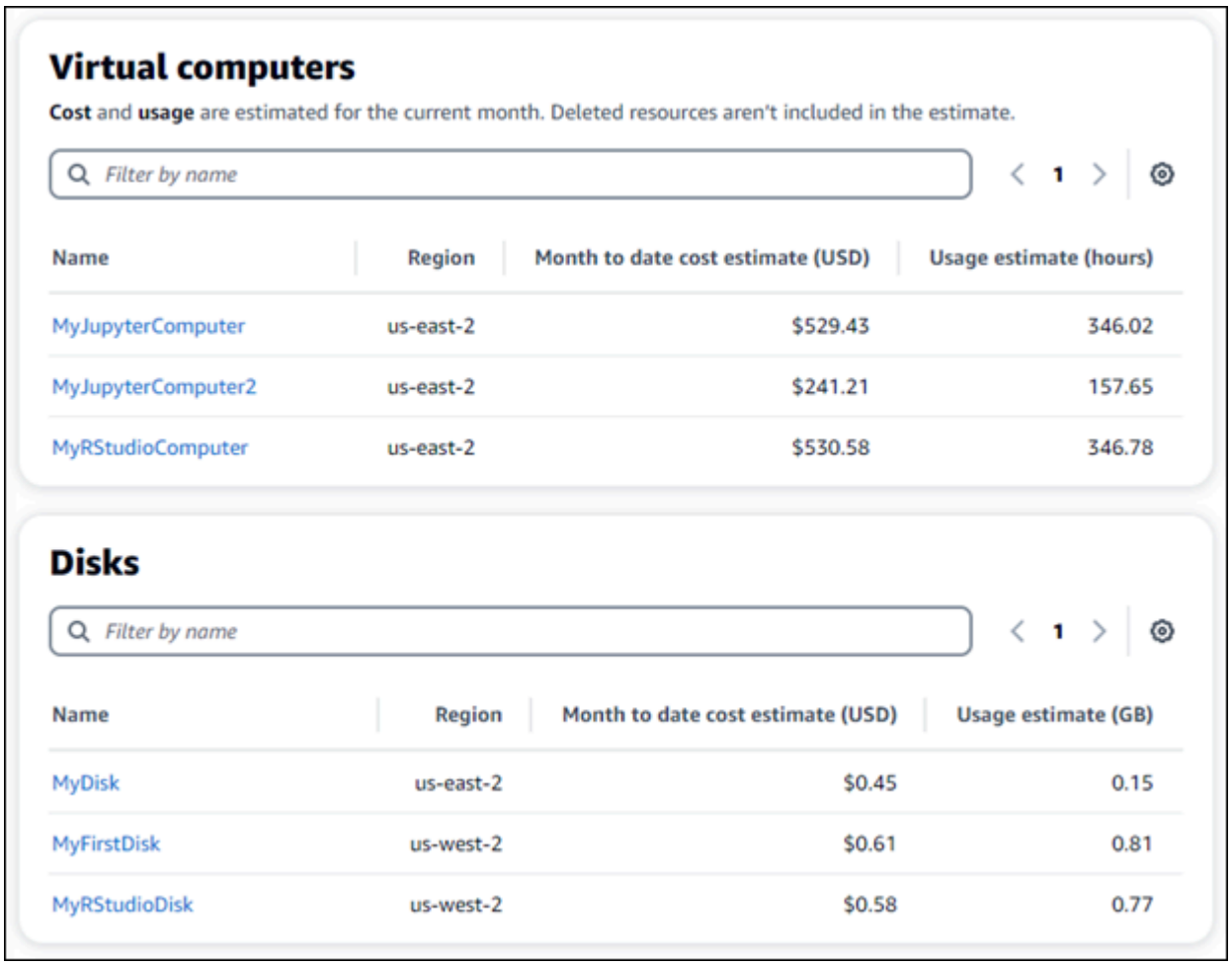
1. Seleccione Ordenadores virtuales en el panel de navegación de la consola de Lightsail for Research. La estimación del costo mensual de sus equipos virtuales hasta la fecha aparece debajo de cada equipo virtual en ejecución.



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:

- Control de costes
- Creación de una regla
- Eliminación de una regla

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:

- Crear una instantánea
- Visualización de instantáneas
- Creación de un equipo virtual o un disco a partir de una instantánea
- Eliminar una instantánea

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 Visualización de los detalles de un equipo virtual. 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.

Introducción a RStudio

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

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

Temas

Paso 1: completar los requisitos previos

Si aún no lo ha hecho, cree un equipo virtual con la aplicación de RStudio. Para obtener más información, consulte Creación de un equipo virtual.

Una vez que su nuevo equipo virtual esté en funcionamiento, continúe con el paso 4 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 Crear un disco y Adjuntar un disco a un equipo virtual.

> **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 equipo virtual de RStudio y descargarlos desde dicho equipo. Para ello, debe completar los siguientes pasos:

1. Obtenga un key pair de Amazon Lightsail. Para obtener más información, consulte Obtención de un par de claves para un equipo virtual.
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 Transferencia de archivos a un equipo virtual 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 Conexión a un equipo virtual mediante Secure Shell.

> **Note**
>
> También puede acceder a la interfaz de línea de comandos de su equipo virtual y transferir archivos mediante el cliente NICE DCV basado en navegador. El NICE DCV está disponible en la consola Lightsail for Research. Para obtener más información, consulte Lanzamiento de la aplicación de un equipo virtual y Acceso al sistema operativo de un equipo virtual.

Paso 4: lanzar la aplicación de RStudio

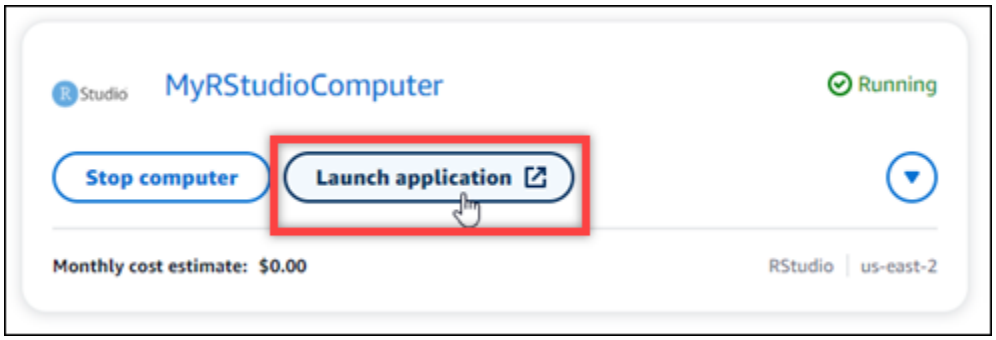
Complete el procedimiento siguiente para lanzar la aplicación de RStudio en el nuevo equipo virtual.

> **Important**
>
> No actualice el sistema operativo ni la aplicación de RStudio aunque se le pida que lo haga. En su lugar, elija la opción de cerrar o ignorar esas indicaciones. Además, no modifique

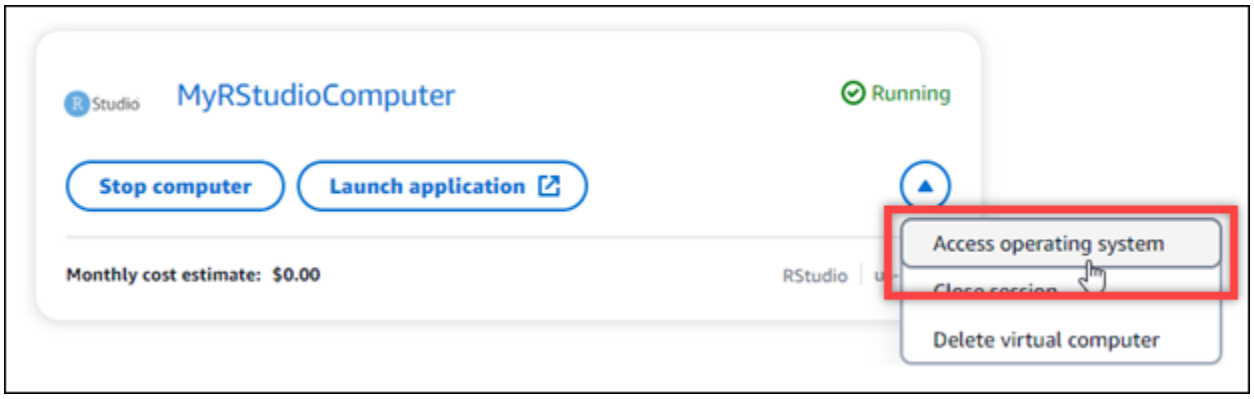
ninguno de los archivos que se encuentran en el directorio /home/lightsail-admin/. Estas acciones pueden inutilizar el equipo virtual.

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) Seleccione Lanzar aplicación para lanzar la aplicación de RStudio 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.

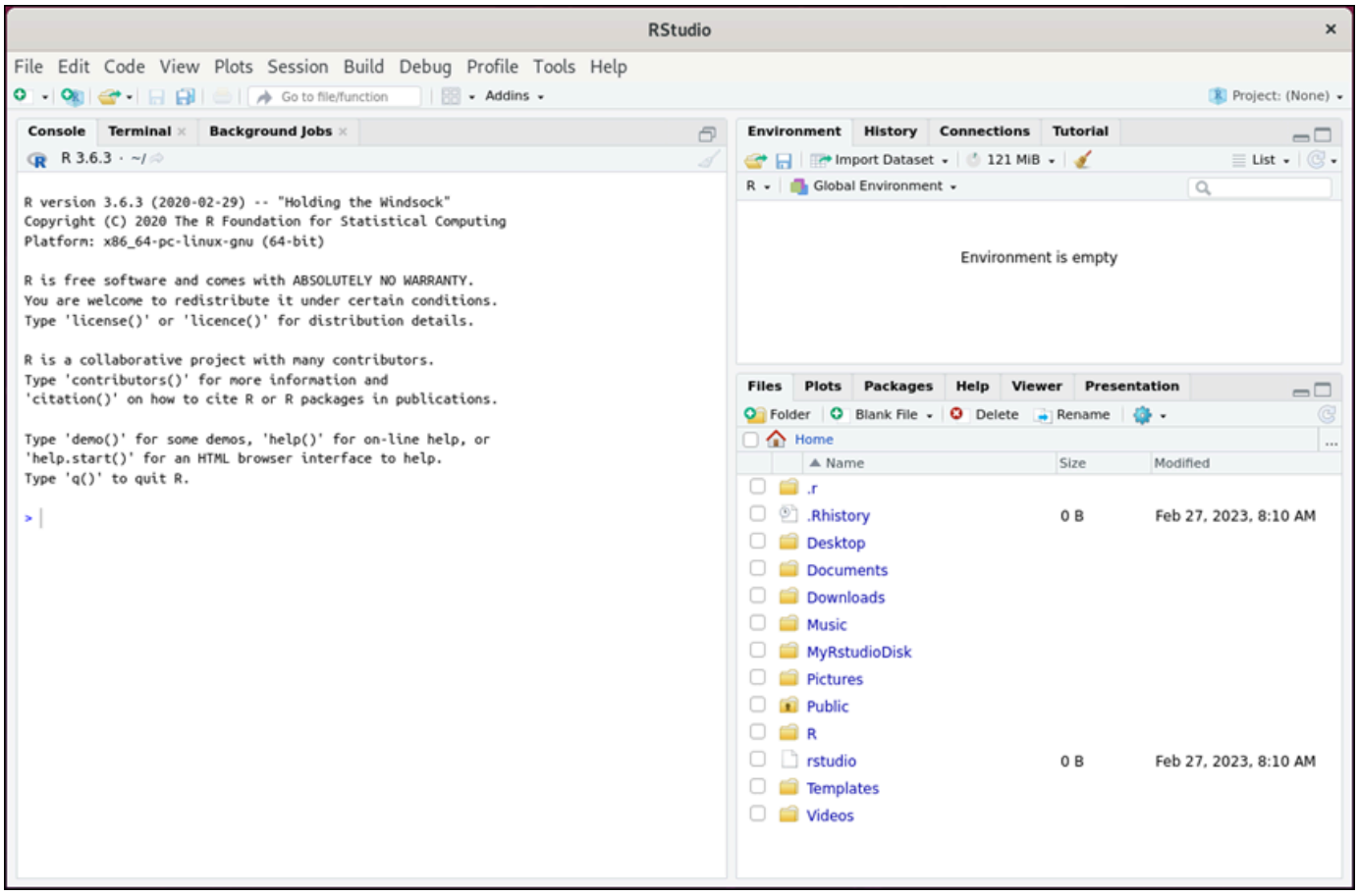


Lightsail for Research ejecuta algunos comandos para iniciar la conexión del protocolo de pantalla remota. Tras unos instantes, se abre una nueva ventana de pestañas del navegador con una conexión de escritorio virtual establecida con su equipo virtual. Si ha elegido la opción

Lanzar aplicación, continúe con el siguiente paso de este procedimiento para abrir un archivo en la aplicación de RStudio. 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.

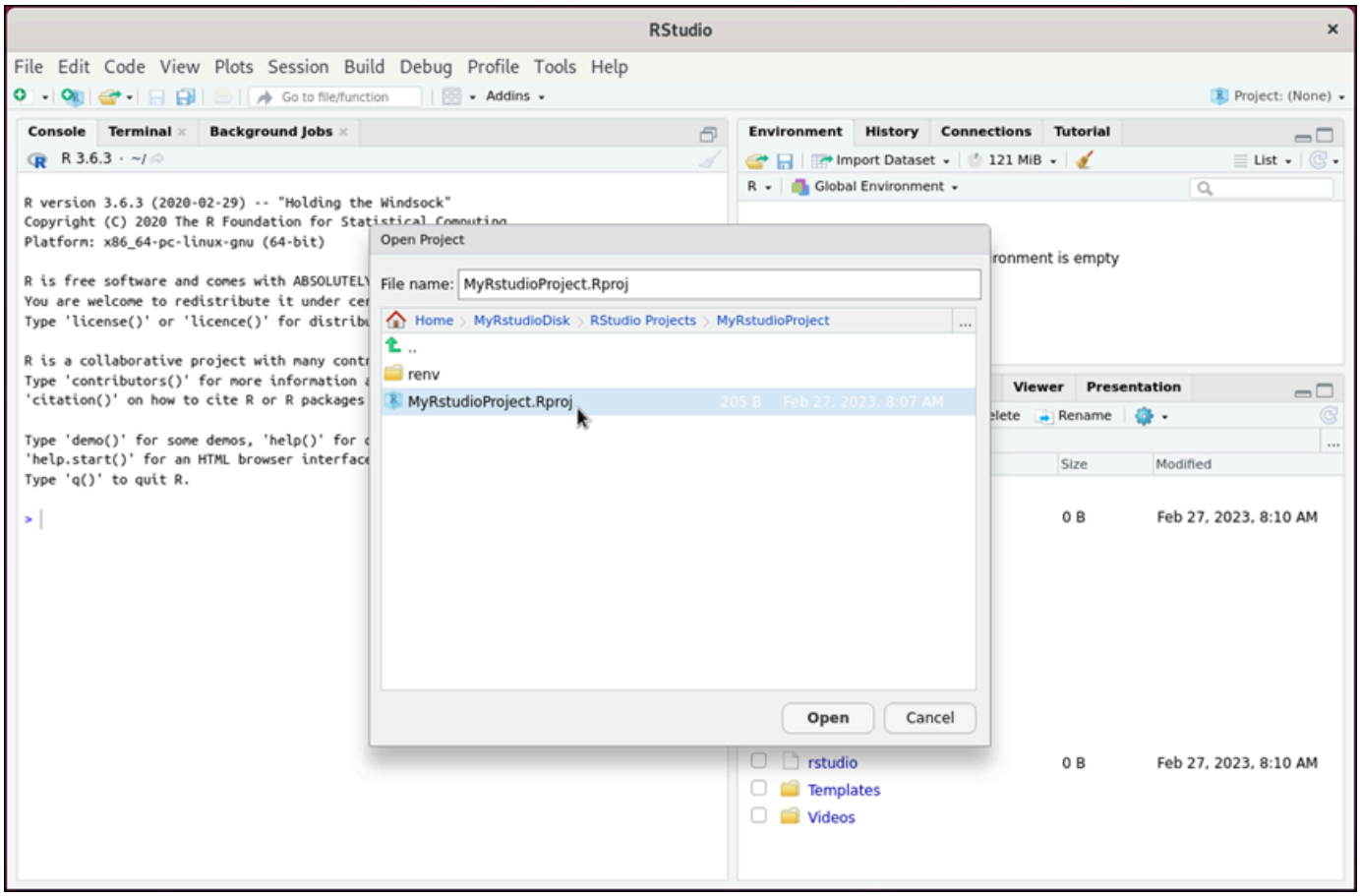
4. Se abre la aplicación de RStudio.



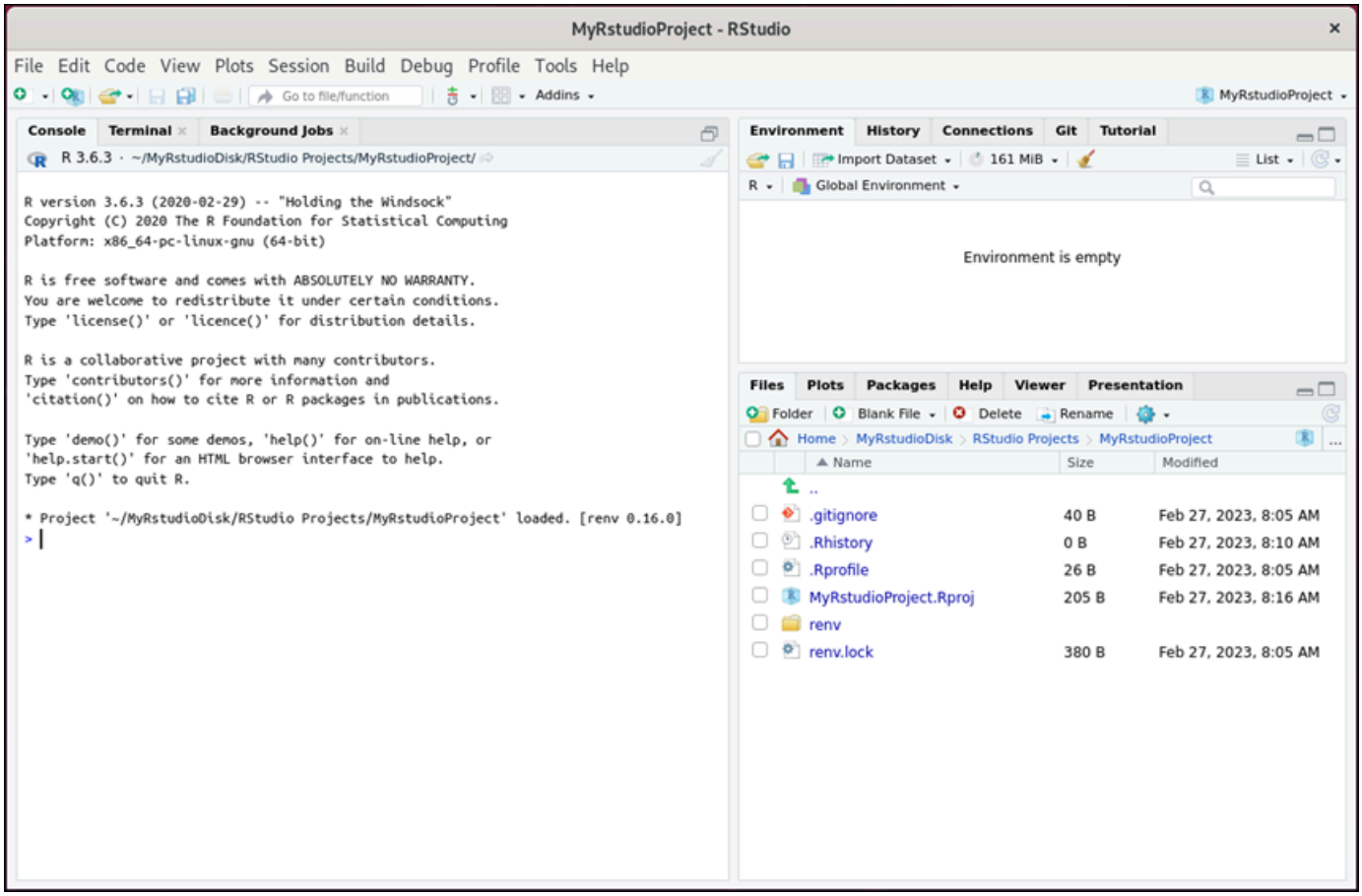
5. Para abrir un proyecto en RStudio, seleccione el menú File y, a continuación, elija Open project. Navegue hasta el directorio o la carpeta donde están almacenados los archivos del proyecto. A continuación, elija el archivo para abrirlo.

   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 directorio `MyRstudioDisk` representa el disco montado y el subdirectorio `Projects` contiene los archivos de nuestro proyecto de RStudio.



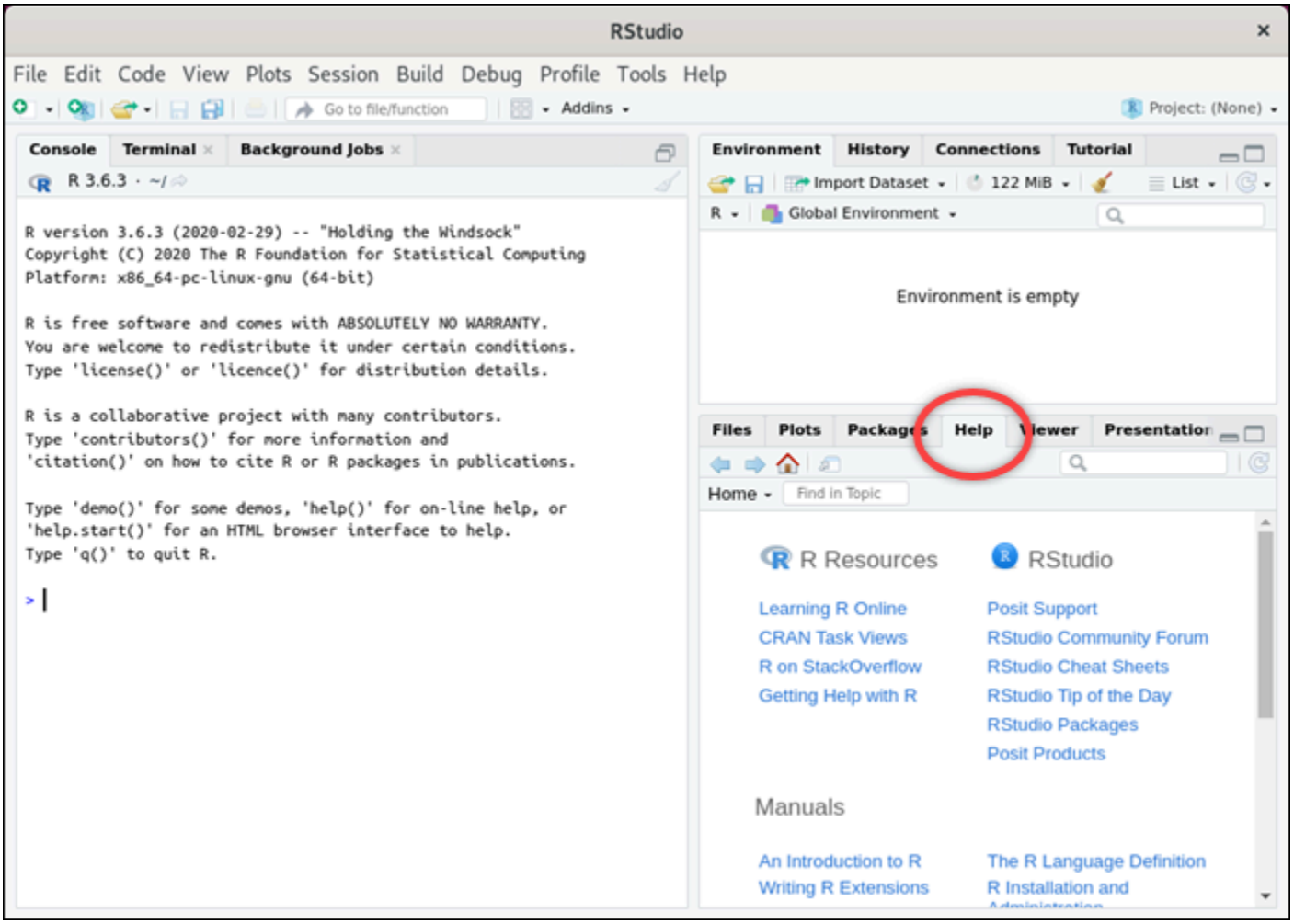
En el siguiente ejemplo, hemos abierto el archivo del proyecto `MyRstudioProject.Rproj`.



Para obtener información sobre cómo comenzar a utilizar RStudio, continúe con la sección Paso 5: leer la documentación de RStudio de este tutorial.

Paso 5: leer la documentación de RStudio

La aplicación de RStudio incluye un paquete de documentación completo. Para empezar a obtener información sobre RStudio, le recomendamos que acceda a la pestaña Help de RStudio, tal y como se muestra en el siguiente ejemplo.



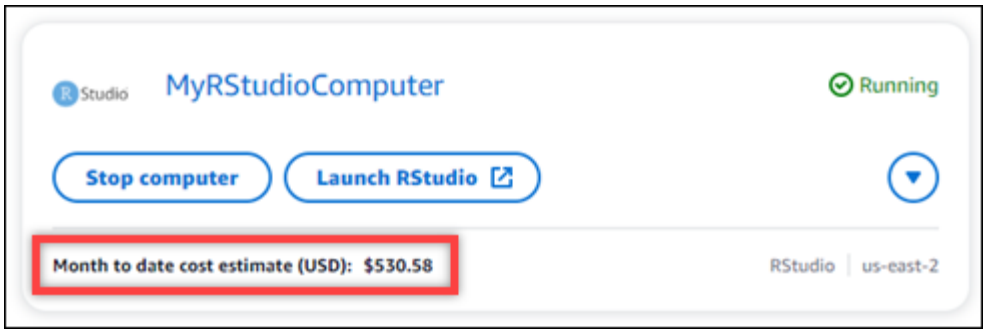
También están disponibles los siguientes recursos en línea de RStudio:

- Aprendizaje de R en línea
- R encendido StackOverflow
- Getting Help with R
- Posit Support
- RStudio Community Forum
- RStudio Cheat Sheets
- RStudio Tip of the Day (Twitter)
- RStudio Packages

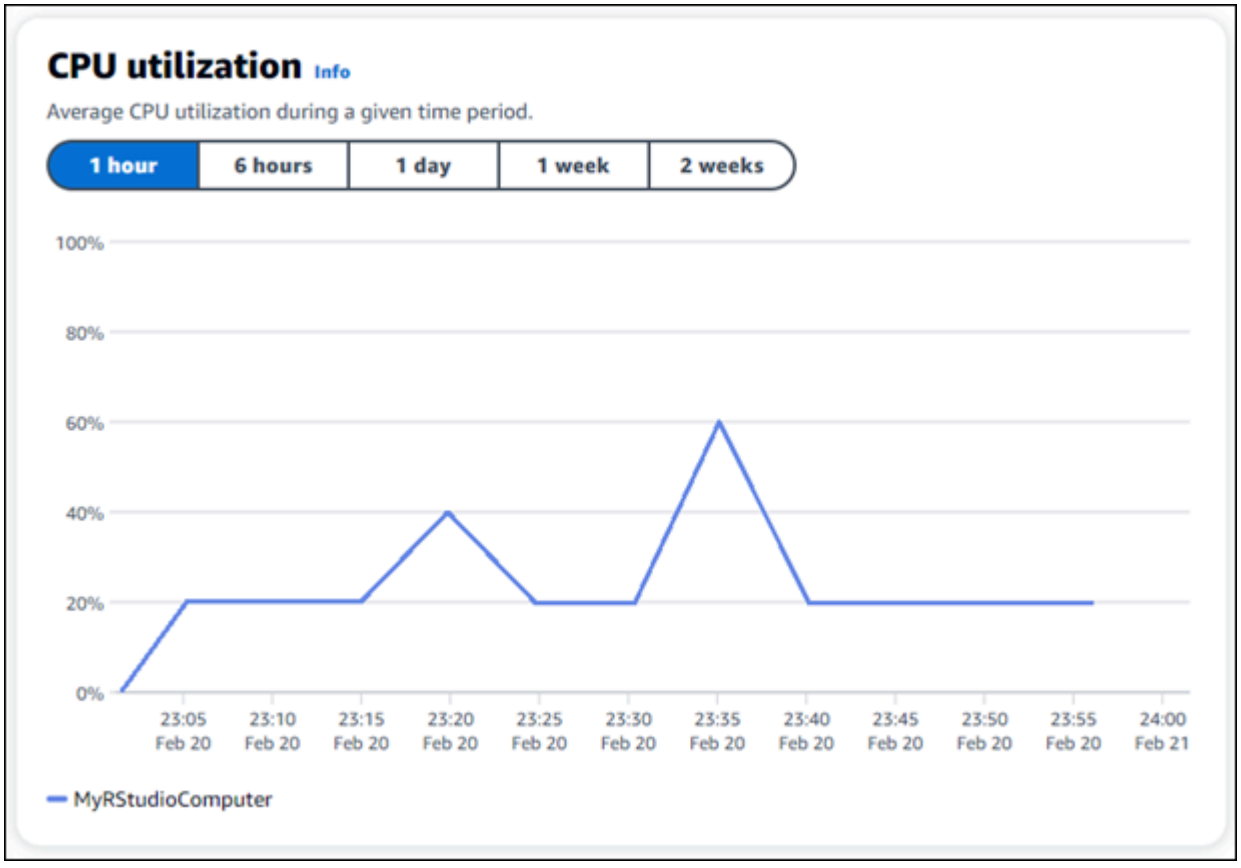
Paso 6: (opcional) supervisar el uso y los costos

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.

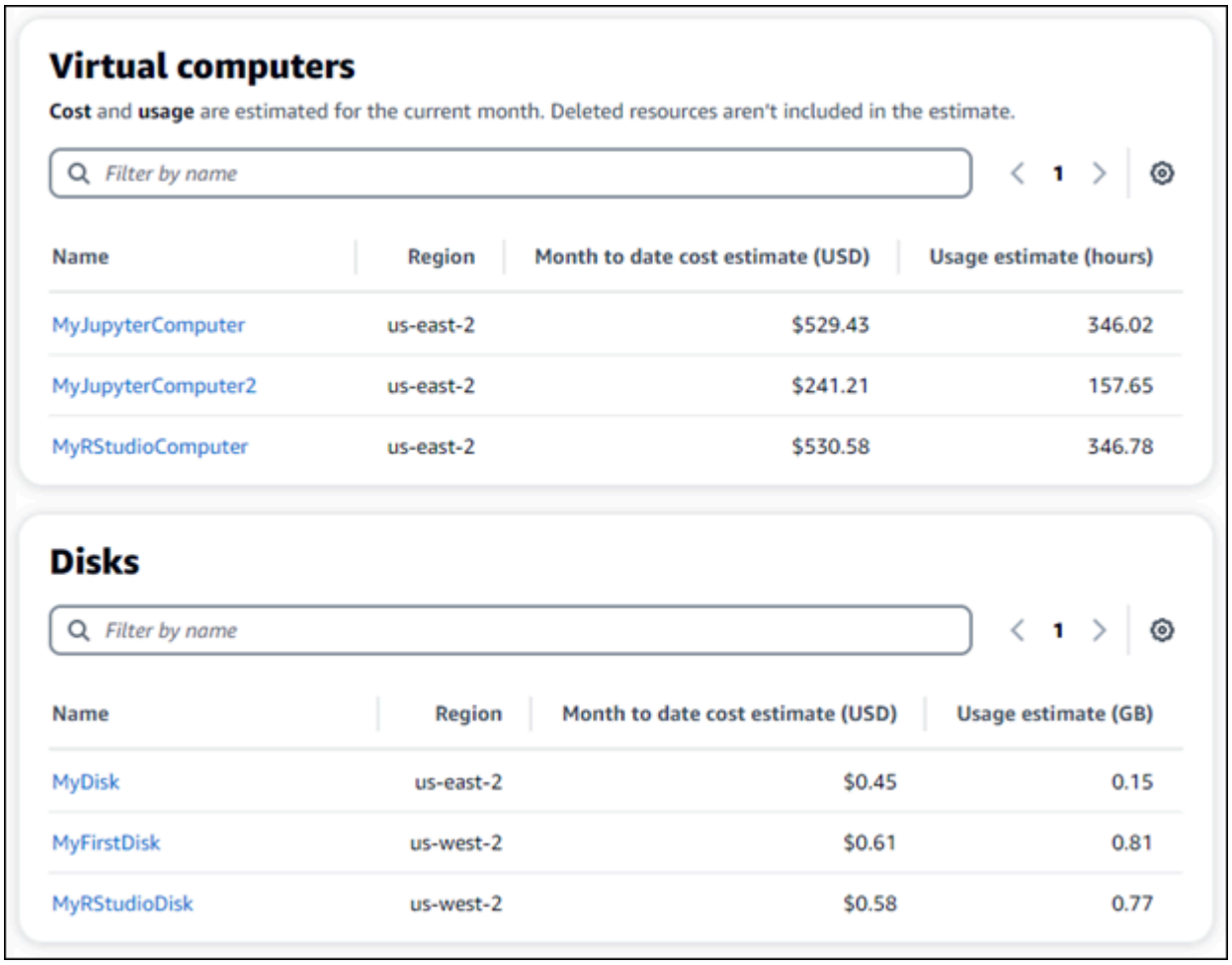
1. Seleccione Ordenadores virtuales en el panel de navegación de la consola de Lightsail for Research. La estimación del costo mensual de sus equipos virtuales hasta la fecha aparece debajo de cada equipo virtual en ejecución.



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:

- Control de costes
- Creación de una regla
- Eliminación de una regla

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:

- Crear una instantánea
- Visualización de instantáneas
- Creación de un equipo virtual o un disco a partir de una instantánea
- Eliminar una instantánea

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 Visualización de los detalles de un equipo virtual. 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.

Equipos virtuales

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 de Lightsail for Research tendrán IMDSv2 activado de forma predeterminada.

Temas

Aplicaciones y planes de hardware

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 del equipo virtual, como la cantidad de vCPU, la

memoria, 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 Instantáneas.

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 RStudio IDE.
- VSCodium: VSCodium es una distribución binaria que promueve la comunidad del editor VS Code de Microsoft. 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 (vCPU), 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	vCPU	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	vCPU	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

Creación de un equipo virtual

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 Aplicaciones y planes de hardware.
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. Lanzamiento de la aplicación de un equipo virtual

> **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 Administración de los puertos de firewall de equipos virtuales.

Visualización de los detalles de un equipo virtual

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
  - Running
  - Deteniendo
  - Stopped (Detenido)

  - 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.

Lanzamiento de la aplicación de un equipo virtual

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.

Acceso al sistema operativo de un equipo virtual

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.

Administración de los puertos de firewall de equipos virtuales

Un firewall en Amazon Lightsail for Research controla el tráfico permitido para conectarse a su ordenador virtual. Agregue reglas al firewall del equipo virtual que especifiquen el protocolo, los puertos y las direcciones IPv4 o IPv6 de origen que pueden conectarse a él. 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 direcciones IPv4 y otro para direcciones IPv6. 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

Cumplir con los requisitos previos

Complete los siguientes requisitos previos antes de comenzar.

- Cree un ordenador virtual en Lightsail for Research. Para obtener más información, consulte Creación de un equipo virtual.
- 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 los comandos de 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.

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

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 los comandos de 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 los comandos de 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.

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

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 Obtención de un par de claves para un equipo virtual.
- Conéctese a su equipo virtual mediante SSH para administrarlo mediante la línea de comandos. Para obtener más información, consulte Transferencia de archivos a un equipo virtual mediante Secure Copy.

- Conéctese a su equipo virtual mediante SCP para transferir archivos de forma segura. Para obtener más información, consulte Transferencia de archivos a un equipo virtual mediante Secure Copy.

Obtención de un par de claves para un equipo virtual

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 con su equipo virtual mediante el cliente NICE DCV basado en navegador. El NICE 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 Lanzamiento de la aplicación de un equipo virtual y Acceso al sistema operativo de un equipo virtual.

Temas

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

Cumplir con los requisitos previos

Complete los siguientes requisitos previos antes de comenzar.

- Cree un ordenador virtual en Lightsail for Research. Para obtener más información, consulte Creación de un equipo virtual.
- 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 los comandos de 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

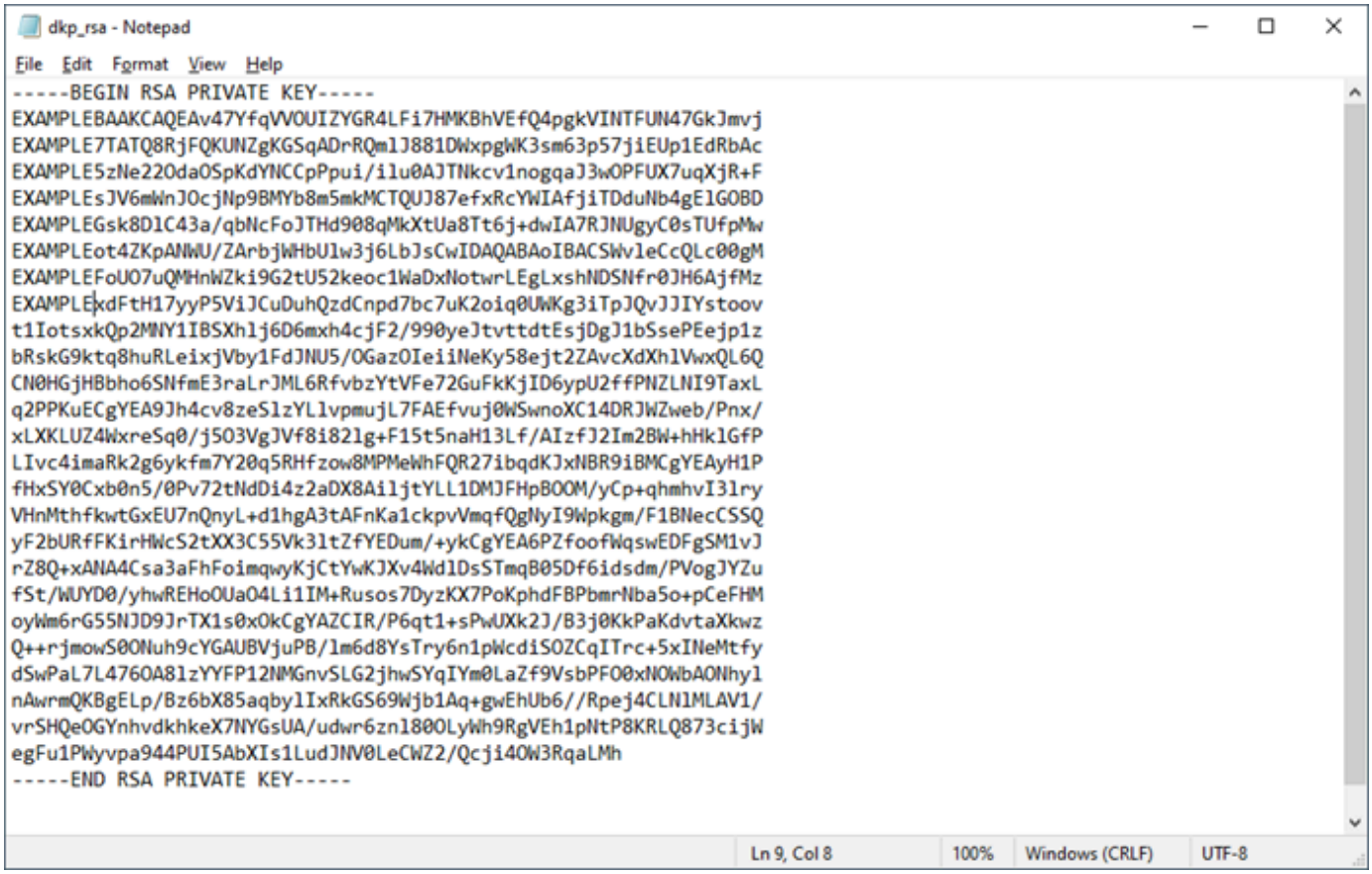
```
aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
```

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 los comandos de 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,

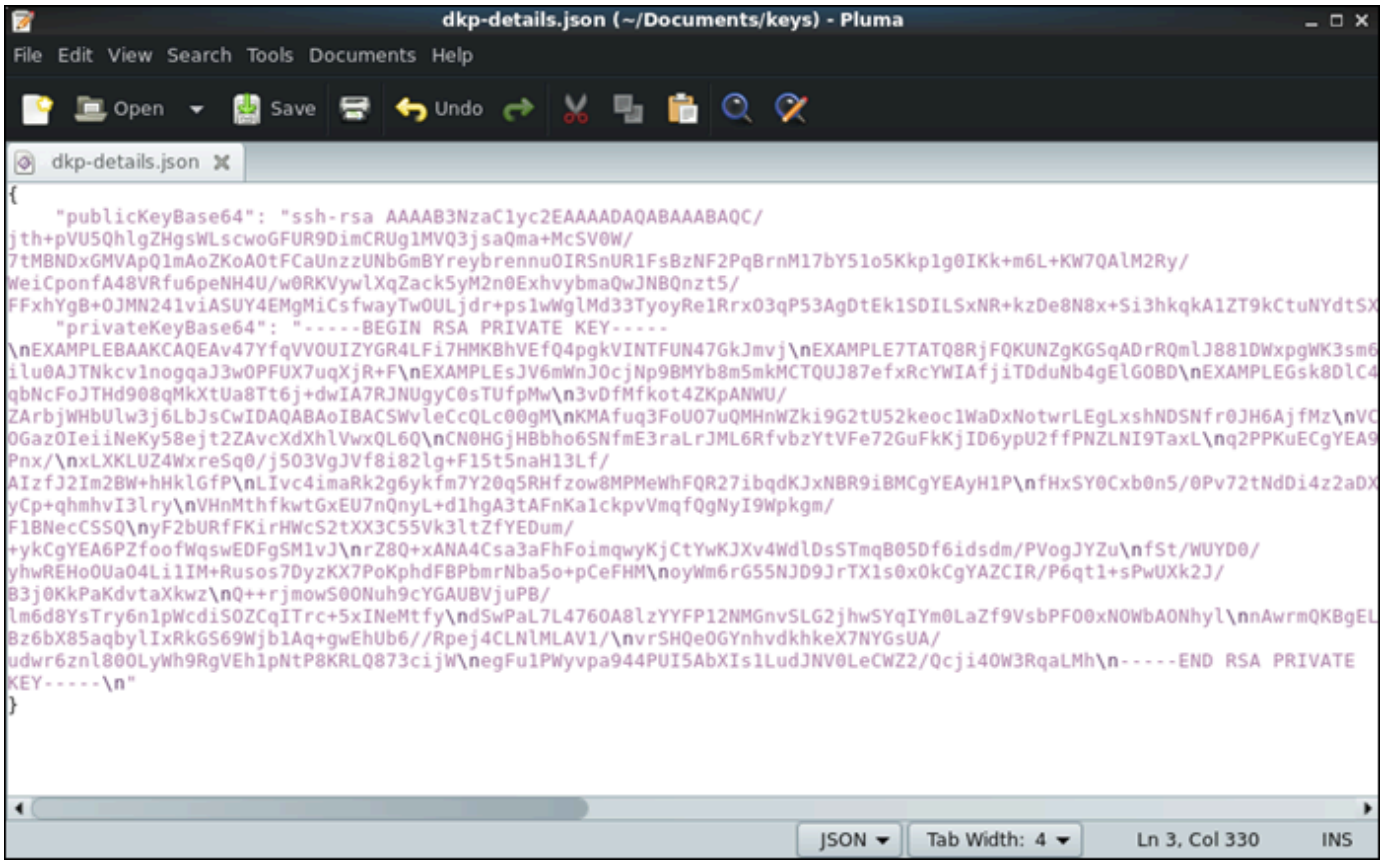
region-code sustitúyalo por el código de la AWS región en la que se creó la computadora virtual, por ejemplo. `us-east-2`

```
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
```

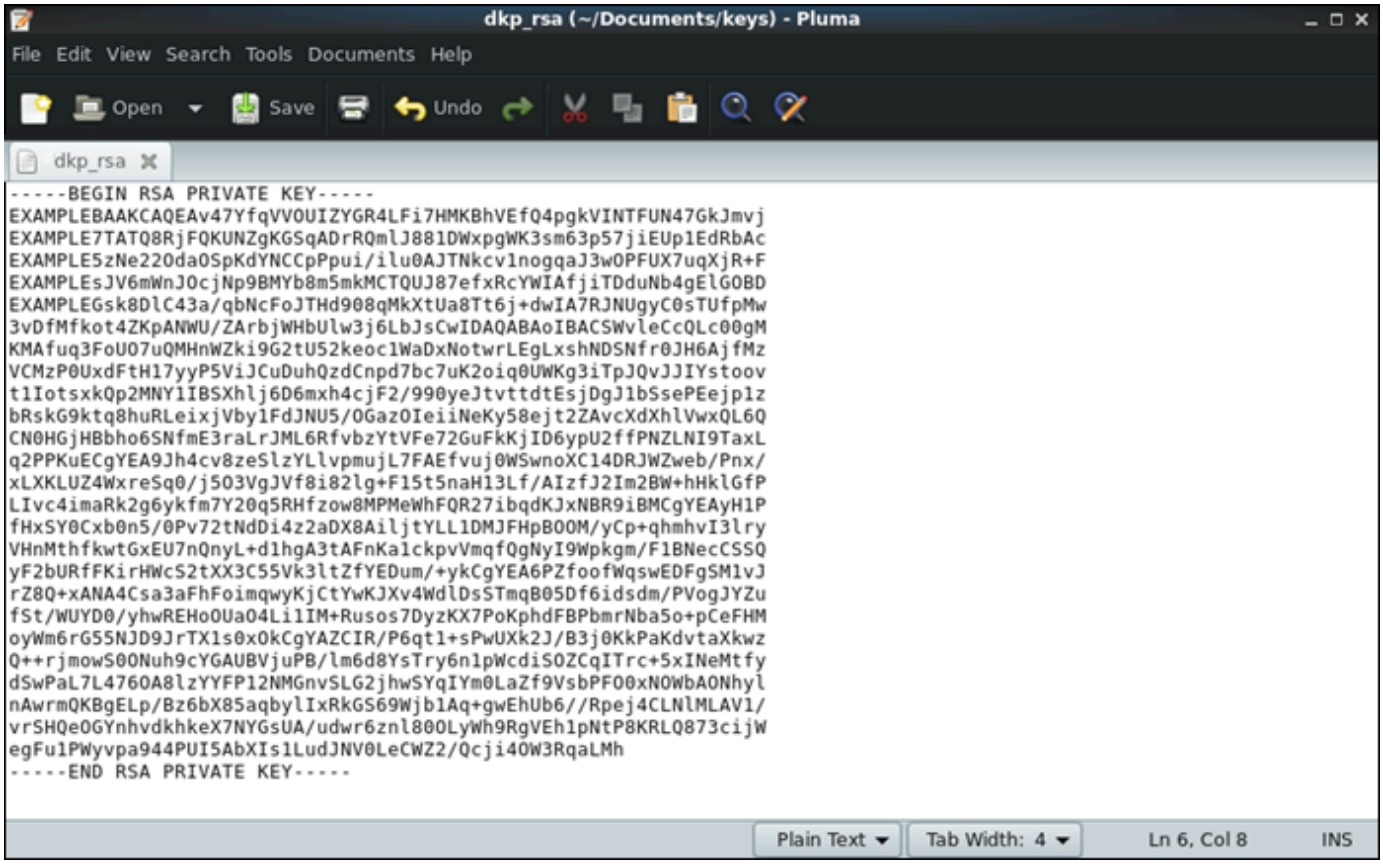
No hay respuesta al comando. Puede confirmar si el comando se ha realizado correctamente abriendo el `dkp-details.json` archivo y comprobando si se ha guardado la información del DKP de Lightsail. El contenido del archivo `dkp-details.json` debe ser similar al siguiente ejemplo. El comando ha fallado 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 Conexión a un equipo virtual mediante Secure Shell.

- Conéctese a su equipo virtual mediante SCP para transferir archivos de forma segura. Para obtener más información, consulte Transferencia de archivos a un equipo virtual mediante Secure Copy.

Conexión a un equipo virtual 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 con su equipo virtual mediante el cliente NICE DCV basado en navegador. El NICE DCV está disponible en la consola Lightsail for Research. Para obtener más información, consulte Acceso al sistema operativo de un equipo virtual.

Temas

Cumplir con los requisitos previos

Complete los siguientes requisitos previos antes de comenzar.

- Cree un ordenador virtual en Lightsail for Research. Para obtener más información, consulte Creación de un equipo virtual.
- 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 Visualización de los detalles de un equipo virtual.
- 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 Administración de los puertos de firewall de equipos virtuales.

- 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

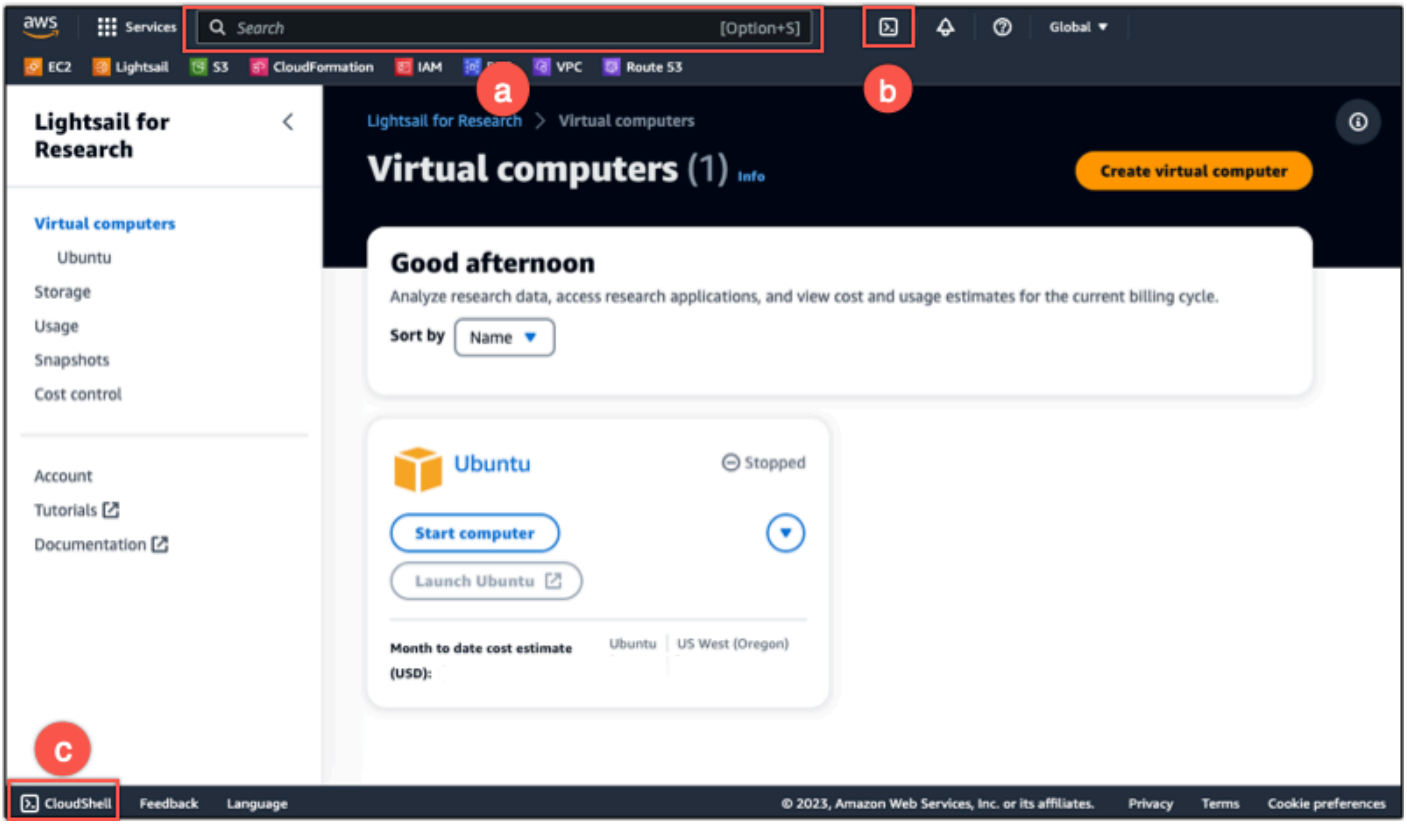
Realice uno de los siguientes procedimientos para establecer una conexión SSH con su ordenador virtual en Lightsail for Research.

Conéctese a un ordenador virtual mediante AWS CloudShell

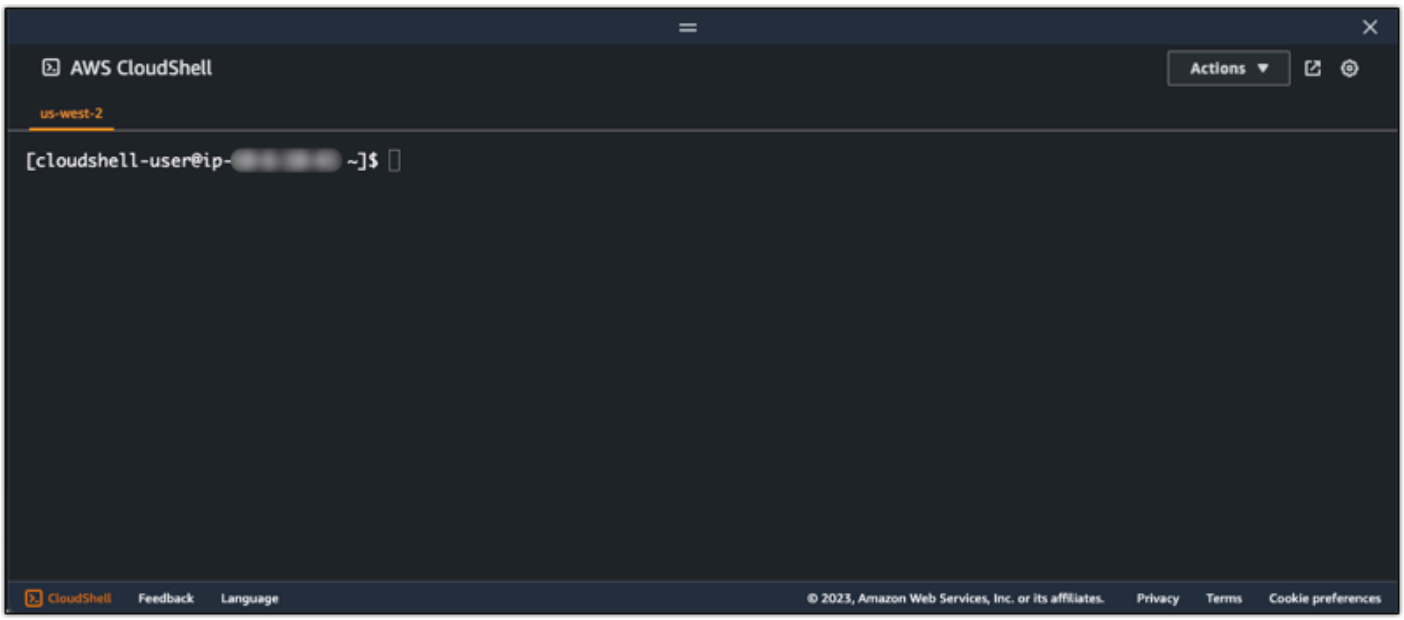
Este procedimiento se aplica si prefiere una configuración mínima para conectarse al equipo virtual. AWS CloudShell utiliza un shell preautenticado y basado en un navegador que puede iniciar directamente desde. AWS Management Console Puede ejecutar AWS CLI comandos con el shell que prefiera, como el 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 Obtención de un par de claves para un equipo virtual.

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, selecciona el CloudShellicono.
   c. Elija 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 a`PS>`.

   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, consulte[Conexión 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 Obtención de un par de claves para un equipo virtual. Este procedimiento envía la clave privada del Lightsail DKP a `dkp_rsa` un archivo que se utiliza en uno de los siguientes comandos.

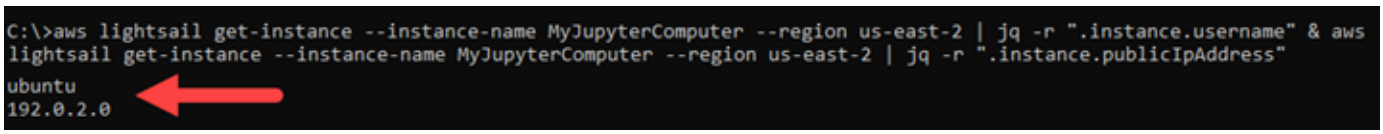
1. Abra una ventana del símbolo del sistema.
2. Ingrese el siguiente comando para mostrar la dirección IP pública y el nombre de usuario de su equipo virtual. En el comando, *`region-code`* sustitúyala por el código Región de AWS en el que se creó la computadora virtual, por ejemplo. `us-east-2` Sustituya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

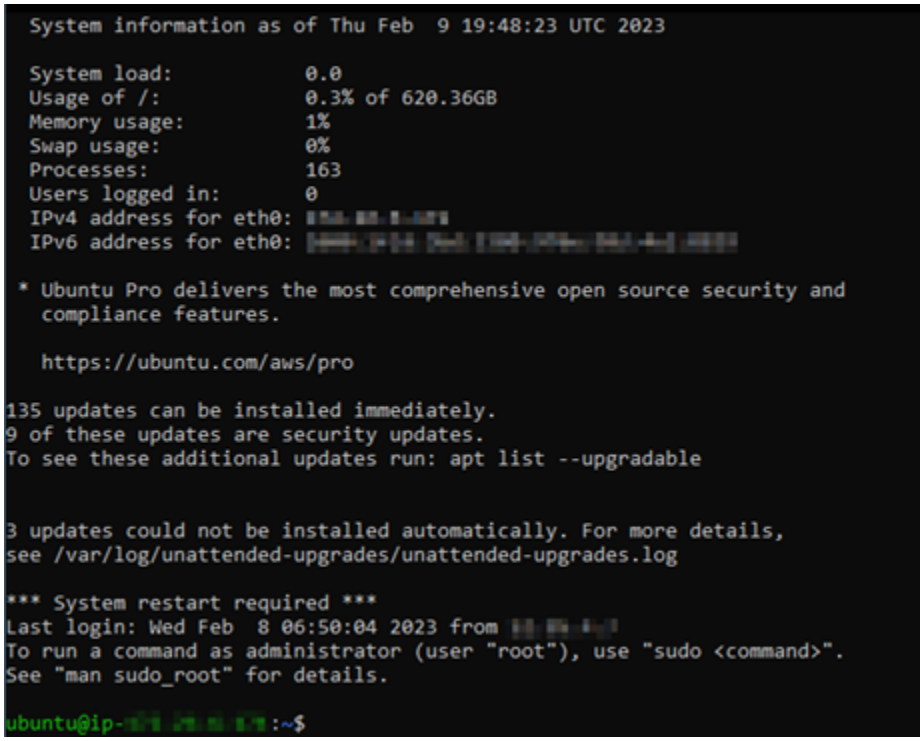
3. Ingrese el siguiente comando para establecer una conexión SSH con su equipo virtual. En el comando, sustituya *user-name* por el nombre de usuario de inicio de sesión y sustituya *public-ip-address* por la dirección IP pública de su equipo virtual.

```
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 Obtención de un par de claves para un equipo virtual. Este procedimiento envía la clave privada del Lightsail DKP a `dkp_rsa` un archivo que se utiliza en uno de los siguientes comandos.

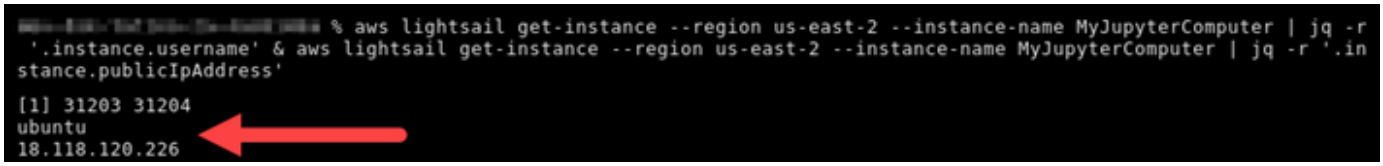
1. Abra una ventana de terminal.
2. Ingrese el siguiente comando para mostrar la dirección IP pública y el nombre de usuario de su equipo virtual. En el comando, *`region-code`* sustitúyalo por el código de la AWS región en la que se creó la computadora virtual, por ejemplo. `us-east-2` Sustituya *`computer-name`*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

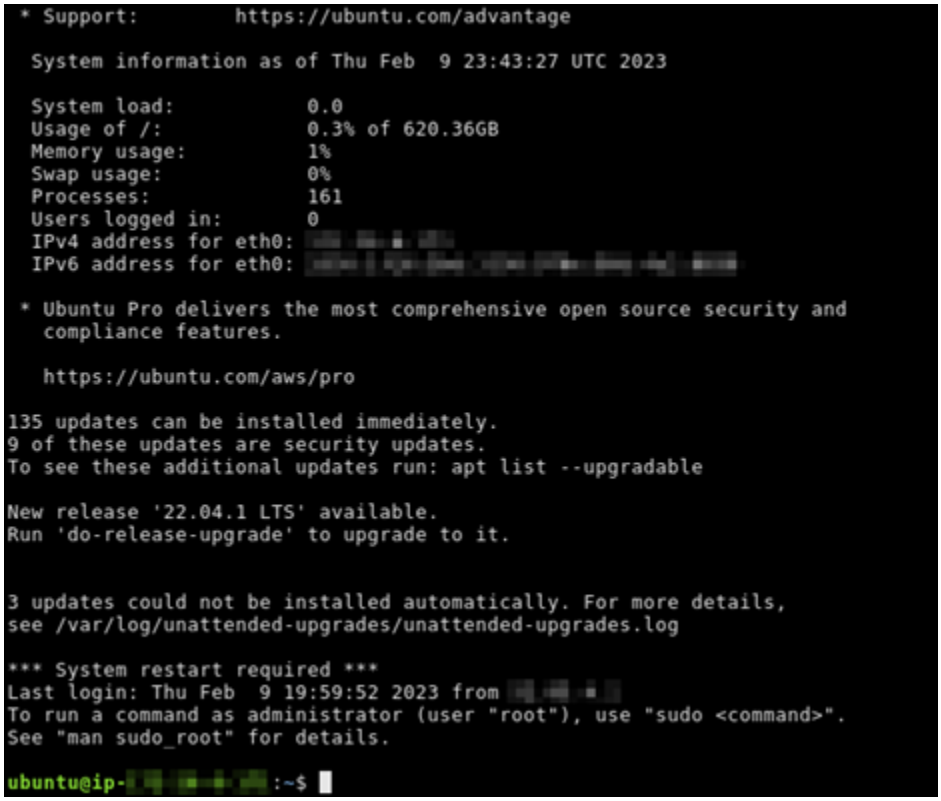
3. Ingrese el siguiente comando para establecer una conexión SSH con su equipo virtual. En el comando, sustituya *`user-name`* por el nombre de usuario de inicio de sesión y sustituya *`public-ip-address`* por la dirección IP pública de su equipo virtual.

```
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 Transferencia de archivos a un equipo virtual mediante Secure Copy.

Transferencia de archivos a un equipo virtual 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 NICE DCV basado en navegador disponible en la consola Lightsail for Research. Con el cliente NICE DCV, puede transferir rápidamente archivos individuales. Para obtener más información, consulte Acceso al sistema operativo de un equipo virtual.

Temas

Cumplir con los requisitos previos

Complete los siguientes requisitos previos antes de comenzar.

- Cree un ordenador virtual en Lightsail for Research. Para obtener más información, consulte Creación de un equipo virtual.
- 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 Visualización de los detalles de un equipo virtual.
- 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 Administración de los puertos de firewall de equipos virtuales.
- Obtenga el key pair predeterminado de Lightsail (DKP) para su ordenador virtual. Para obtener más información, consulte Creación de un equipo virtual.

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 Obtención de un par de claves para un equipo virtual. 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

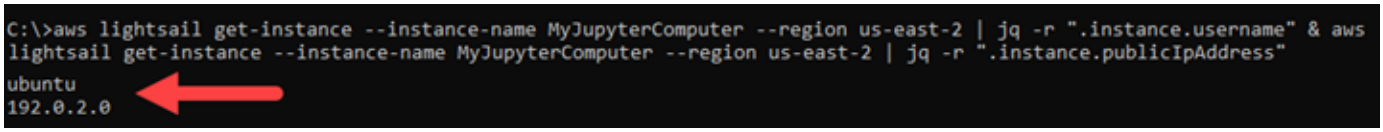
que se creó la computadora virtual, por ejemplo. `us-east-2` Sustituya *`computer-name`* por el nombre del equipo virtual al que desea conectarse.

```
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.

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

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 Obtención de un par de claves para un equipo virtual. 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

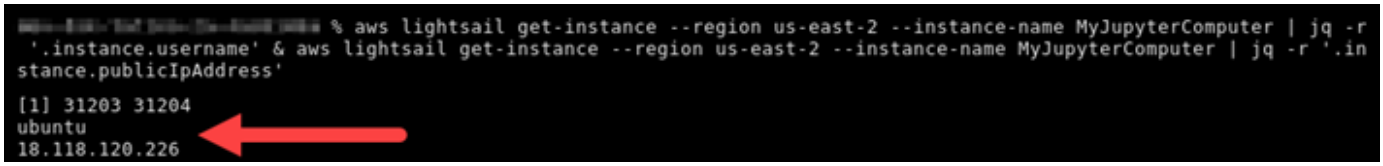
que se creó la computadora virtual, por ejemplo. `us-east-2` Sustituya *`computer-name`* por el nombre del equipo virtual al que desea conectarse.

```
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
```

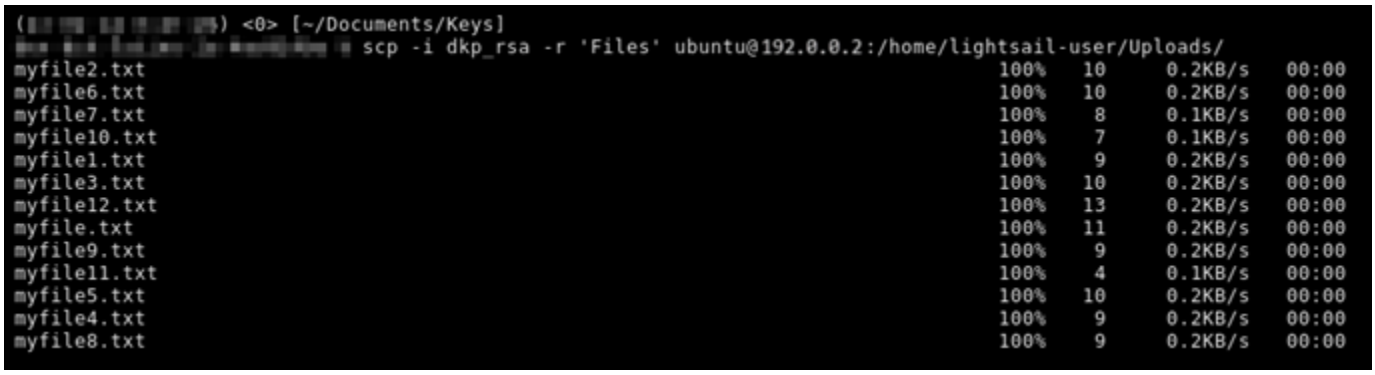
En el comando, sustituya:

- *`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.



Eliminación de un equipo virtual

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.

Almacenamiento

Amazon Lightsail para la investigación ofrece volúmenes de almacenamiento de nivel de bloque (discos) que se pueden adjuntar a un equipo virtual de Lightsail para la investigación 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 al ejecutar una base de datos en un equipo virtual de Lightsail para la investigación.

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

Crear un disco

Complete los siguientes pasos para crear un disco para su equipo virtual de Lightsail para la investigación.

1. Inicie sesión en la consola de Lightsail para la investigación.
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:

- Ser únicos dentro de cada Región de AWS de su cuenta de Lightsail para la investigación.
- Contener entre 2 y 255 caracteres.
- Comenzar y terminar por un carácter alfanumérico o un número.

5. Elija una Región de AWS para el 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.

Visualización de discos

Complete los siguientes pasos para ver los discos de su cuenta de Lightsail para la investigación y los detalles correspondientes.

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

   En la página Almacenamiento, se proporciona una vista completa de los discos de su cuenta de Lightsail para la investigación.

   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.
   - Adjuntado a: equipo de Lightsail al que se ha adjuntado el disco.
   - Fecha de creación: fecha en que se creó el disco.

Adjuntar un disco a un equipo virtual

Complete los siguientes pasos para adjuntar un disco a su equipo virtual en Lightsail para la investigación. Puede adjuntar hasta 15 discos a un equipo virtual. Cuando adjunta un disco al equipo

virtual mediante la consola de Lightsail para la investigación, el servicio lo formatea y lo monta 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 para la investigación monta los discos en el directorio `/home/lightsail-user/<disk-name>`; donde `<disk-name>` es el nombre que le ha dado 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 para la investigación.
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 Attach (Adjuntar).

Desasociar un disco de un equipo virtual

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

1. Inicie sesión en la consola de Lightsail para la investigación.
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.

Eliminar un disco

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 Desasociar un disco de un equipo virtual.

1. Inicie sesión en la consola de Lightsail para la investigación.
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 Delete (Eliminar).

Instantáneas

Las instantáneas son una copia en un momento dado de los datos. Puede crear instantáneas de sus equipos virtuales y discos de almacenamiento de Amazon Lightsail para la investigación y utilizarlas como referencia para crear nuevos equipos 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

Crear una instantánea

Complete los siguientes pasos para crear una instantánea de su equipo virtual o disco de Lightsail para la investigación.

1. Inicie sesión en la consola de Lightsail para la investigación.
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:

- Ser únicos dentro de cada Región de AWS de su cuenta de Lightsail para la investigación.
- Contener entre 2 y 255 caracteres.
- Comenzar y terminar por un carácter alfanumérico o un número.

5. Seleccione Create snapshot (Crear instantánea).

Visualización de instantáneas

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

1. Inicie sesión en la consola de Lightsail para la investigación.
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 equipo virtual o disco de Lightsail para la investigación 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 para la investigación.
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

Complete los siguientes pasos para eliminar una instantánea.

1. Inicie sesión en la consola de Lightsail para la investigación.
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 Amazon 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.

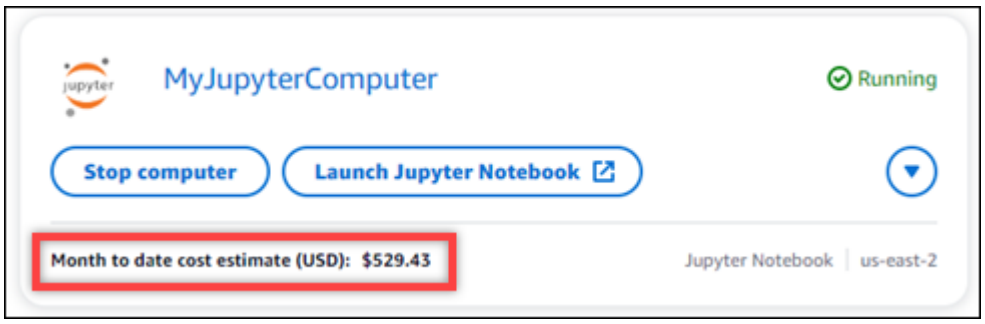
> **Important**
>
> Una estimación es un costo estimado que se basa en el uso del recurso. El coste real se basará en el uso real de los recursos, no en la estimación que se muestra en la consola de Lightsail for Research. Los costos reales se muestran en su estado de AWS Billing cuenta. Inicie sesión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

Temas

Supervise las estimaciones de uso y costos.

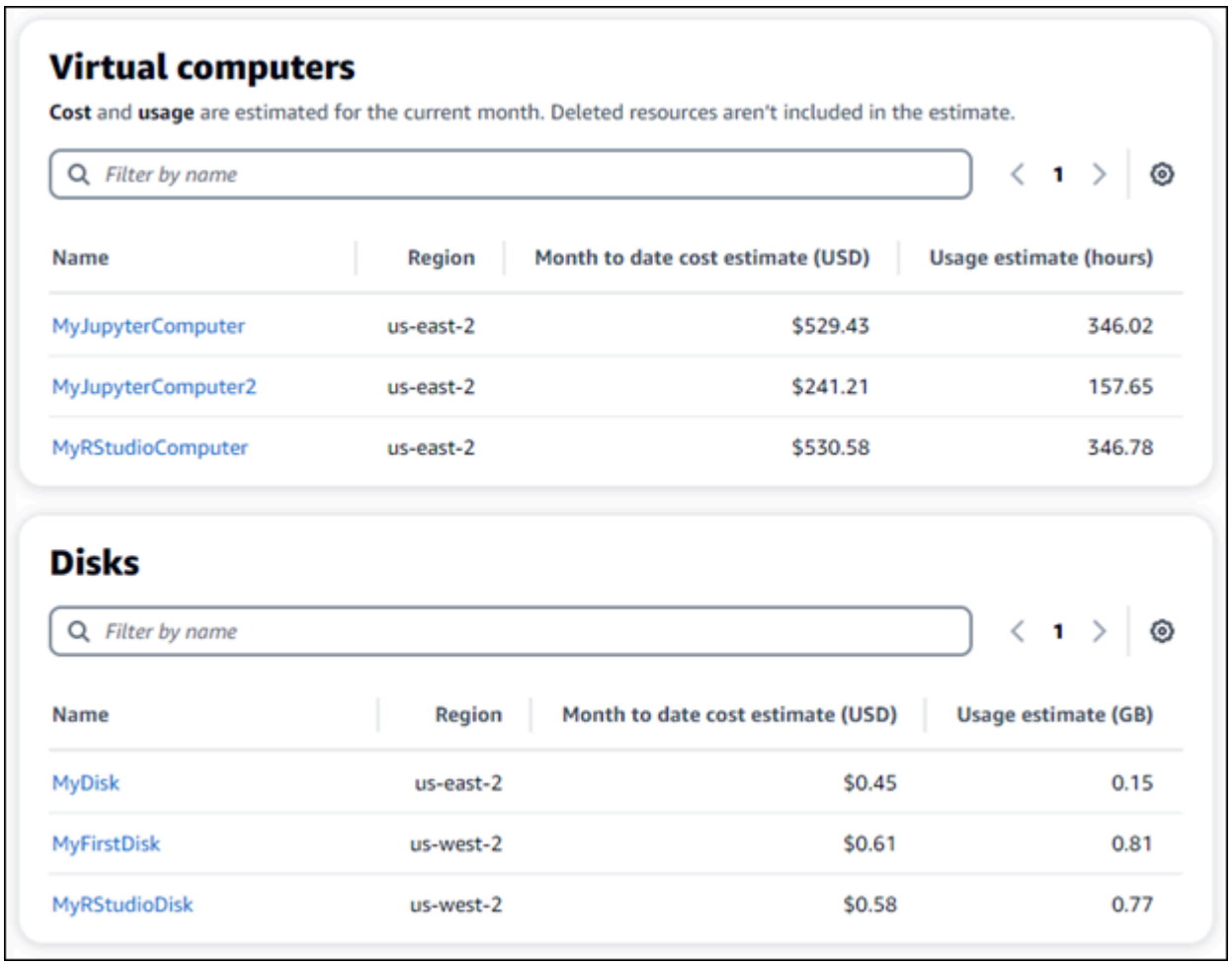
Las estimaciones de coste y uso mensuales de sus recursos de Lightsail for Research se muestran en las siguientes áreas de la consola de Lightsail for Research.

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.


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

Control de costes

El control de costos usa reglas que define para ayudar a administrar el uso y el costo de sus equipos virtuales de Lightsail para la investigación.

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, en el caso de Lightsail para la investigación, lo detiene. Dejará de incurrir en los cargos por hora estándar una vez que se detenga el equipo virtual.

Temas

Creación de una regla

Complete los siguientes pasos para crear una regla para su equipo virtual de Lightsail para la investigación.

> **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 para la investigación.
2. En el panel de navegación, elija Control de costos.
3. Elija Create rule (Crear 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 para la investigación detiene automáticamente el equipo cuando el uso de la CPU es menor o igual que el 5 por ciento durante un periodo de 30 minutos.

6. Elija Create rule (Crear regla).
7. Confirme que la información de la nueva regla es correcta y, a continuación, seleccione Confirmar.

Eliminación de una regla

Complete los siguientes pasos para eliminar una regla para su equipo virtual de Lightsail para la investigación.

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

Etiquetas

Con Amazon Lightsail para la investigación, puede asignar etiquetas a los 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 para la investigación:

- 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, 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 se reserva para uso de AWS.

Temas

Crear una etiqueta

Complete los siguientes pasos para crear una etiqueta para su equipo virtual de Lightsail para la investigación. Los pasos son similares a los de los discos e instantáneas de Lightsail para la investigación.

1. Inicie sesión en la consola de Lightsail para la investigación en la consola de Lightsail para la investigación.
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 Tags (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 una etiqueta

Complete los siguientes pasos para eliminar una etiqueta de su equipo virtual de Lightsail para la investigación. Los pasos son similares a los de los discos e instantáneas de Lightsail para la investigación.

1. Inicie sesión en la consola de Lightsail para la investigación en la consola de Lightsail para la investigación.
2. En el panel de navegación, elija Equipos virtuales.
3. Elija el equipo virtual del que desea eliminar la etiqueta.
4. Elija la pestaña Tags (Etiquetas).
5. Elija Manage tags (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 Save changes (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. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos 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 Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es 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:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 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) 140-2.

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 o con Servicios de AWS otros dispositivos mediante la consola, la API AWS CLI o los SDK. AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede 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. El IAM es un servicio Servicio de AWS que puede utilizar 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 el trabajo que realice en Lightsail for Research.

Usuario del servicio: si utiliza el servicio Lightsail for Research para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más funciones de Lightsail for Research para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función de Lightsail for Research, consulte. Solución de problemas de identidad y acceso a Amazon Lightsail for Research

Administrador de servicios: si está a cargo de los recursos de Lightsail for Research en su empresa, probablemente tenga acceso completo a Lightsail for Research. Es su trabajo determinar a qué funciones y recursos de Lightsail for Research deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con Lightsail for Research, consulte. Cómo funciona Amazon Lightsail for Research con IAM

Administrador de IAM: si es administrador de IAM, puede que desee obtener información detallada sobre cómo redactar políticas para administrar el acceso a Lightsail for Research. Para ver ejemplos de políticas basadas en la identidad de Lightsail for Research que puede usar en IAM, consulte. Ejemplos de políticas basadas en identidad para Amazon Lightsail for Research

Autenticación con identidades

La autenticación es la forma de iniciar sesión con sus credenciales de identidad AWS . Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus

credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como 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, incluidos los que requieren acceso de administrador, 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 de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. 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 propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué

pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .

- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta 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 Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada 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.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

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.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

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 identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir 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 política JSON que se asocian a un recurso. 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 en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

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.

Listas de control de acceso (ACL)

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

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para 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 AWS determinar 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
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
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 identidad, consulte Creación de políticas de IAM 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. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas 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

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. 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 en función de 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. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

Acciones políticas para Lightsail for Research

Admite acciones de política	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. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

Admite 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. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, 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 sus ARN, 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

Admite 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` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. 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

ACL en Lightsail for Research

Admite las ACL	No

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

ABAC con Lightsail para la investigación

Admite 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. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

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 ¿Qué es 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

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando se inicia sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales de servicios cruzados para Lightsail for Research

Admite sesiones de acceso directo (FAS)	No

Cuando utiliza un usuario o un rol de IAM para realizar acciones en él AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

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 Creación de 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

Compatible 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, consulte 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. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede

crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

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 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 los ARN de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon Lightsail for Research en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola Lightsail for Research
- Cómo permitir a los usuarios consultar sus propios permisos

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 trabajo 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 AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice 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 Política de validación de Analizador de acceso de IAM en la Guía de 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 solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las 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, permite 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 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

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

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de

control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para 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 obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos 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. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.

- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: este documento técnico describe cómo las empresas pueden crear aplicaciones aptas para AWS la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

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 Instantáneas y Crear una instantánea.

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 de seguridad de IAM principal. También puede 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. AWS Management Console 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 para la investigación

En la siguiente tabla se describen las versiones de la documentación de Lightsail para la investigación.

Cambio	Descripción	Fecha
Versión inicial	Versión inicial de la Guía del usuario de Lightsail para la investigación.	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.