Manual do usuário

Amazon Lightsail para pesquisa

Amazon Lightsail para pesquisa: Manual do usuário

Table of Contents

O que é o Amazon Lightsail for Research?

Com o Amazon Lightsail for Research, acadêmicos e pesquisadores podem criar computadores virtuais poderosos na nuvem da Amazon Web Services ().AWS Esses computadores virtuais vêm com aplicativos de pesquisa pré-instalados, como o RStudio Scilab.

Com o Lightsail for Research, você pode carregar dados diretamente de um navegador da Web para começar seu trabalho. Você pode criar e excluir seus computadores virtuais a qualquer momento, o que lhe dá acesso sob demanda a poderosos recursos de computação.

Você paga somente pelo tempo que precisar do computador virtual. O Lightsail for Research oferece controles orçamentários que podem parar automaticamente seu computador quando ele atinge um limite de custo pré-configurado, para que você não precise se preocupar com cobranças excedentes.

Tudo o que você faz no console do Lightsail for Research tem o respaldo de uma ferramenta disponível ao público. API Saiba como instalar e usar o AWS CLIe APIpara o Amazon Lightsail.

Definição de preço

Com o Lightsail for Research, você paga somente pelos recursos que criar e usar. Para obter mais informações, consulte os preços do Lightsail for Research.

Disponibilidade

O Lightsail for Research está disponível nas AWS mesmas regiões do Amazon Lightsail, com exceção da região Leste dos EUA (Norte da Virgínia). O Lightsail for Research também usa os mesmos endpoints do Lightsail. Para ver as AWS regiões e endpoints atualmente compatíveis com o Lightsail, consulte Lightsail Endpoints and Quotas na Referência geral.AWS

Configurando o Amazon Lightsail for Research

Se você for um AWS cliente novo, preencha os pré-requisitos de configuração listados nesta página antes de começar a usar o Amazon Lightsail for Research.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira sua senha.

Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .

2. Ative a autenticação multifator (MFA) para seu usuário root.

   Para obter instruções, consulte Habilitar um MFA dispositivo virtual para seu usuário Conta da AWS root (console) no Guia IAM do usuário.

Criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .

2. No IAM Identity Center, conceda acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para entrar com seu usuário do IAM Identity Center, use o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Tutorial: Comece a usar os computadores virtuais do Lightsail for Research

Use este tutorial para começar a usar os computadores virtuais Amazon Lightsail for Research. Você aprenderá a criar, conectar-se e usar um computador virtual. No Lightsail for Research, um computador virtual é uma estação de trabalho de pesquisa que você cria e gerencia no. Nuvem AWS Os computadores virtuais são baseados em instâncias Linux do Lightsail com o sistema operacional Ubuntu. Em seu computador virtual, você pode pré-configurar um aplicativo de pesquisa como JupyterLabRStudio, Scilab e muito mais.

O computador virtual que você cria neste tutorial incorrerá em taxas de uso a partir do momento em que você o cria até o momento em que o exclui. A exclusão é a etapa final deste tutorial. Para obter mais informações sobre preços, consulte Preços do Lightsail for Research.

Tópicos

Etapa 1: Concluir os pré-requisitos

Se você for um AWS cliente novo, preencha os pré-requisitos de configuração antes de começar a usar o Amazon Lightsail for Research. Para obter mais informações, consulte Configurando o Amazon Lightsail for Research.

Etapa 2: criar um computador virtual

Você pode criar um computador virtual usando o console do Lightsail for Research, conforme descrito no procedimento a seguir. Este tutorial tem o objetivo de ajudar você a iniciar rapidamente seu primeiro computador virtual. Também recomendamos explorar as aplicações e os planos de

hardware disponíveis. Para ter mais informações, consulte Escolha imagens de aplicativos e planos de hardware para o Lightsail for Research e Crie um computador virtual Lightsail for Research.

1. Faça login no console do Lightsail for Research.
2. Na página inicial, escolha Criar computador virtual.
3. Selecione um Região da AWS para seu computador virtual.

   Escolha um Região da AWS que esteja mais próximo da sua localização física para reduzir a latência.
4. Escolha um aplicativo, também conhecido como blueprint no API Lightsail.

   O aplicativo escolhido é instalado e configurado no seu computador virtual quando você o cria.
5. Escolha um plano de hardware, também conhecido como pacote no API Lightsail.

   Os planos de hardware oferecem diferentes quantidades de poder de processamento, incluindo v CPU cores, memória, armazenamento e transferência mensal de dados. O Lightsail for Research oferece planos padrão GPU e planos para computadores virtuais. Escolha um plano padrão quando a necessidade computacional do seu trabalho for baixa. Escolha um GPU plano quando esse requisito for alto, como ao executar modelos de aprendizado de máquina ou outras tarefas computacionalmente intensivas.
6. Insira um nome para o computador virtual.
7. Escolha Criar computador virtual no painel Resumo.

Após o seu novo computador virtual estar ativo e em funcionamento, siga para a próxima etapa deste tutorial para aprender como iniciar a aplicação do computador.

Etapa 3: inicie o aplicativo de um computador virtual

Depois de criar um computador virtual e ele estar em um estado em execução, você pode iniciar uma sessão virtual no seu navegador da web. Com a sessão, você pode interagir e gerenciar o aplicativo que está instalado no seu computador virtual.

1. Escolha Computadores virtuais no painel de navegação do console do Lightsail for Research.
2. Localize o nome do computador virtual que você criou na Etapa 1 e escolha Iniciar aplicativo. Por exemplo, Launch JupyterLab. Uma sessão do aplicativo abre em uma nova janela do navegador da web.

> **Important**
>
> Se o seu navegador da web tiver um bloqueador de pop-ups instalado, talvez seja necessário permitir pop-ups do domínio aws.amazon.com antes de abrir sua sessão.

Para saber como se conectar ao computador virtual, prossiga para a próxima etapa deste tutorial.

Etapa 4: conectar o seu computador virtual

Você pode conectar-se ao seu computador virtual usando os seguintes métodos:

- Use o NICE DCV cliente baseado em navegador disponível no console do Lightsail for Research. Com NICEDCV, você pode usar uma interface gráfica de usuário (GUI) para interagir com seu aplicativo de pesquisa e com o sistema operacional do seu computador virtual.

  Você também pode acessar a interface de linha de comando do seu computador virtual e transferir arquivos usando o cliente baseado em navegador NICEDCV.
- Use um cliente shell (SSH) seguro, como Open SSHTTY, Pu ou Windows Subsystem for Linux, para acessar a interface de linha de comando do seu computador virtual. Com um SSH cliente, você pode editar scripts e arquivos de configuração.
- Use Secure Copy (SCP) para transferir arquivos com segurança entre o computador local e o computador virtual. ComSCP, você pode começar seu trabalho localmente e continuar em seu computador virtual. Você também pode baixar arquivos do seu computador virtual para copiar seu trabalho para o seu computador local.

Você deve fornecer o key pair do seu computador virtual para se conectar a ele usando SSH ou transferir arquivos usandoSCP. Um key pair é um conjunto de credenciais de segurança que você usa para provar sua identidade ao se conectar a um computador virtual do Lightsail for Research. Um par de chaves consiste em uma chave pública e uma chave privada.

Para obter mais informações sobre como conectar-se ao seu computador virtual, consulte a documentação a seguir:

- Estabeleça uma conexão de protocolo de exibição remota:
  - Acesse um aplicativo de computador virtual Lightsail for Research

  - Acesse o sistema operacional do seu computador virtual Lightsail for Research
- Estabeleça uma SSH conexão ou transfira arquivos usandoSCP:
  - Obtenha um par de chaves para um computador virtual Lightsail for Research
  - Conecte-se a um computador virtual Lightsail for Research usando o Secure Shell
  - Transfira arquivos para computadores virtuais do Lightsail for Research usando o Secure Copy

Para aprender sobre armazenamento para o seu computador virtual, prossiga para a próxima etapa deste tutorial.

Etapa 5: adicionar armazenamento ao seu computador virtual

O Lightsail for Research fornece volumes de armazenamento (discos) em nível de bloco que você pode conectar a um computador virtual. Mesmo que o seu computador virtual venha com um disco do sistema, você pode anexar discos adicionais ao seu computador virtual conforme suas necessidades de armazenamento mudam. Você também pode desanexar um disco de um computador virtual e anexá-lo a outro computador virtual.

Quando você conecta um disco ao seu computador virtual usando o console, o Lightsail for Research formata e monta automaticamente o disco em seu sistema operacional. Esse processo leva alguns minutos, então você deve confirmar se o disco está no status Montado antes de começar a usá-lo.

Para obter mais informações sobre como criar, anexar e gerenciar um disco, consulte a documentação a seguir:

- Crie um disco de armazenamento no console do Lightsail for Research
- Veja os detalhes do disco de armazenamento no console do Lightsail for Research
- Adicione armazenamento a um computador virtual no Lightsail for Research
- Separe um disco de um computador virtual no Lightsail for Research
- Exclua discos de armazenamento não utilizados no Lightsail for Research

Para aprender a fazer backup de seu computador virtual, prossiga para a próxima etapa deste tutorial.

Etapa 6: criar um snapshot

Os instantâneos são uma point-in-time cópia dos seus dados. Você pode criar snapshots dos seus computadores virtuais e utilizá-los como bases para criar novos computadores ou para backup de dados. Um snapshot contém todos os dados necessários para restaurar o computador (a partir do momento em que o snapshot foi criado).

Para mais informações sobre como criar e gerenciar snapshots, consulte a seguinte documentação:

- Crie instantâneos dos computadores ou discos virtuais do Lightsail for Research
- Visualize e gerencie instantâneos de disco e computadores virtuais no Lightsail for Research
- Crie um computador ou disco virtual a partir de um snapshot
- Excluir um instantâneo no console do Lightsail for Research

Para aprender a limpar os recursos de seu computador virtual, prossiga para a próxima etapa deste tutorial.

Etapa 7: limpar

Após concluir o uso do computador virtual criado para este tutorial, você pode excluí-lo. Isso interrompe a geração de cobranças para o computador virtual, caso você não o necessite mais.

Excluir um computador virtual não deleta os snapshots associados ou discos anexados a ele. Se você criou snapshots e discos, você deve excluí-los manualmente para interromper a geração de cobranças relacionadas a eles.

Para salvar o seu computador virtual para uso posterior, mas evitando incorrer em cobranças com preços padrão por hora, você pode interromper o computador virtual em vez de excluí-lo. Você poderá reiniciá-la mais tarde. Para obter mais informações, consulte Veja os detalhes do computador virtual Lightsail for Research. Para obter mais informações sobre preços, consulte Preços do Lightsail for Research.

> **Important**
>
> Excluir um recurso do Lightsail for Research é uma ação permanente. Não foi possível recuperar o objeto excluído. Se você precisar dos dados posteriormente, crie um snapshot

de seu computador virtual antes de excluí-lo. Para obter mais informações, consulte Criar um snapshot.

1. Faça login no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação.
3. Escolha o computador virtual a ser excluído.
4. Escolha Ações e, em seguida, escolha Excluir computador virtual.
5. Digite confirmar no bloco de texto. Em seguida, escolha Excluir computador virtual.

Comece a usar aplicativos de ciência de dados no Lightsail for Research

Os tutoriais a seguir fornecem informações adicionais sobre como começar a usar aplicativos específicos que estão disponíveis no Lightsail for Research.

Tópicos

> **Note**
>
> Um tutorial detalhado para começar a usar o Lightsail for Research, publicado no Public RStudio Sector Blog. AWS Para obter mais informações, consulte Introdução ao Amazon Lightsail for Research: um tutorial usando. RStudio

Inicie e use JupyterLab no Lightsail for Research

Neste tutorial, mostramos como começar a gerenciar e usar seu computador JupyterLab virtual no Amazon Lightsail for Research.

Tópicos

Etapa 1: Concluir os pré-requisitos

Crie um computador virtual usando o JupyterLab aplicativo, caso ainda não tenha feito isso. Para obter mais informações, consulte Crie um computador virtual Lightsail for Research.

Depois que seu novo computador virtual estiver instalado e funcionando, continue com a seção de inicialização do JupyterLab aplicativo deste tutorial.

Etapa 2: (opcional) adicionar espaço de armazenamento

Seu computador virtual vem com um disco do sistema. No entanto, à medida que suas necessidades de armazenamento mudam, você pode anexar discos adicionais ao seu computador virtual para aumentar o espaço de armazenamento.

Você também pode armazenar seus arquivos de trabalho em um disco conectado. Em seguida, você pode desconectar o disco e conectá-lo a um computador virtual diferente para mover rapidamente seus arquivos de um computador para outro.

Como alternativa, você pode criar um snapshot de um disco anexado que tenha seus arquivos de trabalho e depois criar um disco duplicado a partir do snapshot. Em seguida, você pode conectar o novo disco duplicado a outro computador para duplicar seu trabalho em diferentes computadores virtuais. Para ter mais informações, consulte Crie um disco de armazenamento no console do Lightsail for Research e Adicione armazenamento a um computador virtual no Lightsail for Research.

> **Note**
>
> Quando você conecta um disco ao seu computador virtual usando o console, o Lightsail for Research formata e monta automaticamente o disco. Esse processo leva alguns minutos, portanto, você deve confirmar que o disco atingiu o status de Montagem antes de começar a usá-lo. Por padrão, o Lightsail for Research monta discos no diretório. `/home/lightsail-user/<disk-name>` `<disk-name>`é o nome que você deu ao seu disco.

Etapa 3: transferir e baixar arquivos

Você pode fazer upload de arquivos para o seu computador JupyterLab virtual e baixar arquivos dele. Para fazer isso, você deve executar as etapas a seguir:

1. Obtenha um par de chaves do Amazon Lightsail. Para obter mais informações, consulte Obtenha um par de chaves para um computador virtual Lightsail for Research.

2. Depois de ter o par de chaves, você pode usá-lo para estabelecer uma conexão usando o utilitário Secure Copy (SCP). SCPpermite fazer upload e download de arquivos usando o prompt de comando ou o terminal. Para obter mais informações, consulte Transfira arquivos para computadores virtuais do Lightsail for Research usando o Secure Copy.
3. (Opcional) Você também pode usar o key pair para se conectar ao seu computador virtual comSSH. Para obter mais informações, consulte Conecte-se a um computador virtual Lightsail for Research usando o Secure Shell.

> **Note**
>
> Você também pode acessar a interface de linha de comando do seu computador virtual e transferir arquivos usando o cliente baseado em navegador NICEDCV. NICEDCVestá disponível no console do Lightsail for Research. Para ter mais informações, consulte Acesse um aplicativo de computador virtual Lightsail for Research e Acesse o sistema operacional do seu computador virtual Lightsail for Research.

Para gerenciar seus arquivos de projeto em um disco de armazenamento anexado, certifique-se de carregá-los no diretório de montagem correto para o disco conectado. Quando você conecta um disco ao seu computador virtual usando o console, o Lightsail for Research formata e monta automaticamente o disco no diretório. `/home/lightsail-user/<disk-name>` `<disk-name>`é o nome que você deu ao seu disco.

Etapa 4: iniciar o JupyterLab aplicativo

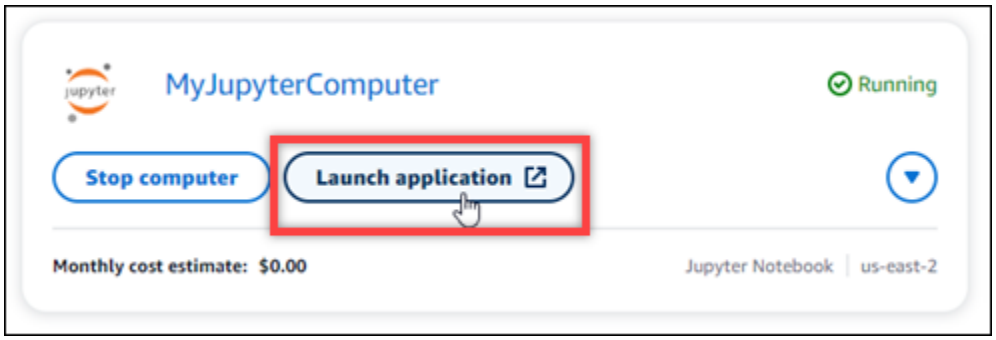
Conclua o procedimento a seguir para iniciar o JupyterLab aplicativo em seu novo computador virtual.

> **Important**
>
> Não atualize o sistema operacional nem o JupyterLab aplicativo, mesmo que você seja solicitado a fazer isso. Em vez disso, escolha a opção de fechar ou ignorar essas solicitações. Além disso, não modifique nenhum dos arquivos que estão no diretório /home/lightsail-admin/. Essas ações podem tornar o computador virtual inutilizável.

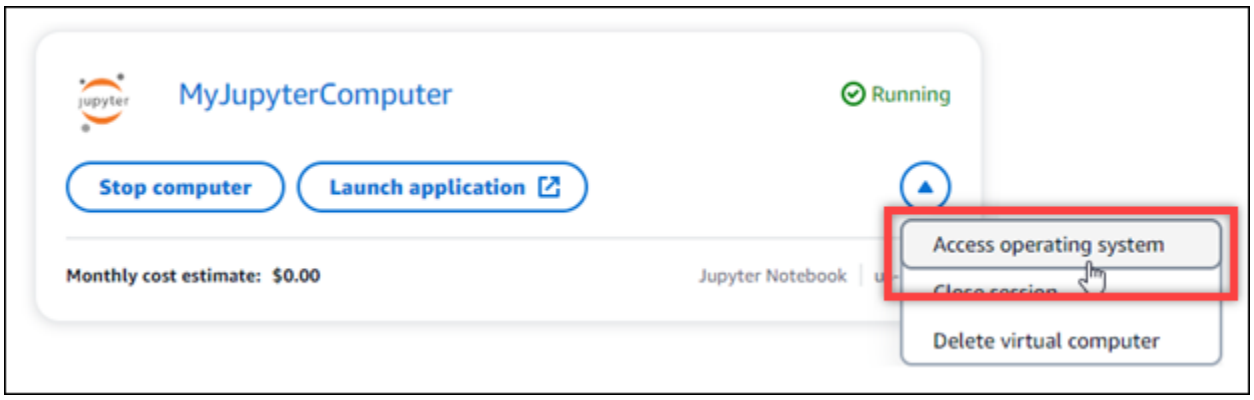
1. Faça login no console do Lightsail for Research.

2. Escolha Computadores virtuais no painel de navegação para ver uma lista de computadores virtuais disponíveis em sua conta.
3. Na página Computadores virtuais, encontre seu computador virtual e escolha uma das seguintes opções para se conectar a ele:

   a. (Recomendado) Escolha Iniciar aplicativo para iniciar o JupyterLab aplicativo no modo focado. Se você não se conectou ao seu computador virtual recentemente, talvez precise esperar alguns minutos enquanto o Lightsail for Research prepara sua sessão.



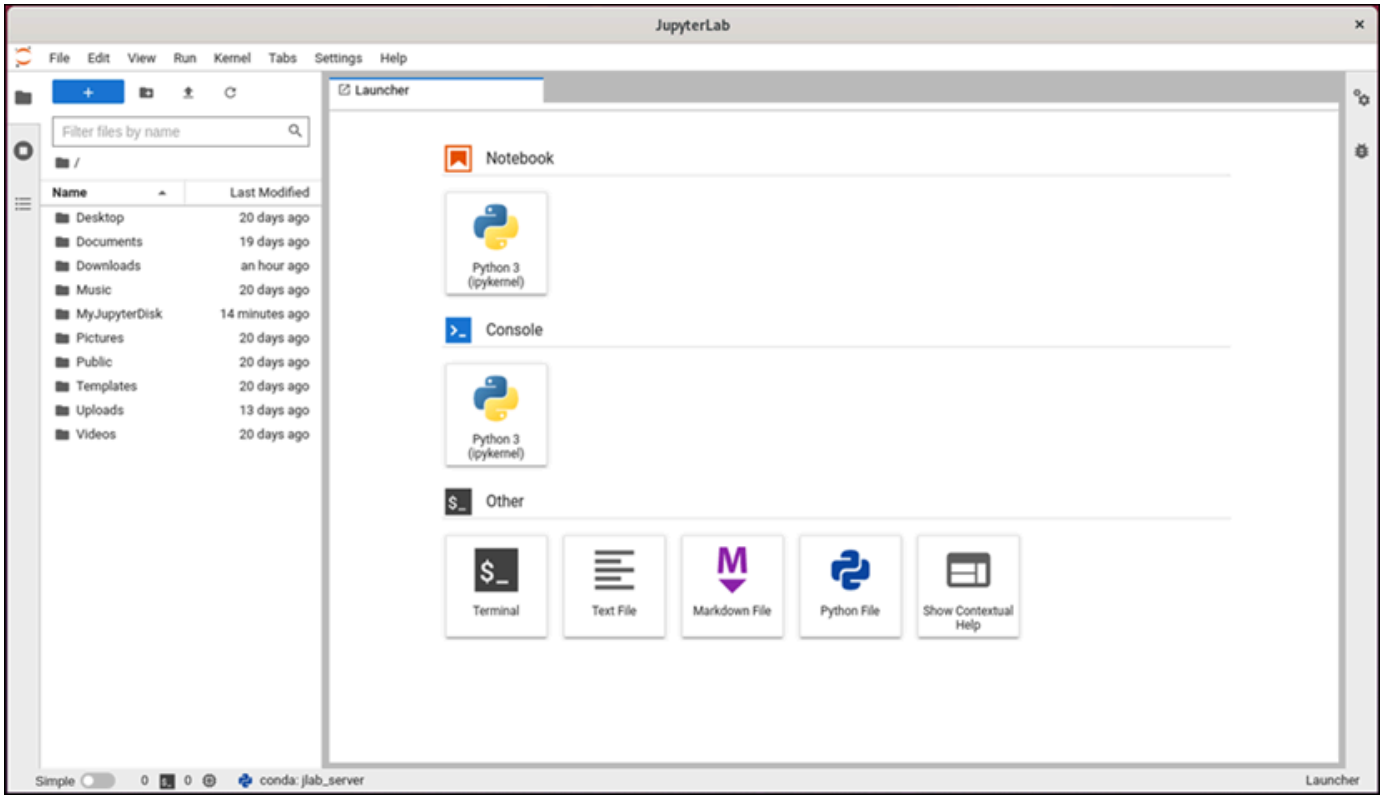
   b. Escolha o menu suspenso do computador e, em seguida, escolha Acessar sistema operacional para acessar a área de trabalho do seu computador virtual.



O Lightsail for Research executa alguns comandos para iniciar a conexão do protocolo de exibição remota. Depois de alguns instantes, uma nova janela da guia do navegador é aberta com uma conexão de área de trabalho virtual estabelecida com seu computador virtual. Se você escolheu a opção Iniciar aplicativo, vá para a próxima etapa desse procedimento para abrir um arquivo no JupyterLab aplicativo. Se você escolher a opção Acessar sistema operacional, poderá abrir outros aplicativos por meio da área de trabalho do Ubuntu.

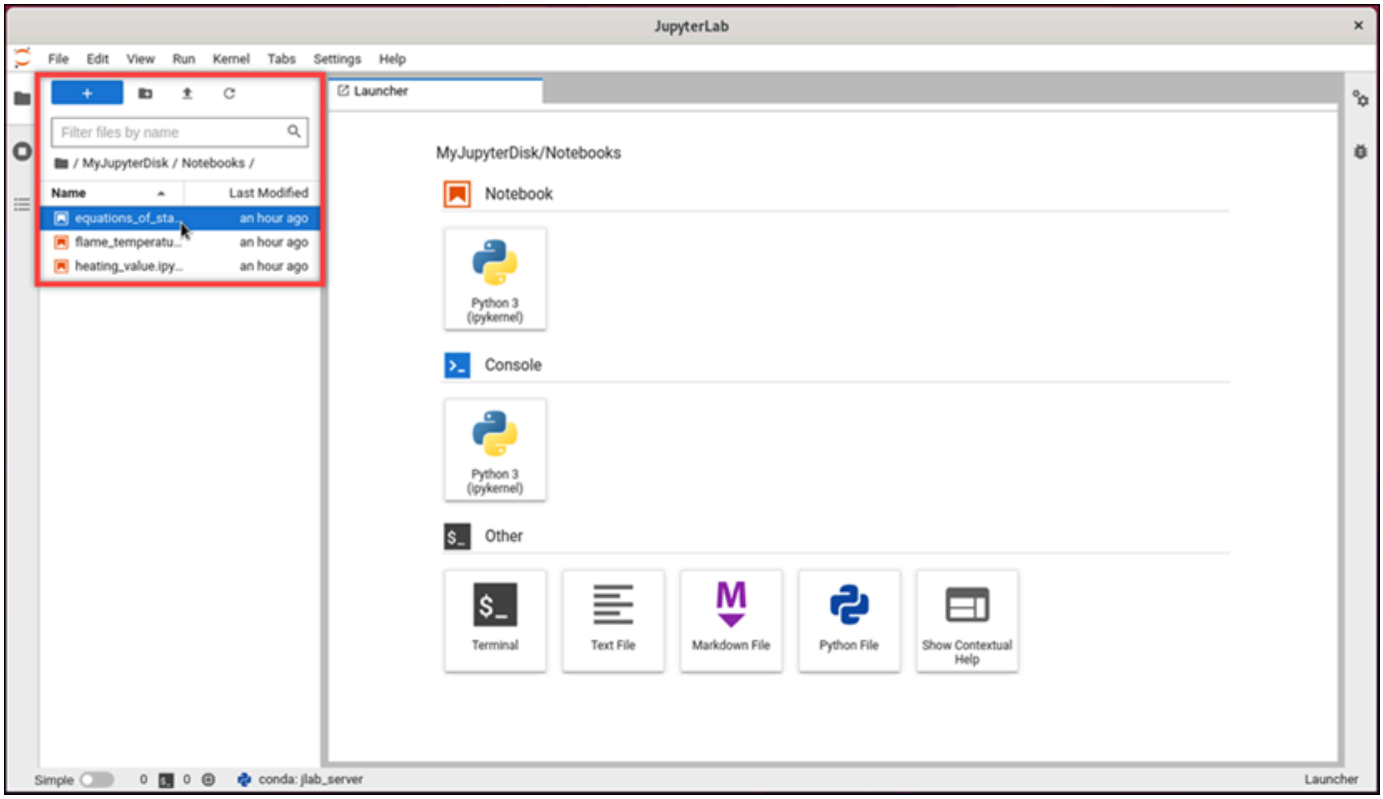
> **Note**
>
> Seu navegador pode solicitar que você autorize o compartilhamento da sua área de transferência. Permitir isso permite copiar e colar entre o computador local e o computador virtual.
>
> O Ubuntu também pode solicitar uma configuração inicial. Siga as instruções até concluir a configuração e poder usar o sistema operacional.

4. O JupyterLab aplicativo é aberto. No menu do inicializador, você pode criar um novo notebook, iniciar o console, iniciar o terminal e criar vários arquivos.

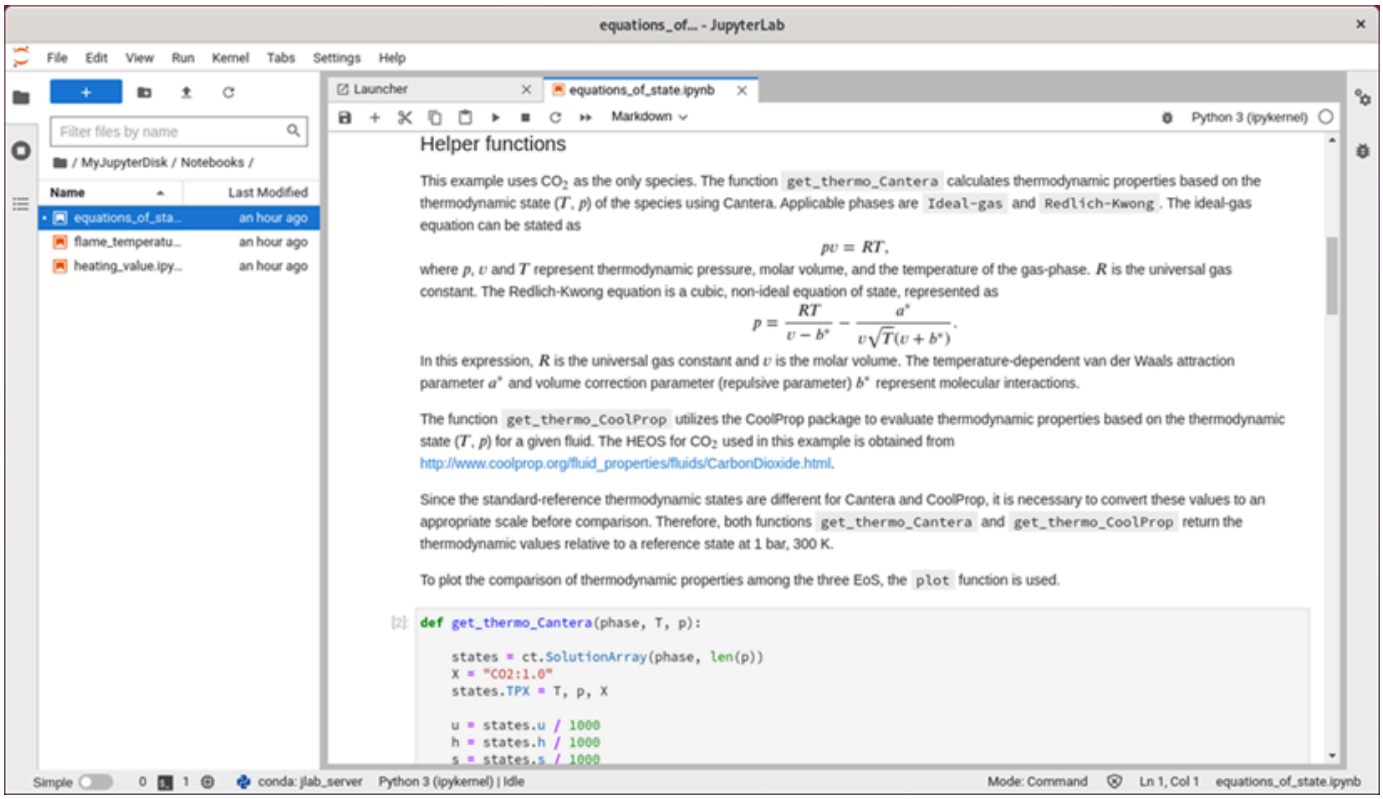


5. Para abrir um arquivo JupyterLab, no painel Navegador de arquivos, escolha o diretório ou a pasta em que os arquivos do projeto estão armazenados. Em seguida, escolha o arquivo para abrir.

   Se você fez upload dos arquivos do projeto em um disco conectado, procure o diretório em que o disco está montado. Por padrão, o Lightsail for Research monta discos no diretório. `/home/lightsail-user/<disk-name>` `<disk-name>`é o nome que você deu ao seu disco. No exemplo a seguir, o `MyJupyterDisk` diretório representa o disco montado e o `Notebooks` subdiretório contém nossos arquivos do caderno Jupyter.



No exemplo a seguir, abrimos o arquivo do `equations_of_state.ipynb` caderno Jupyter.



Para obter informações sobre como começar a usar, prossiga para a Etapa 5: leia a JupyterLab documentação seção deste tutorial.

Etapa 5: leia a JupyterLab documentação

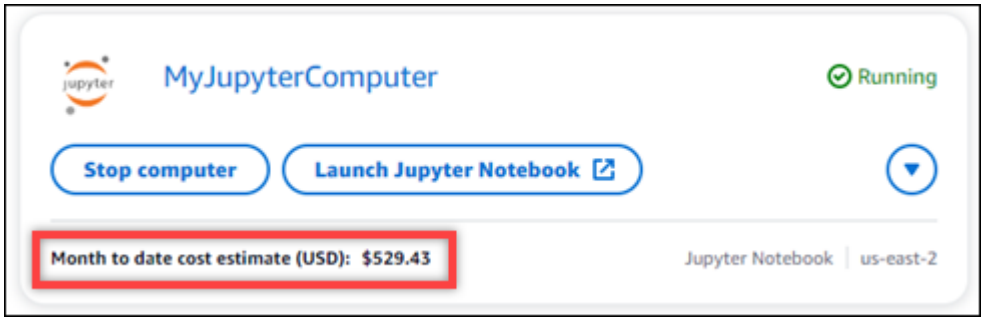
Se você não estiver familiarizado JupyterLab, recomendamos que leia a documentação oficial deles. Os seguintes recursos JupyterLab on-line estão disponíveis:

- JupyterLabDocumentação
- Fórum de discussão do Jupyter
- JupyterLab em StackOverflow
- JupyterLab em GitHub

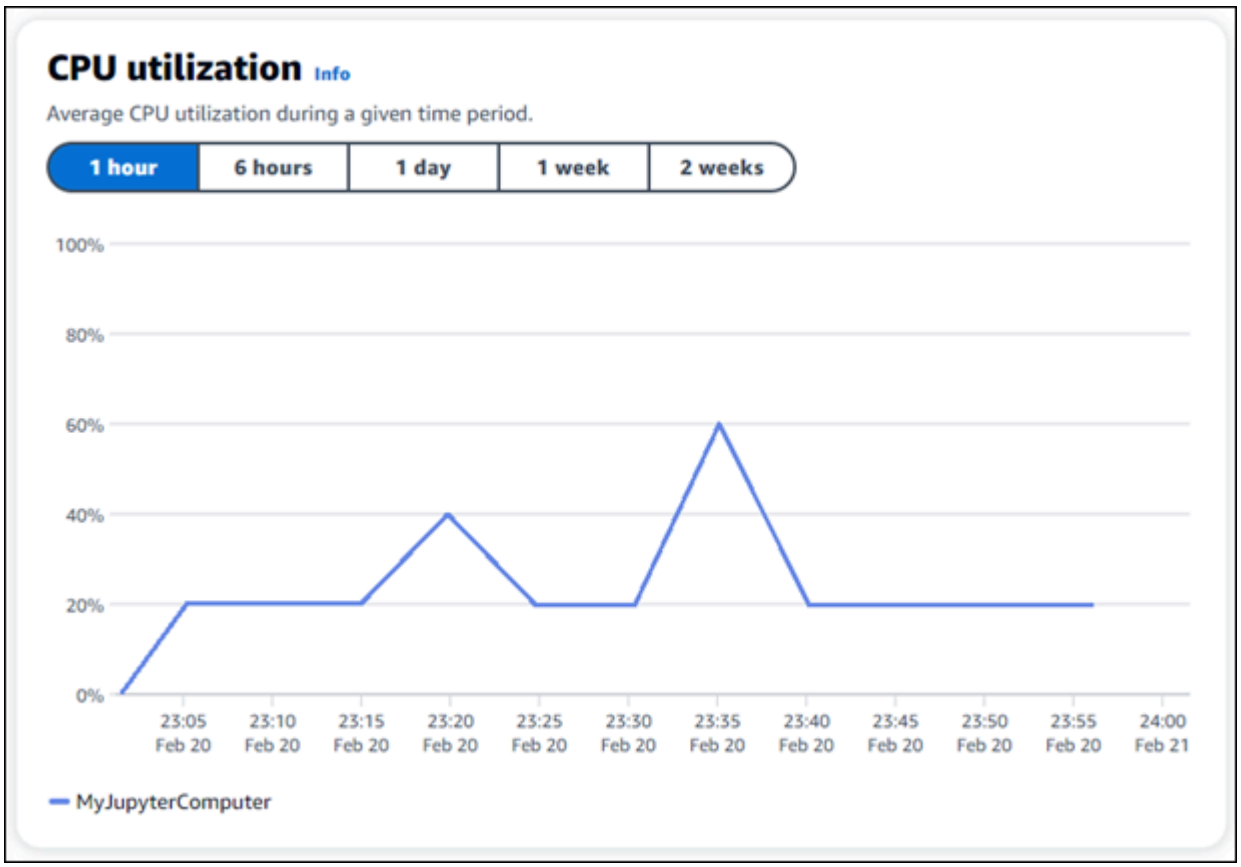
Etapa 6: (opcional) monitorar o uso e os custos

As estimativas mensais de custo e uso de seus recursos do Lightsail for Research são exibidas nas seguintes áreas do console do Lightsail for Research.

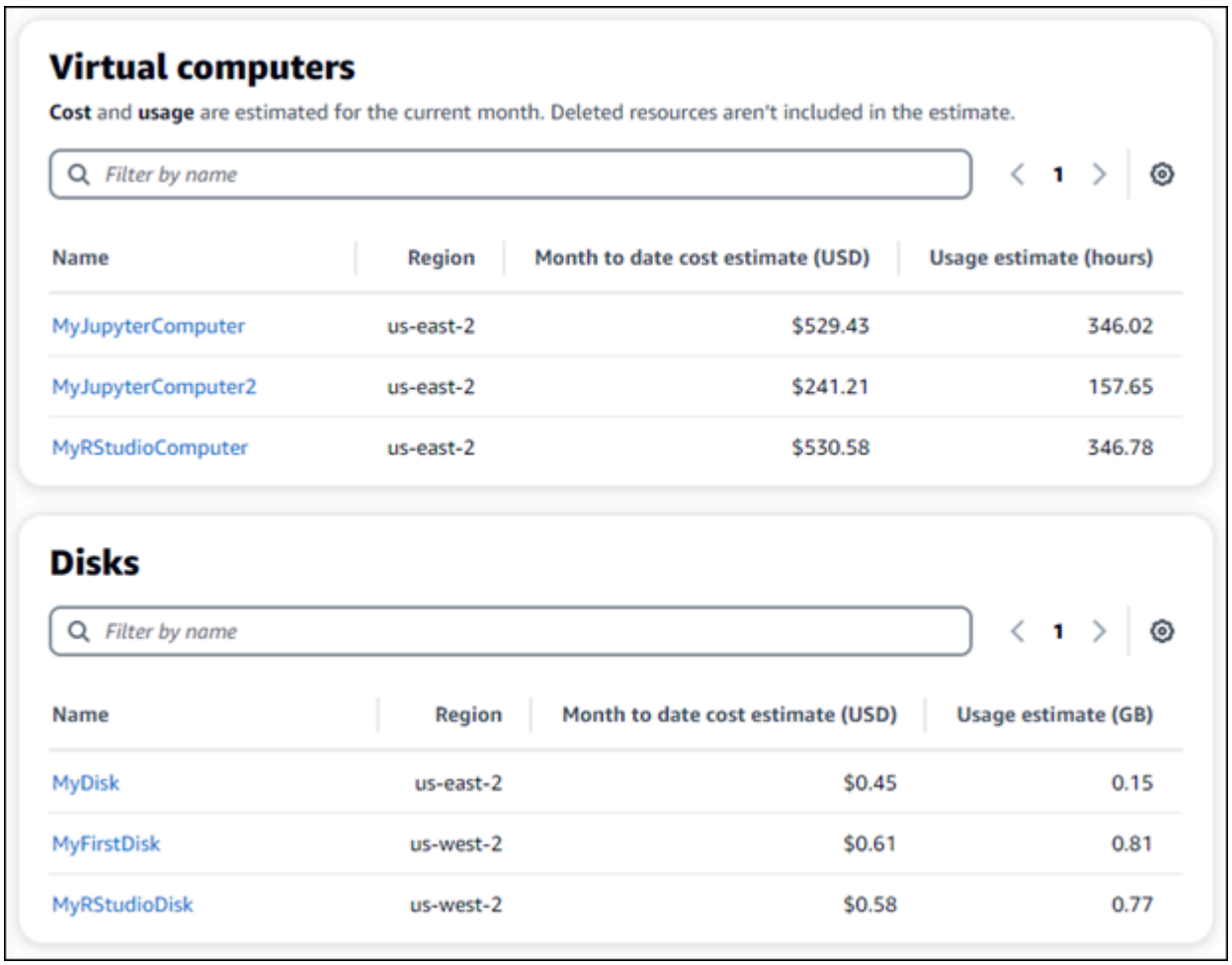
1. Escolha Computadores virtuais no painel de navegação do console do Lightsail for Research. A estimativa de custo mensal para seus computadores virtuais está listada em cada computador virtual em execução.



2. Para ver a CPU utilização de um computador virtual, escolha o nome do computador virtual e, em seguida, escolha a guia Painel.



3. Para ver as estimativas de custo e uso do mês para todos os seus recursos do Lightsail for Research, escolha Uso no painel de navegação.



Etapa 7: (opcional) criar uma regra de controle de custos

Gerencie o uso e o custo de seus computadores virtuais criando regras de controle de custos. Você pode criar uma regra de Parar computador virtual em inatividade que interrompe um computador em execução quando ele atinge uma porcentagem especificada de sua CPU utilização durante um determinado período. Por exemplo, uma regra pode parar automaticamente um computador específico quando sua CPU utilização for igual ou inferior a 5% durante um período de 30 minutos. Isso pode significar que o computador está ocioso e o Lightsail for Research interrompe o computador para que você não incorra em cobranças por um recurso ocioso.

> **Important**
>
> Antes de criar uma regra para parar o computador virtual de ficar ocioso, recomendamos monitorar sua CPU utilização por alguns dias. Anote a CPU utilização enquanto seu computador virtual está sob cargas diferentes. Por exemplo, quando estiver compilando

código, processando uma operação e ficando ocioso. Isso ajudará você a determinar um limite preciso para a regra. Para obter mais informações, consulte a seção Etapa 6: (opcional) monitorar o uso e os custos deste tutorial.
Se você criar uma regra com um limite de CPU utilização maior do que sua carga de trabalho, a regra poderá interromper consecutivamente seu computador virtual. Por exemplo, se você iniciar o computador virtual imediatamente após a interrupção de uma regra, a regra será reativada e o computador será interrompido novamente.

Instruções detalhadas para criar e gerenciar regras de controle de custos podem ser encontradas nos guias a seguir:

- Gerencie as regras de controle de custos no Lightsail for Research
- Crie regras de controle de custos para seus computadores virtuais do Lightsail for Research
- Exclua regras de controle de custos para seus computadores virtuais do Lightsail for Research

Etapa 8: (opcional) criar um snapshot

Os instantâneos são uma point-in-time cópia dos seus dados. Você pode criar snapshots dos seus computadores virtuais e utilizá-los como bases para criar novos computadores ou para backup de dados. Um snapshot contém todos os dados necessários para restaurar o computador (a partir do momento em que o snapshot foi criado).

Instruções detalhadas para criar e gerenciar snapshots podem ser encontradas nos seguintes guias:

- Crie instantâneos dos computadores ou discos virtuais do Lightsail for Research
- Visualize e gerencie instantâneos de disco e computadores virtuais no Lightsail for Research
- Crie um computador ou disco virtual a partir de um snapshot
- Excluir um instantâneo no console do Lightsail for Research

Etapa 9: (opcional) parar ou excluir seu computador virtual

Após concluir o uso do computador virtual criado para este tutorial, você pode excluí-lo. Isso interrompe a geração de cobranças para o computador virtual, caso você não o necessite mais.

Excluir um computador virtual não deleta os snapshots associados ou discos anexados a ele. Se você criou snapshots e discos, você deve excluí-los manualmente para interromper a geração de cobranças relacionadas a eles.

Para salvar o seu computador virtual para uso posterior, mas evitando incorrer em cobranças com preços padrão por hora, você pode interromper o computador virtual em vez de excluí-lo. Você poderá reiniciá-la mais tarde. Para obter mais informações, consulte Veja os detalhes do computador virtual Lightsail for Research. Para obter mais informações sobre preços, consulte Preços do Lightsail for Research.

> **Important**
>
> Excluir um recurso do Lightsail for Research é uma ação permanente. Não foi possível recuperar o objeto excluído. Se você precisar dos dados posteriormente, crie um snapshot de seu computador virtual antes de excluí-lo. Para obter mais informações, consulte Criar um snapshot.

1. Faça login no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação.
3. Escolha o computador virtual a ser excluído.
4. Escolha Ações e, em seguida, escolha Excluir computador virtual.
5. Digite confirmar no bloco de texto. Em seguida, escolha Excluir computador virtual.

Inicie e use RStudio no Lightsail for Research

Neste tutorial, mostramos como começar a gerenciar e usar seu computador RStudio virtual no Amazon Lightsail for Research.

> **Note**
>
> Um tutorial detalhado para começar a usar o Lightsail for Research, publicado no Public RStudio Sector Blog. AWS Para obter mais informações, consulte Introdução ao Amazon Lightsail for Research: um tutorial usando. RStudio

Tópicos

Etapa 1: Concluir os pré-requisitos

Crie um computador virtual usando o RStudio aplicativo, caso ainda não tenha feito isso. Para obter mais informações, consulte Crie um computador virtual Lightsail for Research.

Etapa 2: (opcional) adicionar espaço de armazenamento

Seu computador virtual vem com um disco do sistema. No entanto, à medida que suas necessidades de armazenamento mudam, você pode anexar discos adicionais ao seu computador virtual para aumentar o espaço de armazenamento.

Você também pode armazenar seus arquivos de trabalho em um disco conectado. Em seguida, você pode desconectar o disco e conectá-lo a um computador virtual diferente para mover rapidamente seus arquivos de um computador para outro.

Como alternativa, você pode criar um snapshot de um disco anexado que tenha seus arquivos de trabalho e depois criar um disco duplicado a partir do snapshot. Em seguida, você pode conectar o novo disco duplicado a outro computador para duplicar seu trabalho em diferentes computadores virtuais. Para ter mais informações, consulte Crie um disco de armazenamento no console do Lightsail for Research e Adicione armazenamento a um computador virtual no Lightsail for Research.

> **Note**
>
> Quando você conecta um disco ao seu computador virtual usando o console, o Lightsail for Research formata e monta automaticamente o disco. Esse processo leva alguns minutos,

portanto, você deve confirmar que o disco atingiu o status de Montagem antes de começar a usá-lo. Por padrão, o Lightsail for Research monta discos no `<disk-name>` diretório com `/home/lightsail-user/<disk-name>` o nome que você deu ao disco.

Etapa 3: transferir e baixar arquivos

Você pode fazer upload de arquivos para o seu computador RStudio virtual e baixar arquivos dele. Para fazer isso, você deve executar as etapas a seguir:

1. Obtenha um par de chaves do Amazon Lightsail. Para obter mais informações, consulte Obtenha um par de chaves para um computador virtual Lightsail for Research.
2. Depois de ter o par de chaves, você pode usá-lo para estabelecer uma conexão usando o utilitário Secure Copy (SCP). SCPpermite fazer upload e download de arquivos usando o prompt de comando ou o terminal. Para obter mais informações, consulte Transfira arquivos para computadores virtuais do Lightsail for Research usando o Secure Copy.
3. (Opcional) Você também pode usar o key pair para se conectar ao seu computador virtual comSSH. Para obter mais informações, consulte Conecte-se a um computador virtual Lightsail for Research usando o Secure Shell.

> **Note**
>
> Você também pode acessar a interface de linha de comando do seu computador virtual e transferir arquivos usando o cliente baseado em navegador NICEDCV. NICEDCVestá disponível no console do Lightsail for Research. Para ter mais informações, consulte Acesse um aplicativo de computador virtual Lightsail for Research e Acesse o sistema operacional do seu computador virtual Lightsail for Research.

Etapa 4: iniciar o RStudio aplicativo

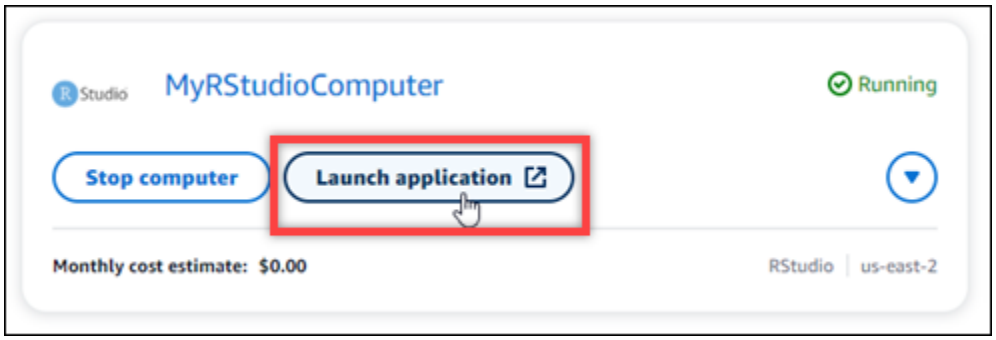
Conclua o procedimento a seguir para iniciar o RStudio aplicativo em seu novo computador virtual.

> **Important**
>
> Não atualize o sistema operacional nem o RStudio aplicativo, mesmo que você seja solicitado a fazer isso. Em vez disso, escolha a opção de fechar ou ignorar essas

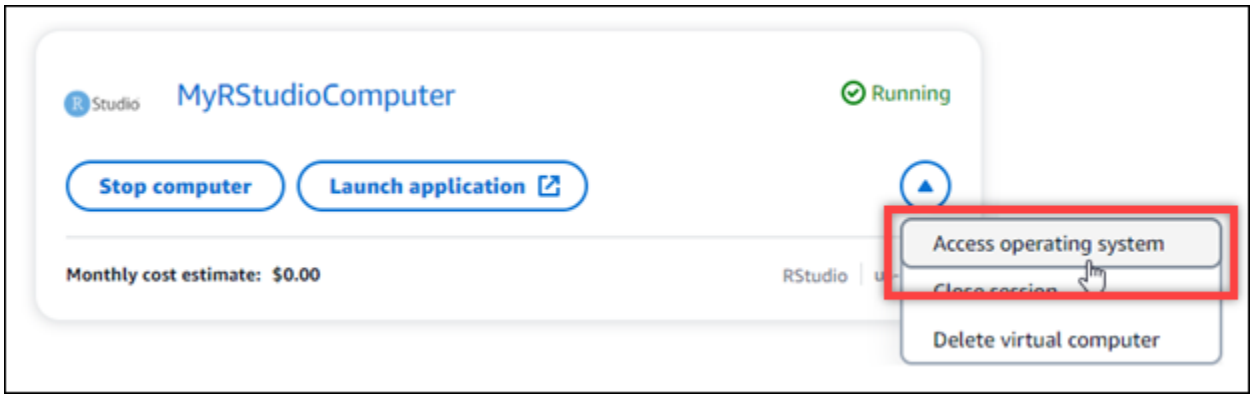
solicitações. Além disso, não modifique nenhum dos arquivos que estão no diretório /home/lightsail-admin/. Essas ações podem tornar o computador virtual inutilizável.

1. Faça login no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação para ver uma lista de computadores virtuais disponíveis em sua conta.
3. Na página Computadores virtuais, encontre seu computador virtual e escolha uma das seguintes opções para se conectar a ele:

   a. (Recomendado) Escolha Iniciar aplicativo para iniciar o RStudio aplicativo no modo focado. Se você não se conectou ao seu computador virtual recentemente, talvez precise esperar alguns minutos enquanto o Lightsail for Research prepara sua sessão.



   b. Escolha o menu suspenso do computador e, em seguida, escolha Acessar sistema operacional para acessar a área de trabalho do seu computador virtual. Faça isso se quiser instalar um aplicativo diferente no sistema operacional.

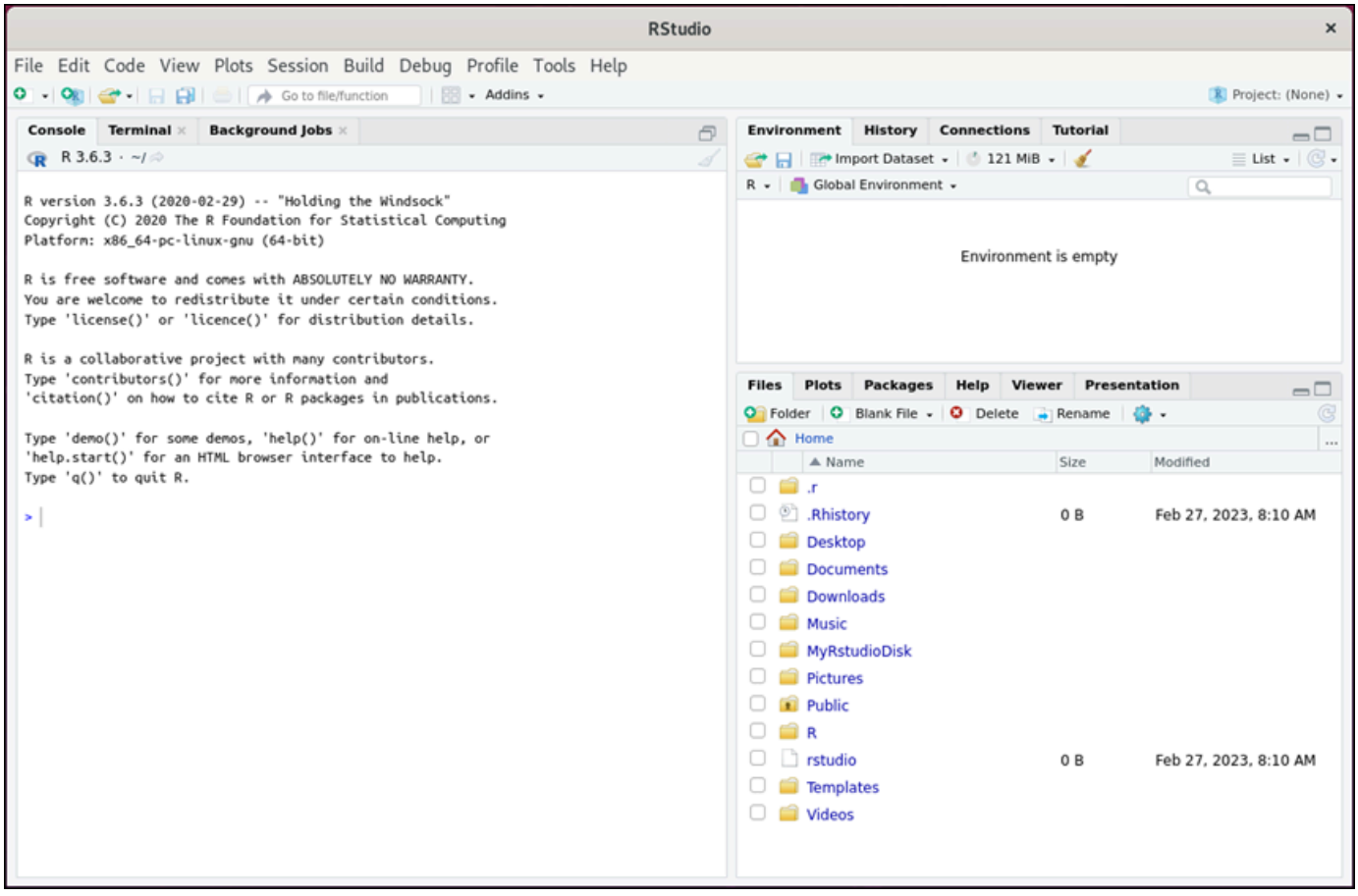


O Lightsail for Research executa alguns comandos para iniciar a conexão do protocolo de exibição remota. Depois de alguns instantes, uma nova janela da guia do navegador é aberta com uma conexão de área de trabalho virtual estabelecida com seu computador virtual. Se você

escolheu a opção Iniciar aplicativo, vá para a próxima etapa desse procedimento para abrir um arquivo no RStudio aplicativo. Se você escolher a opção Acessar sistema operacional, poderá abrir outros aplicativos por meio da área de trabalho do Ubuntu.

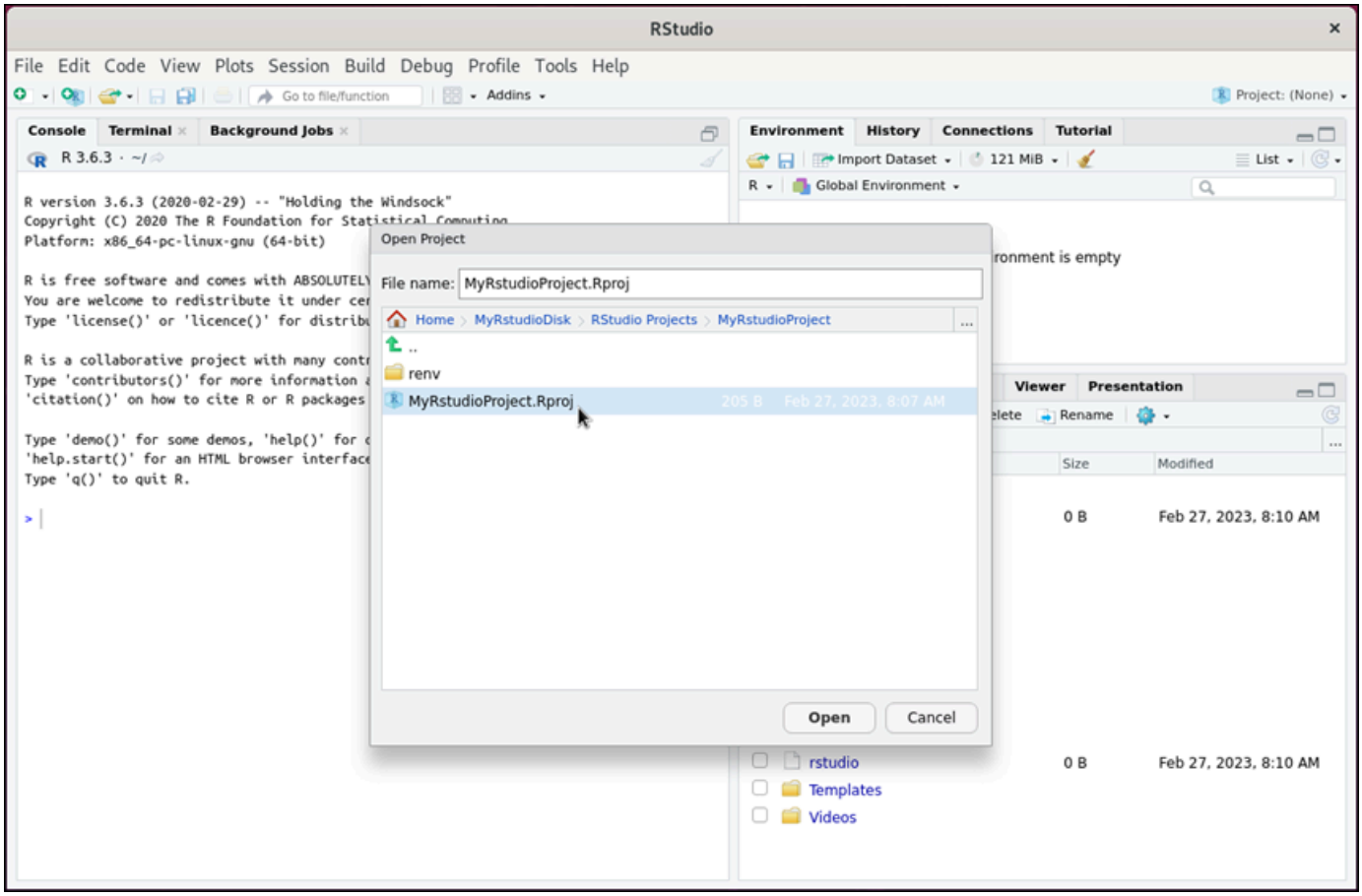
> **Note**
>
> Seu navegador pode solicitar que você autorize o compartilhamento da sua área de transferência. Permitir isso permite copiar e colar entre o computador local e o computador virtual.
>
> O Ubuntu também pode solicitar uma configuração inicial. Siga as instruções até concluir a configuração e poder usar o sistema operacional.

4. O RStudio aplicativo é aberto.

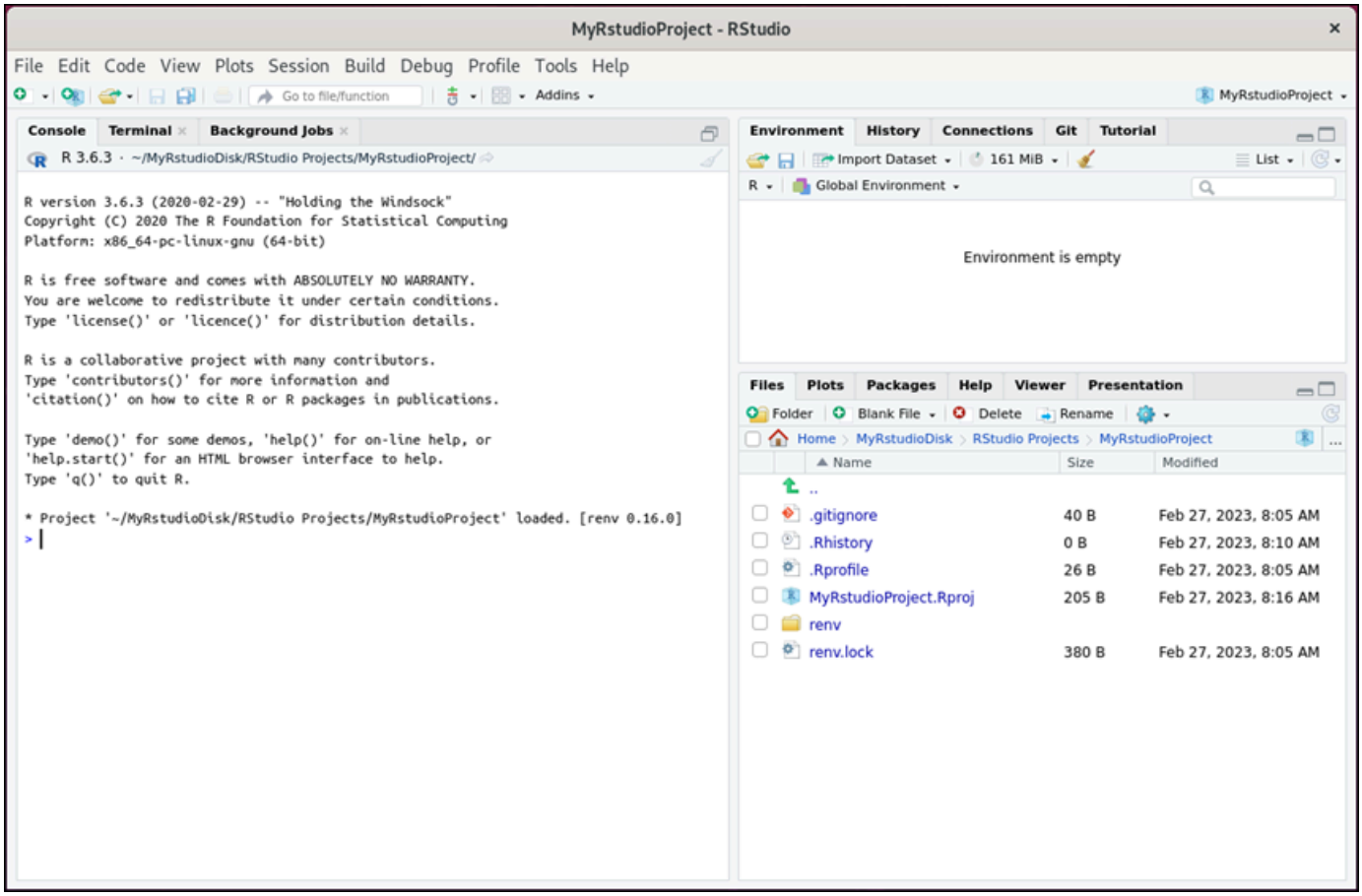


5. Para abrir um projeto emRStudio, escolha o menu Arquivo e, em seguida, escolha Abrir projeto. Navegue até o diretório ou a pasta em que os arquivos do projeto estão armazenados. Em seguida, escolha o arquivo para abrir.

Se você fez upload dos arquivos do projeto em um disco conectado, procure o diretório em que o disco está montado. Por padrão, o Lightsail for Research monta discos no diretório. `/home/lightsail-user/<disk-name>` `<disk-name>`é o nome que você deu ao seu disco. No exemplo a seguir, o `MyRstudioDisk` diretório representa o disco montado e o `Projects` subdiretório contém nossos arquivos de RStudio projeto.



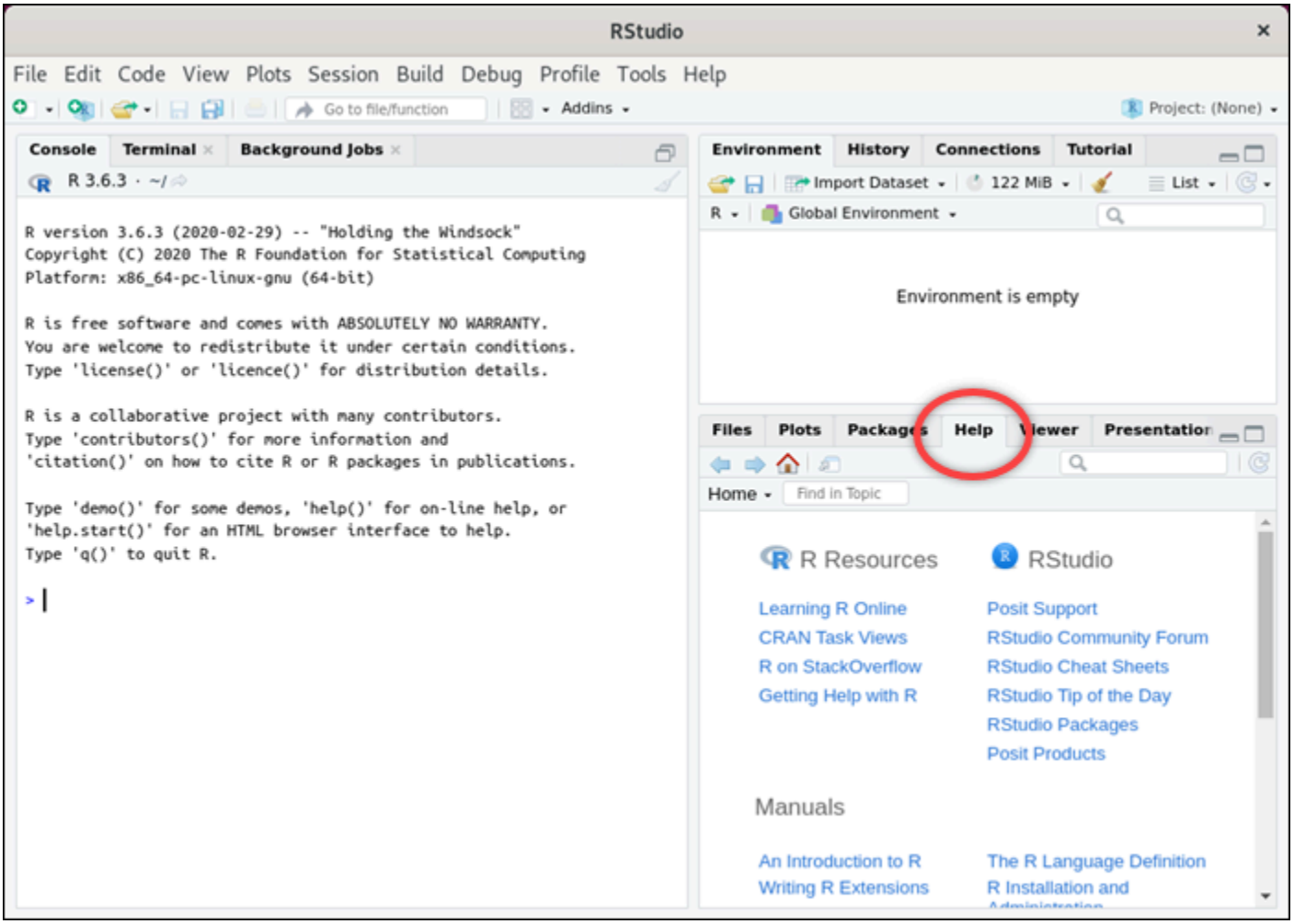
No exemplo a seguir, abrimos o arquivo `MyRstudioProject.Rproj` do projeto.



Para obter informações sobre como começarRStudio, continue até a [Etapa 5: leia a RStudio documentação](#) seção deste tutorial.

Etapa 5: leia a RStudio documentação

O RStudio aplicativo vem com um pacote de documentação abrangente. Para começar a aprenderRStudio, recomendamos que você acesse a guia Ajuda RStudio conforme mostrado no exemplo a seguir.



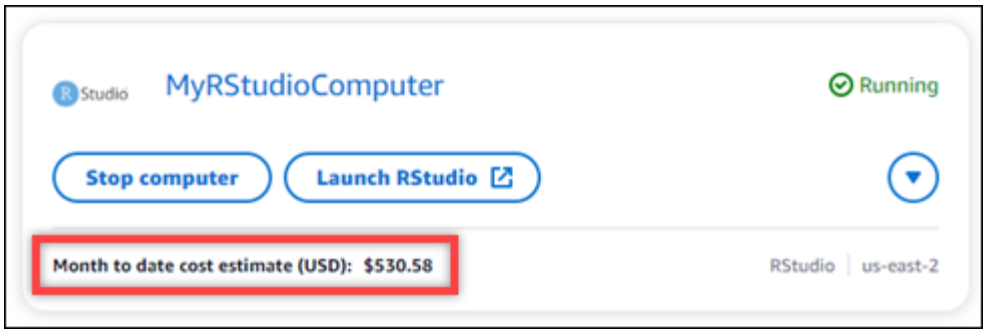
Os seguintes recursos RStudio on-line também estão disponíveis:

- Aprendendo R online
- R em StackOverflow
- Receber ajuda com R
- Suporte Posit
- RStudioFórum da comunidade
- RStudioFolhas de dicas
- RStudioDica do dia (Twitter)
- RStudioPacotes

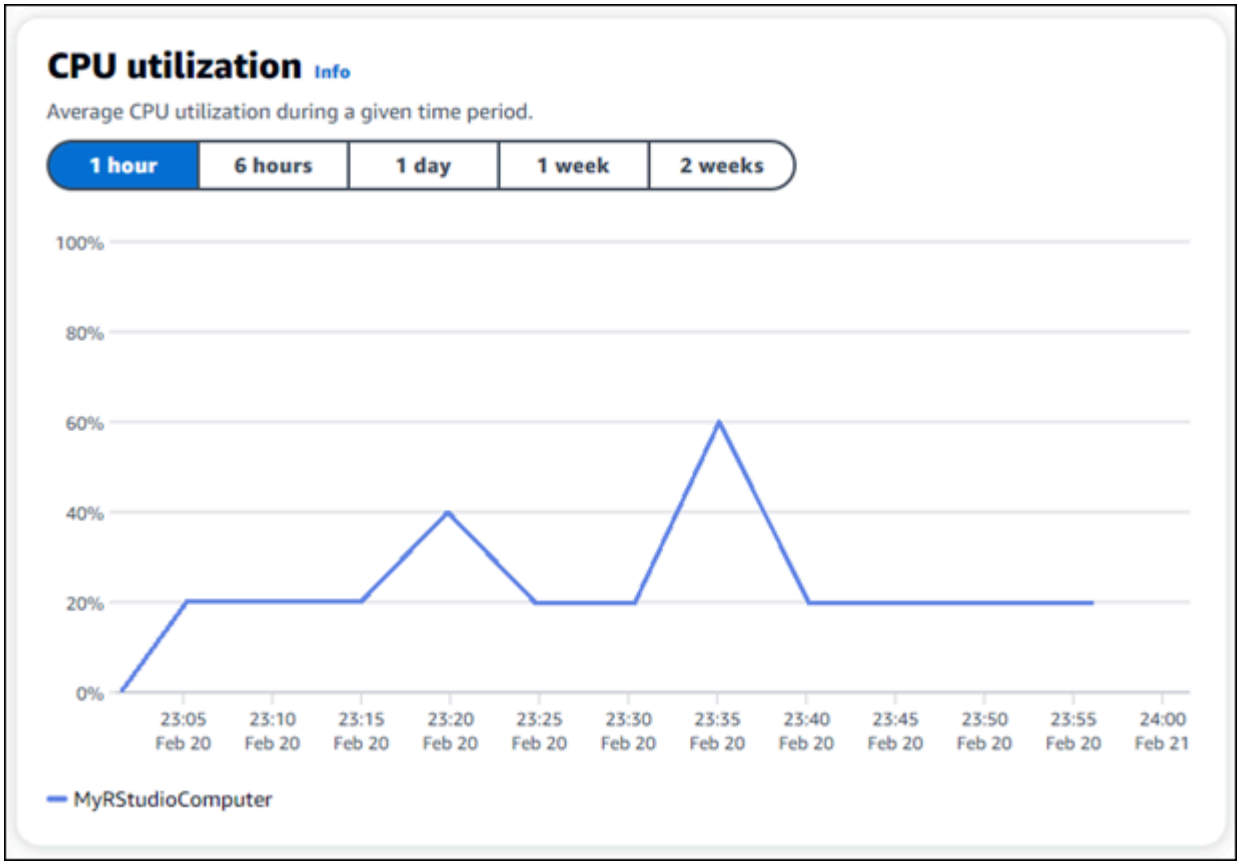
Etapa 6: (opcional) monitorar o uso e os custos

As estimativas mensais de custo e uso de seus recursos do Lightsail for Research são exibidas nas seguintes áreas do console do Lightsail for Research.

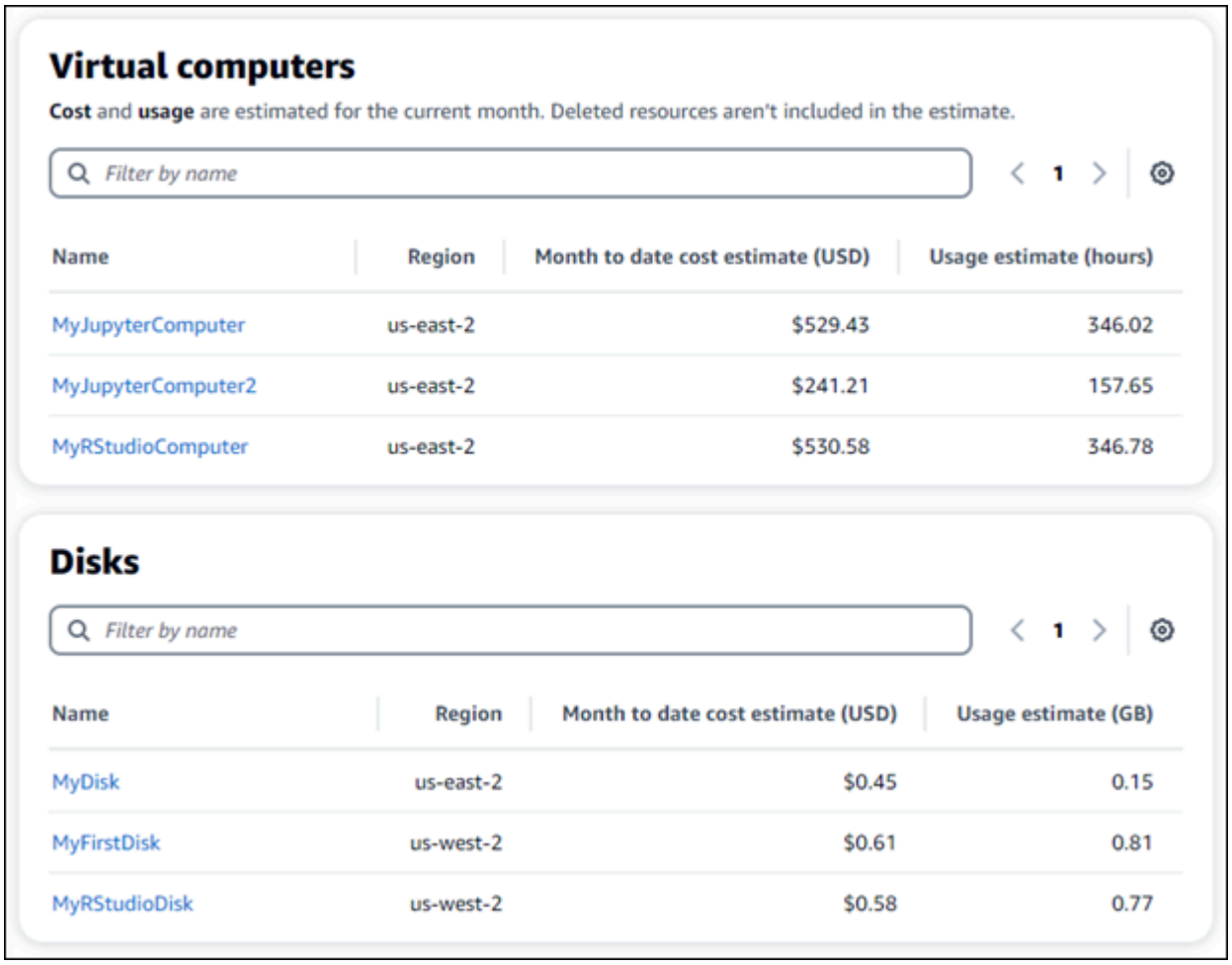
1. Escolha Computadores virtuais no painel de navegação do console do Lightsail for Research. A estimativa de custo mensal para seus computadores virtuais está listada em cada computador virtual em execução.



2. Para ver a CPU utilização de um computador virtual, escolha o nome do computador virtual e, em seguida, escolha a guia Painel.



3. Para ver as estimativas de custo e uso do mês para todos os seus recursos do Lightsail for Research, escolha Uso no painel de navegação.



Etapa 7: (opcional) criar uma regra de controle de custos

Gerencie o uso e o custo de seus computadores virtuais criando regras de controle de custos. Você pode criar uma regra de Parar computador virtual em inatividade que interrompe um computador em execução quando ele atinge uma porcentagem especificada de sua CPU utilização durante um determinado período. Por exemplo, uma regra pode parar automaticamente um computador específico quando sua CPU utilização for igual ou inferior a 5% durante um período de 30 minutos. Isso pode significar que o computador está ocioso e o Lightsail for Research interrompe o computador para que você não incorra em cobranças por um recurso ocioso.

> **Important**
>
> Antes de criar uma regra para parar o computador virtual de ficar ocioso, recomendamos monitorar sua CPU utilização por alguns dias. Anote a CPU utilização enquanto seu computador virtual está sob cargas diferentes. Por exemplo, quando estiver compilando código, processando uma operação e ficando ocioso. Isso ajudará você a determinar um limite preciso para a regra. Para obter mais informações, consulte a seção Etapa 6: (opcional) monitorar o uso e os custos deste tutorial.
>
> Se você criar uma regra com um limite de CPU utilização maior do que sua carga de trabalho, a regra poderá interromper consecutivamente seu computador virtual. Por exemplo, se você iniciar o computador virtual imediatamente após a interrupção de uma regra, a regra será reativada e o computador será interrompido novamente.

Instruções detalhadas para criar e gerenciar regras de controle de custos podem ser encontradas nos guias a seguir:

- Gerencie as regras de controle de custos no Lightsail for Research
- Crie regras de controle de custos para seus computadores virtuais do Lightsail for Research
- Exclua regras de controle de custos para seus computadores virtuais do Lightsail for Research

Etapa 8: (opcional) criar um snapshot

Os instantâneos são uma point-in-time cópia dos seus dados. Você pode criar snapshots dos seus computadores virtuais e utilizá-los como bases para criar novos computadores ou para backup de dados. Um snapshot contém todos os dados necessários para restaurar o computador (a partir do momento em que o snapshot foi criado).

Instruções detalhadas para criar e gerenciar snapshots podem ser encontradas nos seguintes guias:

- Crie instantâneos dos computadores ou discos virtuais do Lightsail for Research
- Visualize e gerencie instantâneos de disco e computadores virtuais no Lightsail for Research
- Crie um computador ou disco virtual a partir de um snapshot
- Excluir um instantâneo no console do Lightsail for Research

Etapa 9: (opcional) parar ou excluir seu computador virtual

Após concluir o uso do computador virtual criado para este tutorial, você pode excluí-lo. Isso interrompe a geração de cobranças para o computador virtual, caso você não o necessite mais.

Excluir um computador virtual não deleta os snapshots associados ou discos anexados a ele. Se você criou snapshots e discos, você deve excluí-los manualmente para interromper a geração de cobranças relacionadas a eles.

Para salvar o seu computador virtual para uso posterior, mas evitando incorrer em cobranças com preços padrão por hora, você pode interromper o computador virtual em vez de excluí-lo. Você poderá reiniciá-la mais tarde. Para obter mais informações, consulte Veja os detalhes do computador virtual Lightsail for Research. Para obter mais informações sobre preços, consulte Preços do Lightsail for Research.

> **Important**
>
> Excluir um recurso do Lightsail for Research é uma ação permanente. Não foi possível recuperar o objeto excluído. Se você precisar dos dados posteriormente, crie um snapshot de seu computador virtual antes de excluí-lo. Para obter mais informações, consulte Criar um snapshot.

1. Faça login no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação.
3. Escolha o computador virtual a ser excluído.
4. Escolha Ações e, em seguida, escolha Excluir computador virtual.
5. Digite confirmar no bloco de texto. Em seguida, escolha Excluir computador virtual.

Crie e gerencie computadores virtuais no Lightsail for Research

Com o Amazon Lightsail for Research, você pode criar computadores virtuais no. Nuvem AWS

Ao criar um computador virtual, você escolhe uma aplicação e um plano de hardware para usar. Você pode definir um limite de gastos para seu computador virtual e escolher o que acontece quando o computador virtual atinge esse limite. Por exemplo, você pode optar por interromper automaticamente o computador virtual para que não seja cobrado mais do que o orçamento estipuiado.

> **Important**
>
> A partir de 22 de março de 2024, os computadores virtuais do Lightsail for Research serão IMDSv2 aplicados por padrão.

Tópicos

Escolha imagens de aplicativos e planos de hardware para o Lightsail for Research

Ao criar um computador virtual Amazon Lightsail for Research, você seleciona um aplicativo e um plano de hardware (plano) para ele.

Uma aplicação fornece uma configuração de software (por exemplo, um aplicativo e um sistema operacional). Um plano fornece o hardware do computador virtual, como o número, a memóriavCPUs, o espaço de armazenamento e o subsídio mensal de transferência de dados. Juntos, a aplicação e o plano compõem a configuração do computador virtual.

> **Note**
>
> Não é possível alterar a aplicação ou plano do computador virtual depois que ela é criada. No entanto, você pode criar um instantâneo do computador virtual e, em seguida, escolher um novo plano ao criar um novo computador virtual a partir do instantâneo. Para obter mais informações sobre snapshots, consulte Faça backup de computadores e discos virtuais com instantâneos do Lightsail for Research.

Tópicos

Aplicações

O Amazon Lightsail for Research fornece e gerencia imagens de máquinas que contêm o aplicativo e o sistema operacional necessários para iniciar um computador virtual. Você escolhe em uma lista de aplicativos ao criar um computador virtual no Lightsail for Research. Todas as imagens do aplicativo Lightsail for Research usam o sistema operacional Ubuntu (Linux).

Os seguintes aplicativos estão disponíveis no Lightsail for Research:

- JupyterLab— JupyterLab é um Ambiente de Desenvolvimento Integrado (IDE) baseado na Web para notebooks, códigos e dados. Com sua interface flexível, você pode configurar e organizar fluxos de trabalho em ciência de dados, computação científica, jornalismo computacional e machine learning. Para obter mais informações, consulte a Documentação do projeto Jupyter.

- RStudio— RStudio é um Ambiente de Desenvolvimento Integrado (IDE) de código aberto para R, uma linguagem de programação para computação estatística e gráficos, e Python. Combina um editor de código-fonte, ferramentas de automação de construção e um depurador, além de ferramentas para plotagem e gerenciamento de espaço de trabalho. Para obter mais informações, consulte RStudioIDEo.
- VSCodium— VSCodium é uma distribuição binária orientada pela comunidade do editor VS Code da Microsoft. Para obter mais informações, consulte VSCodium.
- Scilab — Scilab é um pacote computacional numérico de código aberto e uma linguagem de programação de alto nível orientada numericamente. Para obter mais informações, consulte Scilab.
- Ubuntu 20.04 LTS — Ubuntu é uma distribuição Linux de código aberto baseada no Debian. Simples, rápido e poderoso, o Ubuntu Server oferece serviços de forma confiável, previsível e econômica. É uma excelente base para construir seus computadores virtuais. Para obter mais informações, consulte Releases Ubunty.

Planos

Um plano fornece as especificações de hardware e determina o preço do seu computador virtual Lightsail for Research. Um plano inclui uma quantidade fixa de memória (RAM), computação (vCPUs), espaço de volume de armazenamento (disco) SSD baseado e um subsídio mensal de transferência de dados. Os planos são cobrados por hora, sob demanda, então você paga apenas pelo tempo em que seu computador virtual está funcionando.

O plano escolhido pode depender dos recursos necessários para sua workload. O Lightsail for Research oferece os seguintes tipos de planos:

- Padrão - Os planos padrão são otimizados para computação e são ideais para aplicações dependentes de computação que se beneficiam de processadores de alto desempenho.
- GPU— GPU os planos fornecem uma plataforma econômica e de alto desempenho para computação de uso GPU geral. Você pode usar esses planos para acelerar aplicações e workloads científicas, de engenharia e renderização.

Planos padrão

A seguir estão as especificações de hardware dos planos padrão disponíveis no Lightsail for Research.

Nome do plano	vCPUs	Memória	Espaço de armazenamento	Subsídio mensal para transferência de dados
XL padrão	4	8 GB	50 GB	512 GB
Padrão 2XL	8	16 GB	50 GB	512 GB
Padrão 4XL	16	32 GB	50 GB	512 GB

GPUplanos

A seguir estão as especificações de hardware dos GPU planos disponíveis no Lightsail for Research.

Nome do plano	vCPUs	Memória	Espaço de armazenamento	Subsídio mensal para transferência de dados
GPUXL	4	16 GB	50 GB	1 TB
GPU2XL	8	32 GB	50 GB	1 TB
GPU4XL	16	64 GB	50 GB	1 TB

Crie um computador virtual Lightsail for Research

Conclua as etapas a seguir para criar um computador virtual Lightsail for Research executando um aplicativo.

1. Faça login no console do Lightsail for Research.
2. Na página inicial, escolha Criar computador virtual.
3. Selecione um Região da AWS para o seu computador virtual que esteja próximo à sua localização física.
4. Escolha um plano de aplicação e hardware. Para obter mais informações, consulte Escolha imagens de aplicativos e planos de hardware para o Lightsail for Research.

5. Insira um nome para o computador virtual. Caracteres válidos incluem caracteres alfanuméricos, números, pontos, hífens e sublinhados.

   Os nomes de computadores virtuais também devem atender aos seguintes requisitos:

   - Seja único Região da AWS em cada um em sua conta do Lightsail for Research.
   - Contêm de 2 a 255 caracteres.
   - Comece e termine com um caractere alfanumérico ou com um número.
6. Escolha Criar computador virtual no painel Resumo.

Em minutos, seu computador virtual Lightsail for Research está pronto e você pode se conectar a ele por meio de uma sessão de interface GUI gráfica de usuário (). Para obter mais informações sobre como se conectar ao seu computador virtual Lightsail for Research, consulte. Acesse um aplicativo de computador virtual Lightsail for Research

> **Important**
>
> Os computadores virtuais recém-criados têm um conjunto de portas de firewall abertas por padrão. Para obter mais informações sobre essas portas, consulte Gerencie portas de firewall para computadores virtuais do Lightsail for Research.

Veja os detalhes do computador virtual Lightsail for Research

Conclua as etapas a seguir para ver uma lista de computadores virtuais e seus detalhes em sua conta do Lightsail for Research.

1. Faça login no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação para ver uma lista de computadores virtuais em sua conta.

Escolha o nome de um computador virtual para navegar até a página de gerenciamento. A seguir estão as informações que a página de gerenciamento fornece:

- Nome do computador virtual — O nome do seu computador virtual.
- Status — Seu computador virtual pode ter um dos seguintes códigos de status:
  - Criando

  - Executando
  - Parando
  - Interrompido
  - Desconhecido
- Região da AWS— O Região da AWS seu computador virtual foi criado em.
- Aplicação e hardware — O plano de aplicação e hardware do computador virtual.
- Estimativa de uso mensal — O uso horário estimado para esse computador virtual, para o ciclo de cobrança atual.
- Estimativa de custo acumulada no mês — O custo estimado (emUSD) para o computador virtual, para esse ciclo de cobrança.
- Painel — Na guia Painel, você pode iniciar uma sessão para acessar a aplicação do computador virtual. Você também pode ver a CPU utilização. CPUa utilização identifica a capacidade de processamento usada pelos aplicativos do computador virtual. Cada ponto de dados mostrado no gráfico representa a CPU utilização média em um período de tempo.
- Regras de controle de custos - Regras que você define para ajudar a gerenciar o uso e o custo de seus computador virtual.
- Uso do computador virtual — Uma estimativa de custo e uso para um determinado ciclo de cobrança. Você pode filtrar isso por data e hora.
- Armazenamento — Crie, anexe e desanexe discos de computador virtual na guia Armazenamento. Um disco é um volume de armazenamento que você pode conectar a um computador virtual e montar como um disco rígido.
- Tags — Gerencie as tags do seu computador virtual na guia Tags. Uma tag é um rótulo que você atribui a um AWS recurso. Cada tag consiste em uma chave e um valor opcional. Você pode usar tags para pesquisar e filtrar seus recursos ou monitorar seus AWS custos.

Acesse um aplicativo de computador virtual Lightsail for Research

Conclua as etapas a seguir para iniciar o aplicativo que está sendo executado no seu computador virtual Lightsail for Research.

1. Faça login no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação.
3. Localize o nome do computador virtual do qual você deseja iniciar a aplicação.

> **Note**
>
> Se o computador virtual estiver parado, primeiro escolha o botão Iniciar computador para ligá-lo.

4. Escolha Iniciar aplicação. Por exemplo, Launch JupyterLab. Uma sessão da aplicação será aberta em uma nova janela do navegador da web.

> **Important**
>
> Se o seu navegador da web tiver um bloqueador de pop-ups instalado, talvez seja necessário permitir pop-ups do domínio aws.amazon.com antes de abrir sua sessão.

Acesse o sistema operacional do seu computador virtual Lightsail for Research

Conclua as etapas a seguir para acessar o sistema operacional do seu computador virtual Lightsail for Research.

1. Faça login no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação.
3. Localize o nome do seu computador virtual e escolha o menu suspenso do botão de ações abaixo do status do computador.

> **Note**
>
> Se o computador virtual estiver parado, primeiro escolha o botão Iniciar para ligá-lo.

4. Escolha Access operating system (Acessar o sistema operacional). Uma sessão do sistema operacional será aberta em uma nova janela do navegador.

> **Important**
>
> Se o seu navegador da web tiver um bloqueador de pop-ups instalado, talvez seja necessário permitir pop-ups do domínio aws.amazon.com antes para abrir sua sessão.

Gerencie portas de firewall para computadores virtuais do Lightsail for Research

Um firewall no Amazon Lightsail for Research controla o tráfego permitido para se conectar ao seu computador virtual. Você adiciona regras ao firewall do seu computador virtual que especificam o protocolo, as portas e a origem IPv4 ou os IPv6 endereços que podem se conectar a ele. As regras do firewall sempre são permissivas. Não é possível regras que neguem o acesso. Você adiciona regras ao firewall do seu computador virtual para permitir que o tráfego chegue ao seu computador virtual. Cada computador virtual tem dois firewalls; um para IPv4 endereços e outro para IPv6 endereços. Ambos os firewalls são independentes entre si e contêm um conjunto preconfigurado de regras que filtram o tráfego que chega à instância.

Protocolos

O protocolo é o formato no qual os dados são transmitidos entre dois computadores. Você pode especificar os seguintes protocolos em uma regra de firewall:

- O Protocolo de Controle de Transmissão (TCP) é usado principalmente para estabelecer e manter uma conexão entre clientes e o aplicativo que está sendo executado no seu computador virtual. É um protocolo amplamente utilizado e que, talvez, você especifique com frequência nas regras de firewall.
- O User Datagram Protocol (UDP) é usado principalmente para estabelecer conexões de baixa latência e tolerância a perdas entre clientes e o aplicativo que está sendo executado em seu computador virtual. É o uso ideal para aplicações de rede em que a latência percebida é crítica, como jogos, voz e comunicações por vídeo.
- O Internet Control Message Protocol (ICMP) é usado principalmente para diagnosticar problemas de comunicação de rede, como para determinar se os dados estão chegando ao destino pretendido em tempo hábil. O uso ideal é para o utilitário Ping, que pode ser usado para testar a

velocidade da conexão entre o computador local e computador virtual. Ele relata quanto tempo os dados levam para alcançar o computador virtual e retornar ao computador local.

- All (Todos) é usado para permitir que todo o tráfego do protocolo flua para o computador virtual. Especifique esse protocolo quando não tiver certeza de qual protocolo especificar. Isso inclui todos os protocolos de internet, não apenas aqueles especificados aqui. Para obter mais informações, consulte Protocol Numbers no site da Autoridade de números atribuídos pela Internet.

Portas

Semelhante às portas físicas no seu computador, que permitem que seu computador se comunique com periféricos como seu teclado e ponteiro, as portas de firewall servem como pontos de comunicação na internet para o seu computador virtual. Quando um cliente tenta se conectar ao computador virtual, ele expõe uma porta para estabelecer a comunicação.

As portas que podem ser especificadas em uma regra de firewall podem variar de 0 a 65535. Ao criar uma regra de firewall para permitir que um cliente estabeleça uma conexão com seu computador virtual, você especifica o protocolo a ser utilizado. Você também especifica os números de porta pelos quais a conexão pode ser estabelecida e os endereços IP que têm permissão para estabelecer a conexão.

As portas a seguir estão abertas por padrão para computadores virtuais recém-criados.

- TCP
  - 22 - Usado para Secure Shell (SSH).
  - 80 - Usado para o Hypertext Transfer Protocol (HTTP).
  - 443 - Usado para Hypertext Transfer Protocol Secure ()HTTPS.
  - 8443 - Usado para o Hypertext Transfer Protocol Secure ()HTTPS.

Por que abrir e fechar portas

Ao abrir portas, você permite que um cliente estabeleça uma conexão com seu computador virtual. Ao fechar portas, você bloqueia as conexões com seu computador virtual. Por exemplo, para permitir que um SSH cliente se conecte ao seu computador virtual, você configura uma regra de firewall que permite a passagem TCP pela porta 22 somente a partir do endereço IP do computador que precisa estabelecer uma conexão. Nesse caso, você não quer permitir que nenhum endereço IP estabeleça uma SSH conexão com seu computador virtual. Fazer isso pode levar a um risco de segurança. Se

essa regra já estiver configurada no firewall da sua instância, você poderá excluí-la para impedir que o SSH cliente se conecte ao seu computador virtual.

Os procedimentos a seguir mostram como obter as portas que estão abertas no momento em seu computador virtual, abrir novas portas e fechar portas.

Tópicos

Conclua os pré-requisitos

Conclua os seguintes pré-requisitos antes de começar.

- Crie um computador virtual no Lightsail for Research. Para obter mais informações, consulte Crie um computador virtual Lightsail for Research.
- Baixe e instale o AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI no AWS Command Line Interface Guia do usuário da Versão 2.
- Configure o AWS CLI para acessar seu Conta da AWS. Para obter mais informações, consulte Conceitos básicos de configuração da no AWS Command Line Interface Guia do usuário da Versão 2.

Obtenha estados de porta para um computador virtual

Realize o procedimento a seguir para obter os estados das portas de um computador virtual. Esse procedimento usa o `get-instance-port-states` AWS CLI comando para obter os estados das portas do firewall para um computador virtual específico do Lightsail for Research, os endereços IP permitidos para se conectar ao computador virtual por meio das portas e o protocolo. Para obter mais informações, consulte get-instance-port-statesna Referência de AWS CLI Comandos.

1. Essa etapa é determinada pelo sistema operacional do computador local.

- Se o computador local usa um sistema operacional Windows, abra uma janela do prompt de comando.
- Se o seu computador local usa um sistema operacional baseado em Linux ou UNIX (incluindo macOS), abra uma janela do Terminal.

2. Insira o comando a seguir para obter os estados da porta do firewall e os endereços IP e protocolos permitidos. No comando, *REGION* substitua pelo código da AWS região na qual o computador virtual foi criado, como `us-east-2`. Substitua *NAME* pelo nome do seu computador virtual.

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

Exemplo

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

A resposta exibirá as portas e protocolos abertos e os CIDR intervalos de IP que podem ser conectados ao seu computador 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 obter informações sobre como abrir portas, vá para a próxima seção.

Portas abertas de um computador virtual

Complete o seguinte procedimento para abrir portas para um computador virtual. Esse procedimento usa o `open-instance-public-ports` AWS CLI comando. Abra portas de firewall para permitir que conexões sejam estabelecidas a partir de um endereço IP confiável ou um intervalo de endereços IP confiável. Por exemplo, para permitir o endereço IP `192.0.2.44`, especifique `192.0.2.44` ou `192.0.2.44/32`. Para permitir os endereços IP `192.0.2.0` a `192.0.2.255`,

especifique `192.0.2.0/24`. Para obter mais informações, consulte open-instance-public-portsna Referência de AWS CLI Comandos.

1. Essa etapa é determinada pelo sistema operacional do computador local.

   - Se o computador local usa um sistema operacional Windows, abra uma janela do prompt de comando.
   - Se o seu computador local usa um sistema operacional baseado em Linux ou UNIX (incluindo macOS), abra uma janela do Terminal.

2. Digite o seguinte comando para abrir portas.

   No comando, substitua os seguintes itens:

   - *REGION*Substitua pelo código da AWS região na qual o computador virtual foi criado, como`us-east-2`.
   - Substitua *NAME* pelo nome do seu computador virtual.
   - Substitua *FROM-PORT* pela primeira porta em um intervalo de portas que você deseja abrir.
   - Substitua *PROTOCOL* pelo nome do protocolo IP. Por exemplo,TCP.
   - Substitua *TO-PORT* pela última porta em um intervalo de portas que você deseja abrir.
   - Substitua *IP* pelo endereço IP ou intervalo de endereços IP que você deseja permitir para se conectar ao seu computador virtual.

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

   Exemplo

   ```
   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
   ```

   A resposta exibirá as portas, protocolos e CIDR intervalos de IP recém-adicionados que podem se conectar ao seu computador virtual.

Para obter informações sobre como fechar portas, vá para a próxima seção.

Fechar as portas de um computador virtual

Complete o seguinte procedimento para fechar portas para um computador virtual. Esse procedimento usa o `close-instance-public-ports` AWS CLI comando. Para obter mais informações, consulte close-instance-public-portsna Referência de AWS CLI Comandos.

1. Essa etapa é determinada pelo sistema operacional do computador local.
   - Se o computador local usa um sistema operacional Windows, abra uma janela do prompt de comando.
   - Se o seu computador local usa um sistema operacional baseado em Linux ou UNIX (incluindo macOS), abra uma janela do Terminal.
2. Insira o seguinte comando para fechar portas.

   No comando, substitua os seguintes itens:

   - *REGION*Substitua pelo código da AWS região na qual o computador virtual foi criado, como`us-east-2`.
   - Substitua *NAME* pelo nome do seu computador virtual.
   - Substitua *FROM-PORT* pela primeira porta em um intervalo de portas que você deseja fechar.
   - Substitua *PROTOCOL* pelo nome do protocolo IP. Por exemplo,TCP.
   - Substitua *TO-PORT* pela última porta em um intervalo de portas que você deseja fechar.
   - Substitua *IP* pelo endereço IP ou vários endereços IP que você quer remover.

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

Exemplo

```
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
```

A resposta exibirá as portas, protocolos e CIDR intervalos de IP que foram fechados e não podem mais se conectar ao seu computador virtual.

Continue para as próximas etapas

Você pode concluir as seguintes etapas adicionais após ter gerenciado com sucesso as portas do firewall para o seu computador virtual:

- Obtenha o par de chaves do seu computador virtual. Com o key pair, você pode estabelecer uma conexão usando vários SSH clientes, como Open SSHTTY, Pu e Windows Subsystem for Linux. Para obter mais informações, consulte Obtenha um par de chaves para um computador virtual Lightsail for Research.
- Conecte-se ao seu computador virtual usando SSH para gerenciá-lo usando a linha de comando. Para obter mais informações, consulte Transfira arquivos para computadores virtuais do Lightsail for Research usando o Secure Copy.

- Conecte-se ao seu computador virtual usando SCP para transferir arquivos com segurança. Para obter mais informações, consulte Transfira arquivos para computadores virtuais do Lightsail for Research usando o Secure Copy.

Obtenha um par de chaves para um computador virtual Lightsail for Research

Um par de chaves, composto por uma chave pública e uma chave privada, é um conjunto de credenciais de segurança que você usa para provar sua identidade ao se conectar a um computador virtual Amazon Lightsail for Research. A chave pública é armazenada em cada computador virtual no Lightsail for Research, e você mantém a chave privada em seu computador local. A chave privada permite que você estabeleça com segurança um protocolo Secure Shell (SSH) com seu computador virtual. Qualquer pessoa que possua a chave privada pode se conectar ao seu computador virtual, portanto, é importante que você armazene sua chave privada em um local seguro.

Um par de chaves padrão do Amazon Lightsail DKP () é criado automaticamente na primeira vez que você cria uma instância do Lightsail ou um computador virtual do Lightsail for Research. DKPÉ específico para cada AWS região na qual você cria uma instância ou computador virtual. Por exemplo, o DKP Lightsail para a região Leste dos EUA (Ohio) (us-east-2) se aplica a todos os computadores que você cria no Leste dos EUA (Ohio) no Lightsail e no Lightsail for Research que foram configurados para usar o quando foram criados. DKP O Lightsail for Research armazena automaticamente a chave pública DKP do nos computadores virtuais que você cria. Você pode baixar a chave privada do a qualquer DKP momento fazendo uma API chamada para o serviço Lightsail.

Neste documento, mostramos como obter o DKP para um computador virtual. Depois de ter oDKP, você pode estabelecer uma conexão usando vários SSH clientes, como Open SSHTTY, Pu e Windows Subsystem for Linux. Você também pode usar Secure Copy (SCP) para transferir arquivos com segurança do computador local para o computador virtual.

> **Note**
>
> Você também pode estabelecer uma conexão de protocolo de exibição remota com seu computador virtual usando o cliente baseado em navegador NICEDCV. NICEDCVestá disponível no console do Lightsail for Research. Esse RDP cliente não exige que você obtenha um par de chaves para o seu computador. Para ter mais informações, consulte

Acesse um aplicativo de computador virtual Lightsail for Research e Acesse o sistema operacional do seu computador virtual Lightsail for Research.

Tópicos

Conclua os pré-requisitos

Conclua os seguintes pré-requisitos antes de começar.

- Crie um computador virtual no Lightsail for Research. Para obter mais informações, consulte Crie um computador virtual Lightsail for Research.
- Baixe e instale o AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI no AWS Command Line Interface Guia do usuário da Versão 2.
- Configure o AWS CLI para acessar seu Conta da AWS. Para obter mais informações, consulte Conceitos básicos de configuração da no AWS Command Line Interface Guia do usuário da Versão 2.
- Faça download e instale o jq. É um JSON processador de linha de comando leve e flexível usado nos procedimentos a seguir para extrair detalhes do par de chaves das JSON saídas do AWS CLI. Para obter mais informações sobre como baixar e instalar o jq, consulte Baixar o jq no site do jq.

Obtenha um key pair para um computador virtual

Conclua um dos procedimentos a seguir para obter o Lightsail para um computador virtual no DKP Lightsail for Research.

Obtenha um key pair para um computador virtual usando um computador local Windows

Esse procedimento se aplica a você se o computador local usa um sistema operacional Windows. Esse procedimento usa o `download-default-key-pair` AWS CLI comando para obter o DKP Lightsail para uma região. AWS Para obter mais informações, consulte download-default-key-pairna Referência de AWS CLI Comandos.

1. Abra a janela Command Prompt (Prompt de comando).
2. Digite o comando a seguir para obter o DKP Lightsail para uma região específica. AWS Esse comando salva as informações em um arquivo `dkp-details.json`. No comando, *`region-code`* substitua pelo código da AWS região na qual o computador virtual foi criado, como `us-east-2`.

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

Exemplo

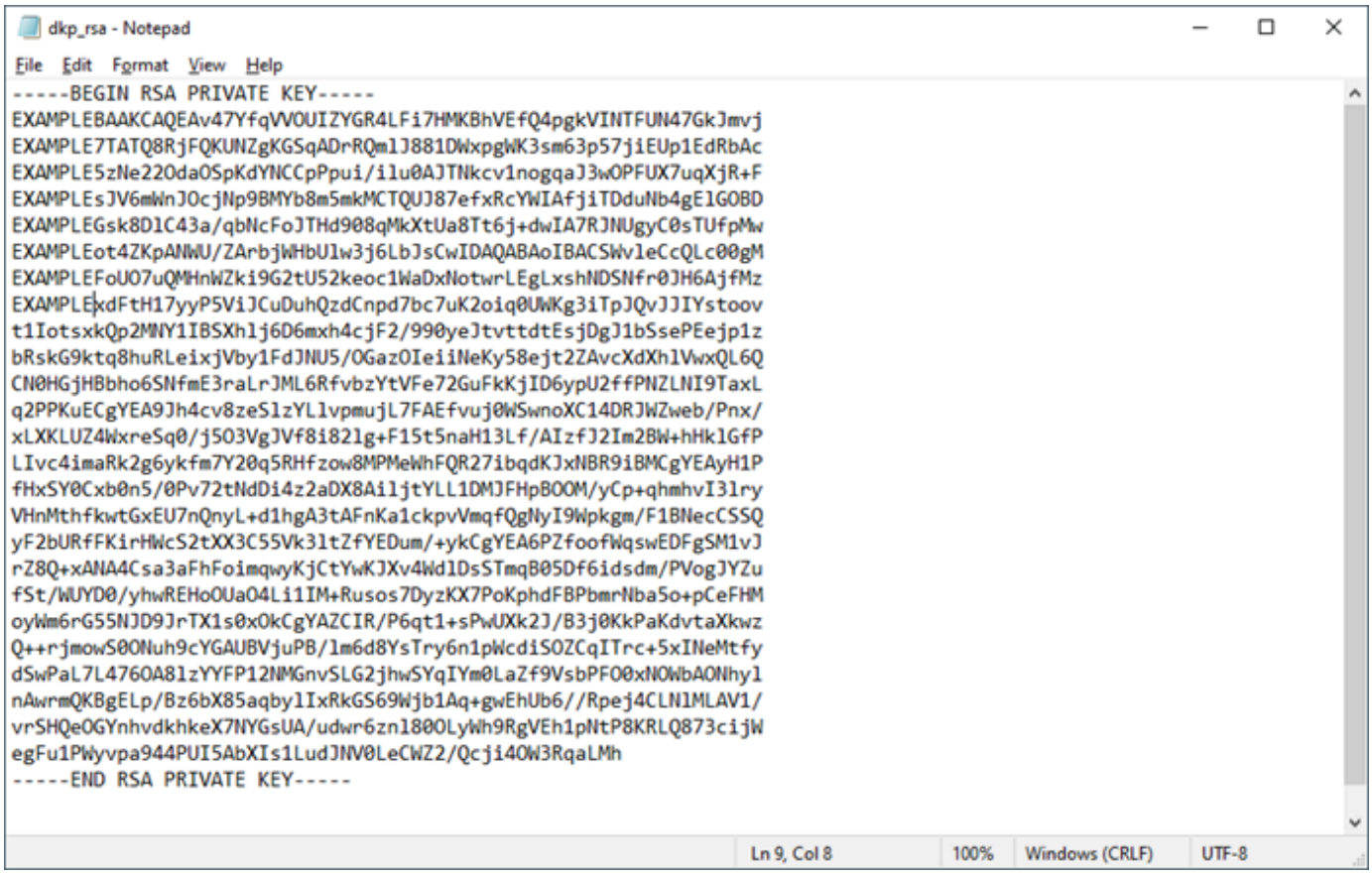
```
aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
```

Não há resposta ao comando. Você pode confirmar se o comando foi bem-sucedido abrindo o `dkp-details.json` arquivo e vendo se as informações do DKP Lightsail foram salvas. O conteúdo do arquivo `dkp-details.json` deve ser semelhante ao seguinte exemplo: O comando falhou se o arquivo estiver em branco.

3. Digite o comando a seguir para extrair as informações da chave privada do `dkp-details.json` arquivo e adicioná-las a um novo arquivo de chave privada `dkp_rsa`.

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

Não há resposta ao comando. Você pode confirmar se o comando foi bem-sucedido abrindo os arquivos `dkp_rsa` e vendo se ele contém informações. O conteúdo do arquivo `dkp_rsa` deve ser semelhante ao seguinte exemplo: O comando falhou se o arquivo estiver em branco.



Agora você tem a chave privada necessária para estabelecer uma SCP conexão SSH ou com seu computador virtual. Continue na próxima seção para ver as próximas etapas adicionais.

Obtenha um par de chaves para um computador virtual usando um computador local com Linux, Unix ou macOS.

Este procedimento se aplica a você se o seu computador local estiver utilizando um sistema operacional Linux, Unix ou macOS. Esse procedimento usa o `download-default-key-pair`

AWS CLI comando para obter o DKP Lightsail para uma região. AWS Para obter mais informações, consulte download-default-key-pairna Referência de AWS CLI Comandos.

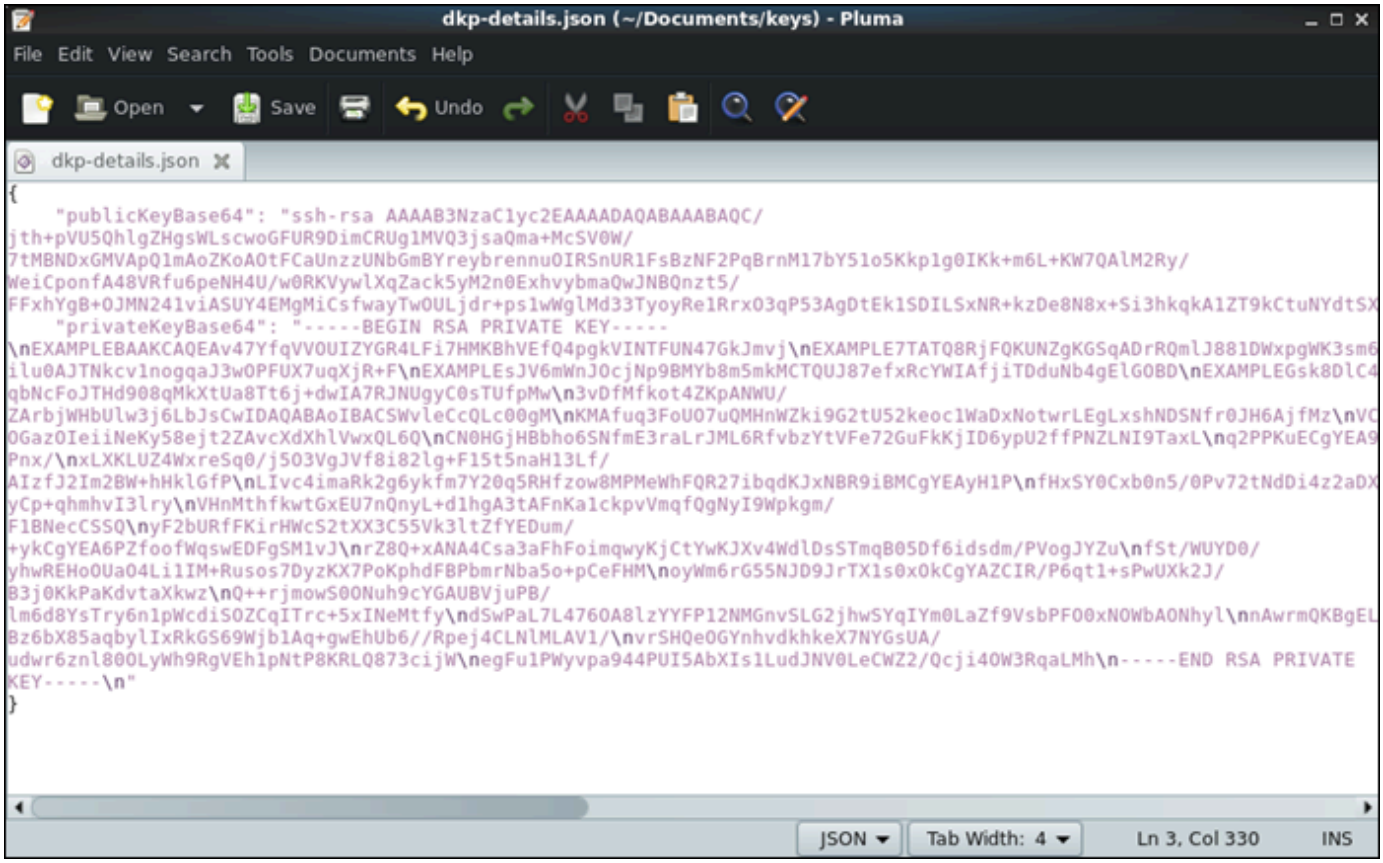
1. Abra uma janela do Terminal.
2. Digite o comando a seguir para obter o DKP Lightsail para uma região específica. AWS Esse comando salva as informações em um arquivo `dkp-details.json`. No comando, *`region-code`* substitua pelo código da AWS região na qual o computador virtual foi criado, como `us-east-2`.

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

   Exemplo

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

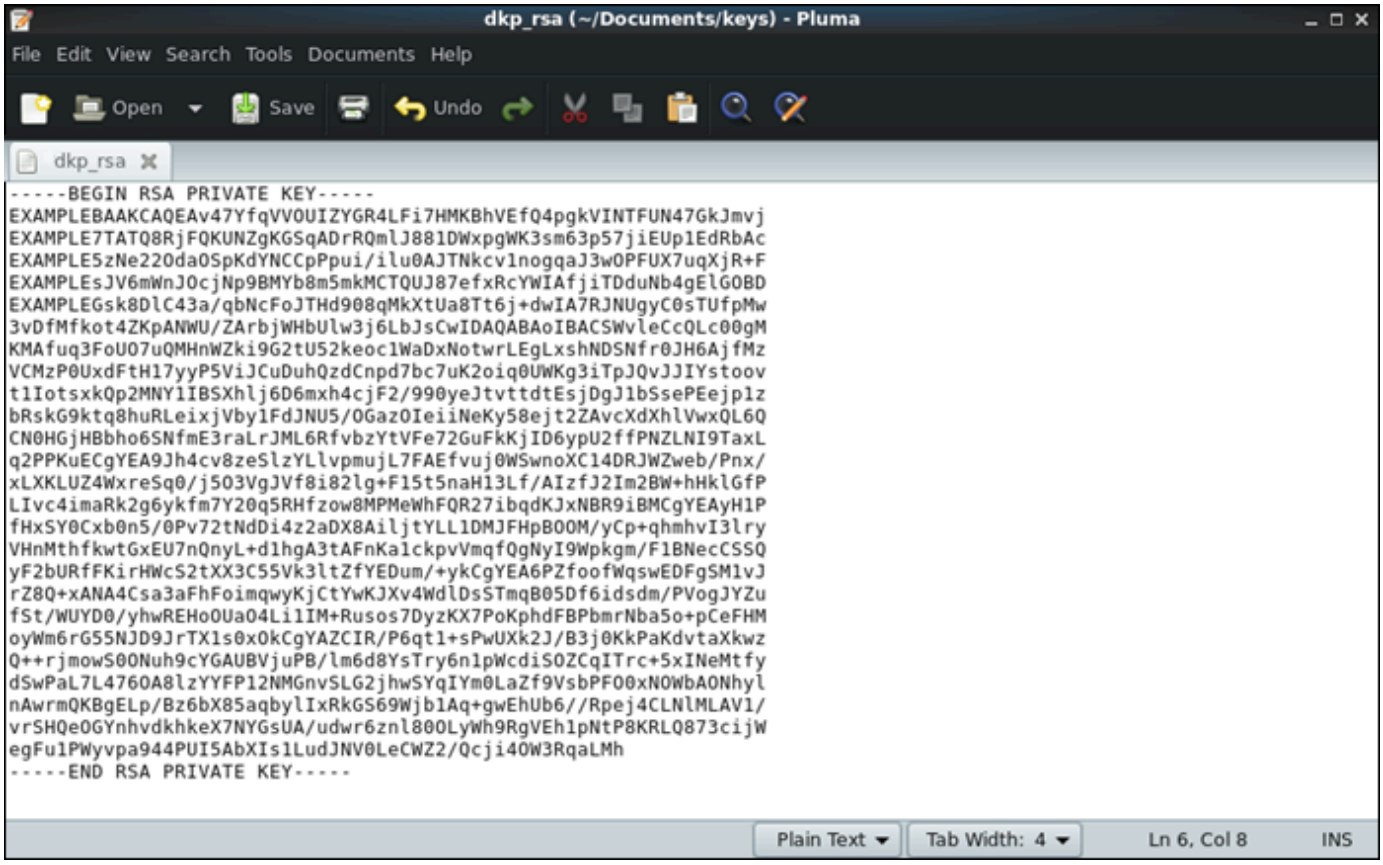
   Não há resposta ao comando. Você pode confirmar se o comando foi bem-sucedido abrindo o `dkp-details.json` arquivo e vendo se as informações do DKP Lightsail foram salvas. O conteúdo do arquivo `dkp-details.json` deve ser semelhante ao seguinte exemplo: O comando falhou se o arquivo estiver em branco.



3. Digite o comando a seguir para extrair as informações da chave privada do `dkp-details.json` arquivo e adicioná-las a um novo arquivo de chave privada `dkp_rsa`.

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

Não há resposta ao comando. Você pode confirmar se o comando foi bem-sucedido abrindo os arquivos `dkp_rsa` e vendo se ele contém informações. O conteúdo do arquivo `dkp_rsa` deve ser semelhante ao seguinte exemplo: O comando falhou se o arquivo estiver em branco.



4. Digite o seguinte comando para definir permissões para o arquivo `dkp_rsa`.

```
chmod 600 dkp_rsa
```

Agora você tem a chave privada necessária para estabelecer uma SCP conexão SSH ou com seu computador virtual. Continue na próxima seção para ver as próximas etapas adicionais.

Continue para as próximas etapas

Você pode concluir as próximas etapas adicionais a seguir depois de obter com êxito os pares de chaves para seu computador virtual:

- Conecte-se ao seu computador virtual usando SSH para gerenciá-lo usando a linha de comando. Para obter mais informações, consulte Conecte-se a um computador virtual Lightsail for Research usando o Secure Shell.
- Conecte-se ao seu computador virtual usando SCP para transferir arquivos com segurança. Para obter mais informações, consulte Transfira arquivos para computadores virtuais do Lightsail for Research usando o Secure Copy.

Conecte-se a um computador virtual Lightsail for Research usando o Secure Shell

Você pode se conectar a um computador virtual no Amazon Lightsail for Research usando o protocolo Secure Shell (). SSH Você pode usar SSH para gerenciar seu computador virtual remotamente para poder entrar no seu computador pela Internet e executar comandos.

> **Note**
>
> Você também pode estabelecer uma conexão de protocolo de exibição remota com seu computador virtual usando o cliente baseado em navegador NICEDCV. NICEDCVestá disponível no console do Lightsail for Research. Para obter mais informações, consulte Acesse o sistema operacional do seu computador virtual Lightsail for Research.

Tópicos

Conclua os pré-requisitos

Conclua os seguintes pré-requisitos antes de começar.

- Crie um computador virtual no Lightsail for Research. Para obter mais informações, consulte Crie um computador virtual Lightsail for Research.
- Verifique se o computador virtual ao qual você deseja se conectar está em execução. Além disso, anote o nome do computador virtual e a AWS região na qual ele foi criado. Você precisará dessas informações posteriormente nesse processo. Para obter mais informações, consulte Veja os detalhes do computador virtual Lightsail for Research.
- Verifique se a porta 22 está aberta no computador virtual ao qual você deseja se conectar. Essa é a porta padrão usada paraSSH. É aberto por padrão Mas se você o fechou, deverá reabri-lo antes de continuar. Para obter mais informações, consulte Gerencie portas de firewall para computadores virtuais do Lightsail for Research.

- Obtenha o par de chaves padrão do Lightsail DKP () para seu computador virtual. Para obter mais informações, consulte Obtenha um key pair para um computador virtual.

> **Tip**
>
> Se você planeja usar AWS CloudShell para se conectar ao seu computador virtual, consulte Conecte-se a um computador virtual usando AWS CloudShell na próxima seção. Para obter mais informações, consulte O que é AWS CloudShell. Caso contrário, continue com o próximo pré-requisito.

- Baixe e instale o AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI no AWS Command Line Interface Guia do usuário da Versão 2.
- Configure o AWS CLI para acessar seu Conta da AWS. Para obter mais informações, consulte Conceitos básicos de configuração da no AWS Command Line Interface Guia do usuário da Versão 2.
- Faça download e instale o jq. É um JSON processador de linha de comando leve e flexível usado nos procedimentos a seguir para extrair detalhes do par de chaves. Para obter mais informações sobre como baixar e instalar o jq, consulte Baixar o jq no site do jq.

Conecte-se a um computador virtual usando SSH

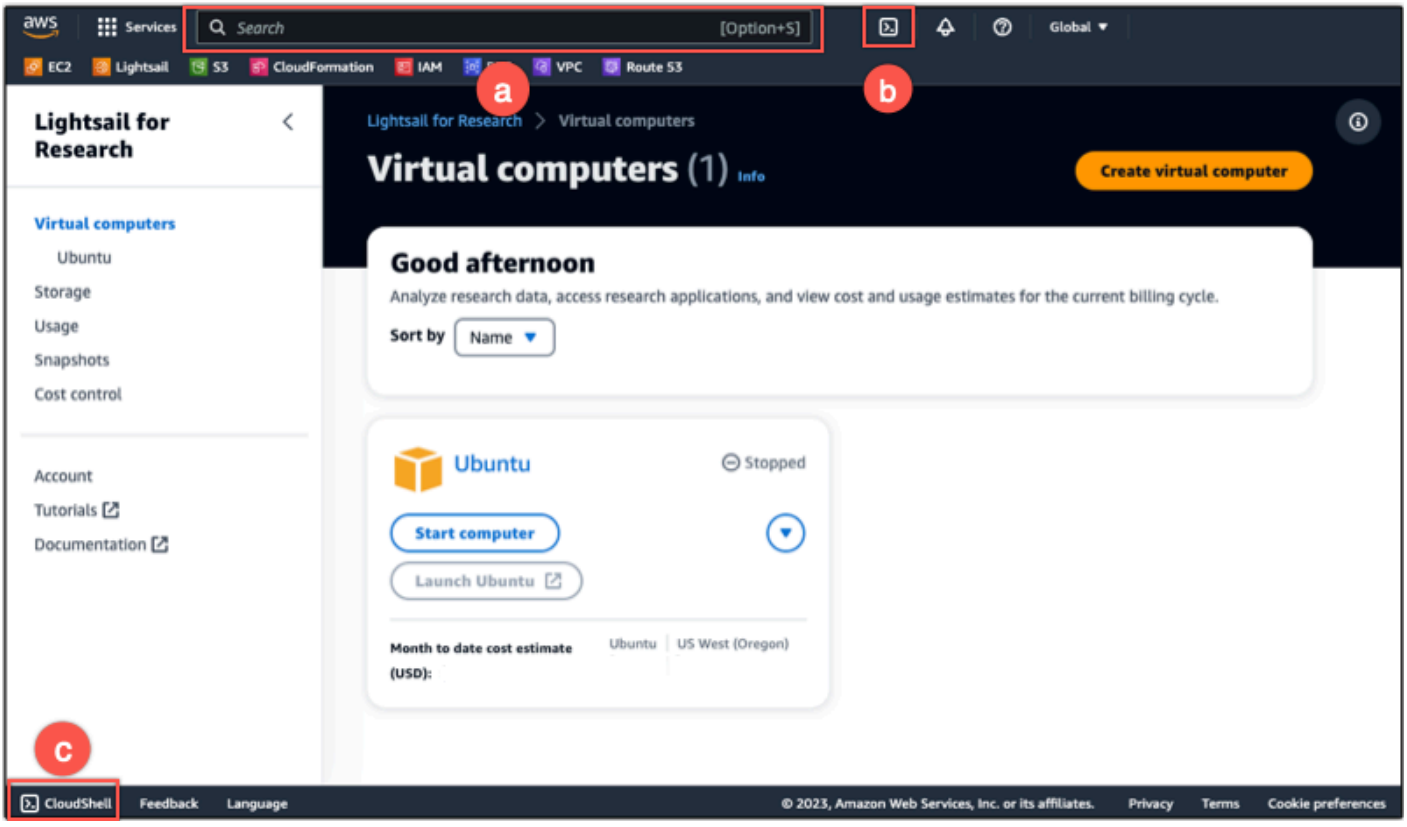
Conclua um dos procedimentos a seguir para estabelecer uma SSH conexão com seu computador virtual no Lightsail for Research.

Conecte-se a um computador virtual usando AWS CloudShell

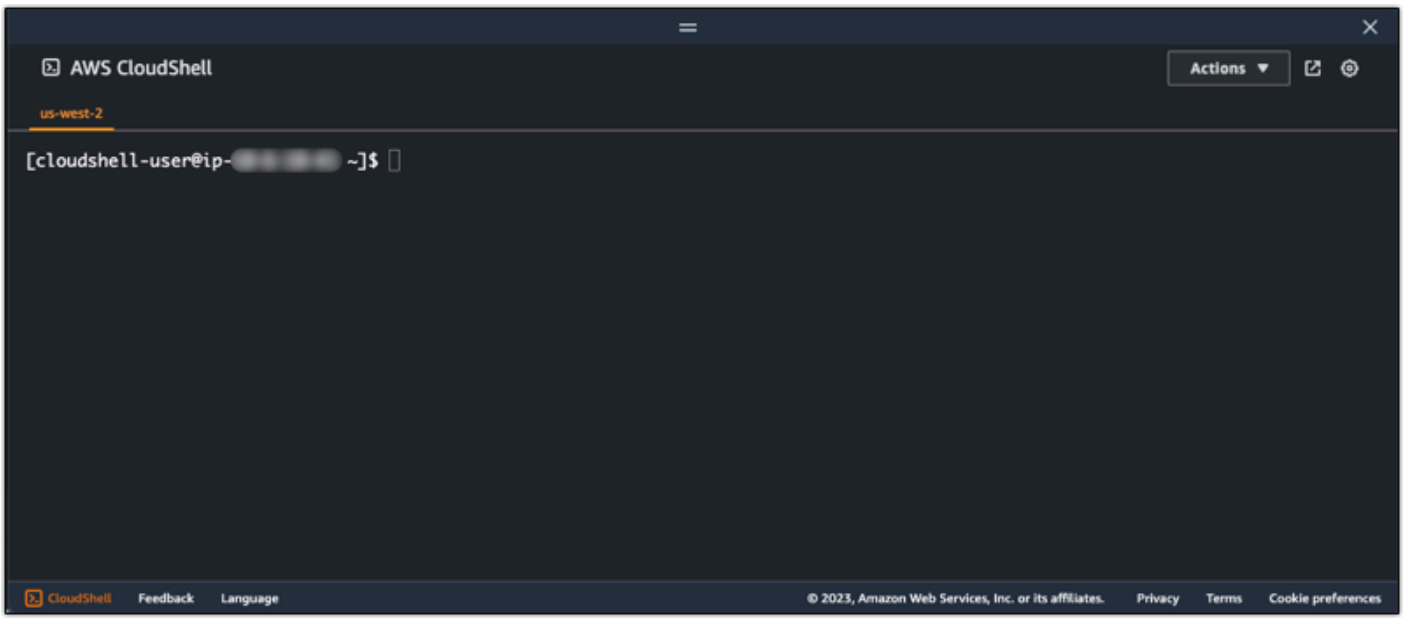
Esse procedimento se aplica se você preferir uma configuração mínima para se conectar ao seu computador virtual. AWS CloudShell usa um shell pré-autenticado baseado em navegador que você pode iniciar diretamente do. AWS Management Console Você pode executar AWS CLI comandos usando seu shell preferido, como Bash ou Z shell. PowerShell Você pode fazer isso sem baixar nem instalar ferramentas de linha de comando. Para obter mais informações, consulte Conceitos básicos do AWS CloudShell no Manual do usuário do AWS CloudShell .

> **Important**
>
> Antes de começar, certifique-se de obter o key pair padrão do Lightsail DKP () para o computador virtual ao qual você está se conectando. Para obter mais informações, consulte Obtenha um par de chaves para um computador virtual Lightsail for Research.

1. No console do Lightsail for Research, CloudShell inicie escolhendo uma das seguintes opções:
   a. Na caixa Pesquisar, digite "CloudShell“e escolha CloudShell.
   b. Na barra de navegação, escolha o CloudShellícone.
   c. Escolha CloudShellna barra de ferramentas do console no canto inferior esquerdo do console.



Quando o prompt de comando for exibido, o shell estará pronto para interação.



2. Escolha um shell pré-instalado para trabalhar. Para alterar o shell padrão, digite um dos seguintes nomes de programa no prompt da linha de comando. Bashé o shell padrão que está sendo executado quando você inicia AWS CloudShell.

   Bash

   ```
   bash
   ```

   Se você alternar para o Bash, o símbolo no prompt de comando será atualizado para $.

   PowerShell

   ```
   pwsh
   ```

   Se você mudar para PowerShell, o símbolo no prompt de comando será atualizado paraPS>.

   Z shell

   ```
   zsh
   ```

   Se você alternar para o Z shell, o símbolo no prompt de comando será atualizado para %.

3. Para se conectar a um computador virtual a partir da janela do CloudShell terminal, consulteConecte-se a um computador virtual usando SSH um computador local Linux, Unix ou macOS.

Para obter informações sobre o software pré-instalado no CloudShell ambiente, consulte o ambiente AWS CloudShell computacional no Guia do AWS CloudShell usuário.

Conecte-se a um computador virtual usando SSH um computador local Windows

Esse procedimento se aplica se o computador local usa um sistema operacional Windows. Esse procedimento usa o `get-instance` AWS CLI comando para obter o nome de usuário e o endereço IP público da instância à qual você deseja se conectar. Para obter mais informações, consulte obtenha-instâncias na Referência de comandos da AWS CLI .

> **Important**
>
> Certifique-se de obter o key pair DKP () padrão do Lightsail para o computador virtual ao qual você está tentando se conectar antes de iniciar esse procedimento. Para obter mais informações, consulte Obtenha um par de chaves para um computador virtual Lightsail for Research. Esse procedimento gera a chave privada do DKP Lightsail em `dkp_rsa` um arquivo usado em um dos comandos a seguir.

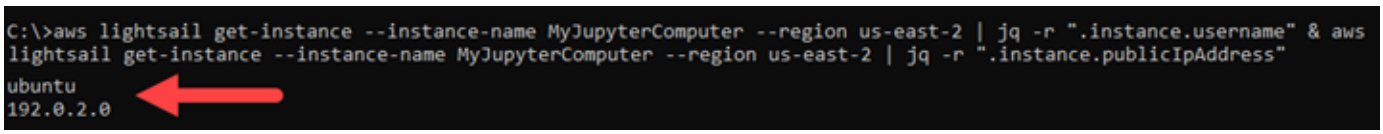
1. Abra a janela Command Prompt (Prompt de comando).
2. Digite o comando a seguir para exibir o endereço IP público e o nome de usuário do seu computador virtual. No comando, *`region-code`* substitua pelo código do Região da AWS no qual o computador virtual foi criado, como`us-east-2`. Substitua *`computer-name`* pelo nome do computador virtual ao qual você deseja se conectar.

   ```
   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"
   ```

   Exemplo

   ```
   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"
   ```

   A resposta exibirá o nome de usuário e endereço IP público do computador virtual conforme mostrado no exemplo a seguir. Anote esses valores, pois você precisará deles na etapa seguinte deste procedimento.

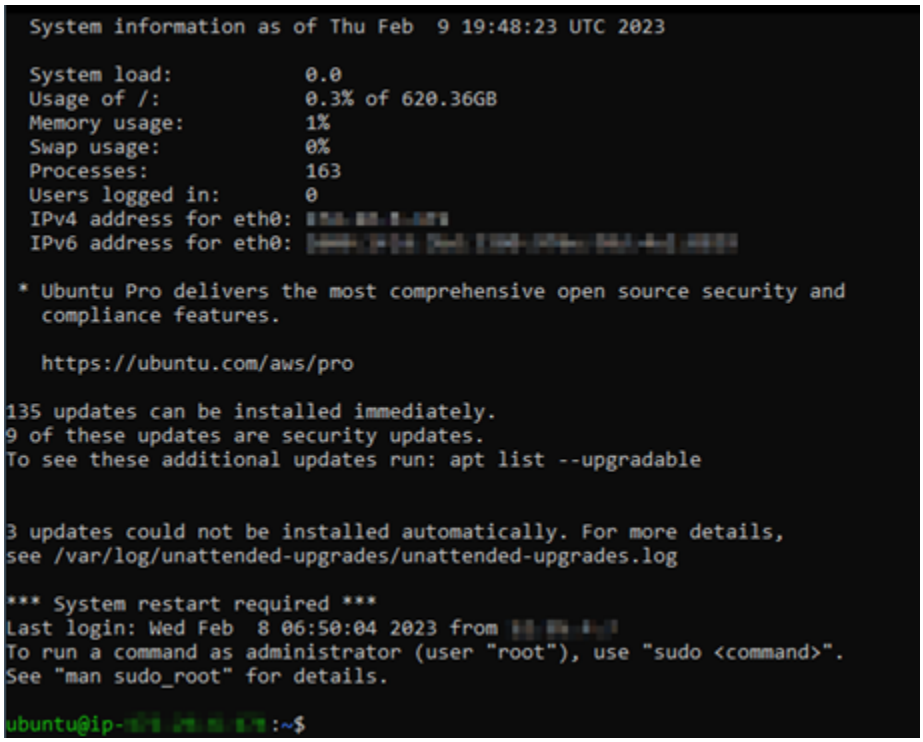
3. Digite o comando a seguir para estabelecer uma SSH conexão com seu computador virtual. No comando, substitua *user-name* pelo nome de usuário de login e *public-ip-address* substitua pelo endereço IP público do seu computador virtual.

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

Exemplo

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

Você deve ver uma resposta semelhante ao exemplo a seguir, que mostra uma SSH conexão estabelecida com um computador virtual Ubuntu no Lightsail for Research.



Agora que você estabeleceu com êxito uma SSH conexão com seu computador virtual, vá para a próxima seção para ver as próximas etapas adicionais.

Conecte-se a um computador virtual usando SSH um computador local Linux, Unix ou macOS

Esse procedimento se aplica se o computador local usa um sistema operacional Linux, Unix ou macOS. Esse procedimento usa o `get-instance` AWS CLI comando para obter o nome de usuário

e o endereço IP público da instância à qual você deseja se conectar. Para obter mais informações, consulte obtenha-instâncias na Referência de comandos da AWS CLI .

> **Important**
>
> Certifique-se de obter o key pair DKP () padrão do Lightsail para o computador virtual ao qual você está tentando se conectar antes de iniciar esse procedimento. Para obter mais informações, consulte Obtenha um par de chaves para um computador virtual Lightsail for Research. Esse procedimento gera a chave privada do DKP Lightsail em `dkp_rsa` um arquivo usado em um dos comandos a seguir.

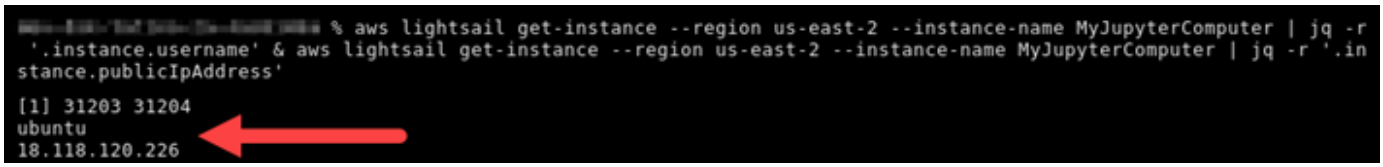
1. Abra uma janela do Terminal.
2. Digite o comando a seguir para exibir o endereço IP público e o nome de usuário do seu computador virtual. No comando, *`region-code`* substitua pelo código da AWS região na qual o computador virtual foi criado, como`us-east-2`. Substitua *`computer-name`* pelo nome do computador virtual ao qual você deseja se conectar.

   ```
   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'
   ```

   Exemplo

   ```
   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'
   ```

   A resposta exibirá o nome de usuário e endereço IP público do computador virtual conforme mostrado no exemplo a seguir. Anote esses valores, pois você precisará deles na etapa seguinte deste procedimento.

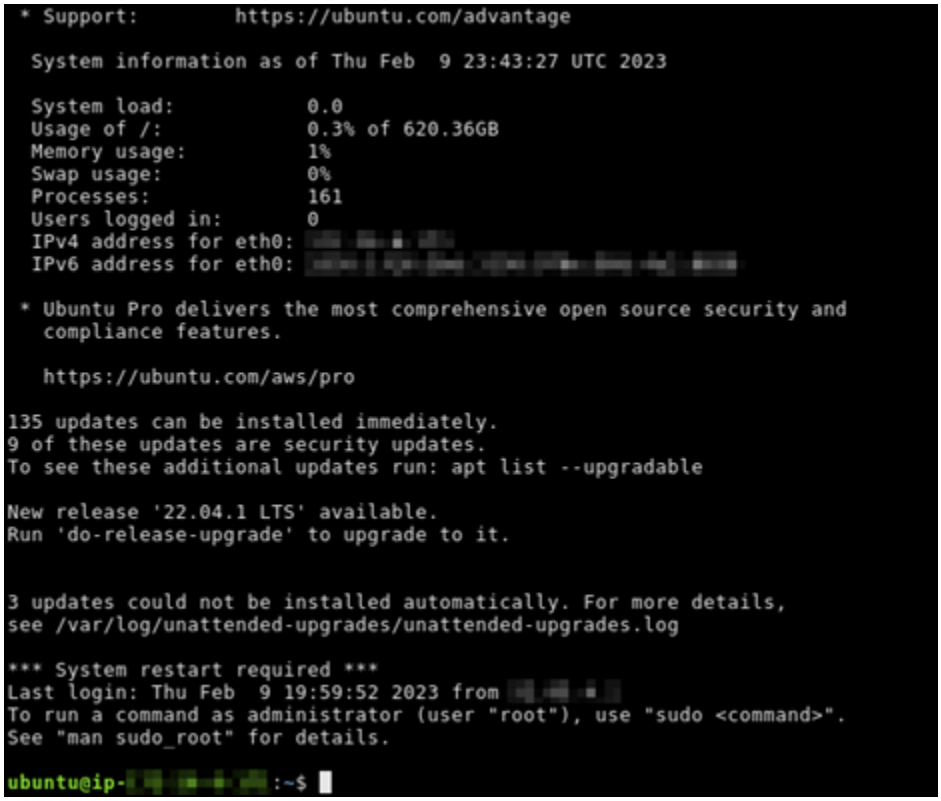
3. Digite o comando a seguir para estabelecer uma SSH conexão com seu computador virtual. No comando, substitua *`user-name`* pelo nome de usuário de login e *`public-ip-address`* substitua pelo endereço IP público do seu computador virtual.

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

Exemplo

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

Você deve ver uma resposta semelhante ao exemplo a seguir, que mostra uma SSH conexão estabelecida com um computador virtual Ubuntu no Lightsail for Research.



Agora que você estabeleceu com êxito uma SSH conexão com seu computador virtual, vá para a próxima seção para ver as próximas etapas adicionais.

Continue para as próximas etapas

Você pode concluir as próximas etapas adicionais a seguir depois de estabelecer com êxito uma SSH conexão com seu computador virtual:

- Conecte-se ao seu computador virtual usando SCP para transferir arquivos com segurança. Para obter mais informações, consulte Transfira arquivos para computadores virtuais do Lightsail for Research usando o Secure Copy.

Transfira arquivos para computadores virtuais do Lightsail for Research usando o Secure Copy

Você pode transferir arquivos do seu computador local para um computador virtual no Amazon Lightsail for Research usando o Secure Copy (). SCP Com esse processo, você pode transferir vários arquivos ou diretórios inteiros ao mesmo tempo.

> **Note**
>
> Você também pode estabelecer uma conexão de protocolo de exibição remota com seu computador virtual usando o NICE DCV cliente baseado em navegador disponível no console do Lightsail for Research. Com o NICE DCV cliente, você pode transferir rapidamente arquivos individuais. Para obter mais informações, consulte Acesse o sistema operacional do seu computador virtual Lightsail for Research.

Tópicos

Conclua os pré-requisitos

Conclua os seguintes pré-requisitos antes de começar.

- Crie um computador virtual no Lightsail for Research. Para obter mais informações, consulte Crie um computador virtual Lightsail for Research.
- Verifique se o computador virtual ao qual você deseja se conectar está em execução. Além disso, anote o nome do computador virtual e a AWS região na qual ele foi criado. Você precisará dessas informações mais tarde neste processo. Para obter mais informações, consulte Veja os detalhes do computador virtual Lightsail for Research.

- Baixe e instale o AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Instalar ou atualizar a versão mais recente da AWS CLI no AWS Command Line Interface Guia do usuário da Versão 2.
- Configure o AWS CLI para acessar seu Conta da AWS. Para obter mais informações, consulte Conceitos básicos de configuração da no AWS Command Line Interface Guia do usuário da Versão 2.
- Faça download e instale o jq. É um JSON processador de linha de comando leve e flexível usado nos procedimentos a seguir para extrair detalhes do par de chaves. Para obter mais informações sobre como baixar e instalar o jq, consulte Baixar o jq no site do jq.
- Certifique-se de que a porta 22 esteja aberta no computador virtual ao qual você deseja se conectar. Essa é a porta padrão usada paraSSH. É aberto por padrão Mas se você o fechou, deverá reabri-lo antes de continuar. Para obter mais informações, consulte Gerencie portas de firewall para computadores virtuais do Lightsail for Research.
- Obtenha o par de chaves padrão do Lightsail DKP () para seu computador virtual. Para obter mais informações, consulte Crie um computador virtual Lightsail for Research.

Conecte-se a um computador virtual usando SCP

Conclua um dos procedimentos a seguir para se conectar ao seu computador virtual no Lightsail for Research usando. SCP

Conecte-se a um computador virtual usando SCP um computador local Windows

Esse procedimento se aplica a você se o computador local usa um sistema operacional Windows. Esse procedimento usa o `get-instance` AWS CLI comando para obter o nome de usuário e o endereço IP público da instância à qual você deseja se conectar. Para obter mais informações, consulte obtenha-instâncias na Referência de comandos da AWS CLI .

> **Important**
>
> Certifique-se de obter o key pair DKP () padrão do Lightsail para o computador virtual ao qual você está tentando se conectar antes de iniciar esse procedimento. Para obter mais informações, consulte Obtenha um par de chaves para um computador virtual Lightsail for Research. Esse procedimento gera a chave privada do DKP Lightsail em `dkp_rsa` um arquivo usado em um dos comandos a seguir.

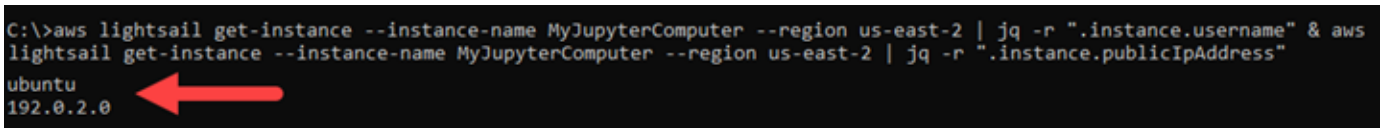
1. Abra a janela Command Prompt (Prompt de comando).
2. Digite o comando a seguir para exibir o endereço IP público e o nome de usuário do seu computador virtual. No comando, *region-code* substitua pelo código da AWS região na qual o computador virtual foi criado, como `us-east-2`. Substitua *computer-name* pelo nome do computador virtual ao qual você deseja se conectar.

```
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"
```

   Exemplo

```
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"
```

   A resposta exibirá o nome de usuário e endereço IP público do computador virtual conforme mostrado no exemplo a seguir. Anote esses valores, pois você precisará deles na etapa seguinte deste procedimento.



3. Digite o comando a seguir para estabelecer uma SCP conexão com seu computador virtual e transferir arquivos para ele.

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

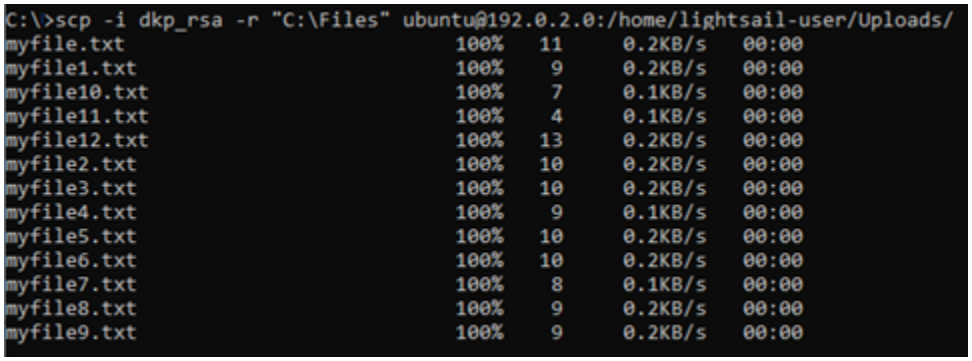
   No comando, substitua:

   - *source-folder* com a pasta em seu computador local que contém os arquivos que você deseja transferir.
   - *user-name* com o nome de usuário da etapa anterior desse procedimento (como `ubuntu`).
   - *public-ip-address* com o endereço IP público do seu computador virtual da etapa anterior deste procedimento.
   - *destination-directory* com o caminho para o diretório no computador virtual no qual você deseja copiar seus arquivos.

O exemplo a seguir copia todos os arquivos da `C:\Files` pasta no computador local para o `/home/lightsail-user/Uploads/` diretório no computador virtual remoto.

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

Você verá um resultado semelhante ao seguinte exemplo. Ele mostra cada arquivo que foi transferido da pasta de origem para o diretório de destino. Agora você deve conseguir acessar esses arquivos em seu computador virtual.



Conecte-se a um computador virtual usando SCP um computador local Linux, Unix ou macOS

Este procedimento se aplica a você se o seu computador local estiver utilizando um sistema operacional Linux, Unix ou macOS. Esse procedimento usa o `get-instance` AWS CLI comando para obter o nome de usuário e o endereço IP público da instância à qual você deseja se conectar. Para obter mais informações, consulte obtenha-instâncias na Referência de comandos da AWS CLI .

> **Important**
>
> Certifique-se de obter o key pair DKP () padrão do Lightsail para o computador virtual ao qual você está tentando se conectar antes de iniciar esse procedimento. Para obter mais informações, consulte Obtenha um par de chaves para um computador virtual Lightsail for Research. Esse procedimento gera a chave privada do DKP Lightsail em `dkp_rsa` um arquivo usado em um dos comandos a seguir.

1. Abra uma janela do Terminal.
2. Digite o comando a seguir para exibir o endereço IP público e o nome de usuário do seu computador virtual. No comando, *`region-code`* substitua pelo código da AWS região na qual

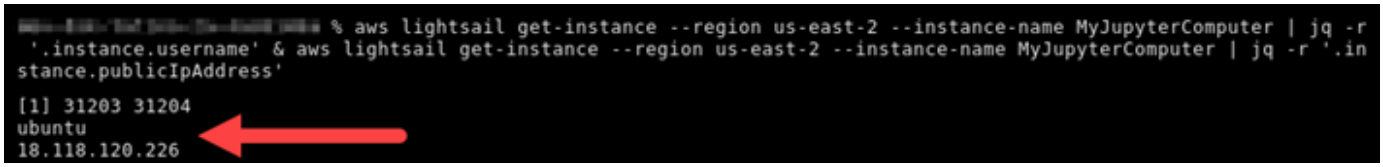
o computador virtual foi criado, comous-east-2. Substitua *computer-name* pelo nome do computador virtual ao qual você deseja se conectar.

```
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'
```

Exemplo

```
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'
```

A resposta exibirá o nome de usuário e endereço IP público do computador virtual conforme mostrado no exemplo a seguir. Anote esses valores, pois você precisará deles na etapa seguinte deste procedimento.



3. Digite o comando a seguir para estabelecer uma SCP conexão com seu computador virtual e transferir arquivos para ele.

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

No comando, substitua:

- *source-folder* com a pasta em seu computador local que contém os arquivos que você deseja transferir.
- *user-name* com o nome de usuário da etapa anterior desse procedimento (como ubuntu).
- *public-ip-address* com o endereço IP público do seu computador virtual da etapa anterior deste procedimento.
- *destination-directory* com o caminho para o diretório no computador virtual no qual você deseja copiar seus arquivos.

O exemplo a seguir copia todos os arquivos da C:\Files pasta no computador local para o /home/lightsail-user/Uploads/ diretório no computador virtual remoto.

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

Você verá um resultado semelhante ao seguinte exemplo. Ele mostra cada arquivo que foi transferido da pasta de origem para o diretório de destino. Agora você deve conseguir acessar esses arquivos em seu computador virtual.

```
([redacted]) <0> [~/Documents/Keys]
[redacted] scp -i dkp_rsa -r 'Files' ubuntu@192.0.0.2:/home/lightsail-user/Uploads/
myfile2.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
myfile10.txt                                  100%    7     0.1KB/s   00:00
myfile1.txt                                   100%    9     0.2KB/s   00:00
myfile3.txt                                   100%   10     0.2KB/s   00:00
myfile12.txt                                  100%   13     0.2KB/s   00:00
myfile.txt                                    100%   11     0.2KB/s   00:00
myfile9.txt                                   100%    9     0.2KB/s   00:00
myfile11.txt                                  100%    4     0.1KB/s   00:00
myfile5.txt                                   100%   10     0.2KB/s   00:00
myfile4.txt                                   100%    9     0.2KB/s   00:00
myfile8.txt                                   100%    9     0.2KB/s   00:00
```

Excluir um computador virtual do Lightsail for Research

Conclua as etapas a seguir para excluir seu computador virtual Lightsail for Research quando você não precisar mais dele. A cobrança será interrompida assim que o computador virtual for excluída. Os recursos que estavam vinculados ao computador excluído, como snapshots, continuam incorrendo em custos até que você os exclua.

> **Important**
>
> A exclusão de um computador virtual é uma ação permanente e o computador não pode ser recuperado. Se você precisar dos seus dados posteriormente, crie um snapshot de seu computador virtual antes de excluí-lo. Para obter mais informações, consulte Criar um snapshot.

1. Faça login no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação.
3. Escolha o computador virtual a ser excluído.
4. Escolha Ações e, em seguida, escolha Excluir computador virtual.
5. Digite confirmar no bloco de texto. Em seguida, escolha Excluir computador virtual.

Proteja e armazene dados com os volumes do Lightsail for Research

O Amazon Lightsail for Research fornece volumes de armazenamento (discos) em nível de bloco que você pode conectar a um computador virtual do Lightsail for Research em execução. Você pode usar o disco como um dispositivo de armazenamento principal para dados que exigem atualizações frequentes e granulares. Por exemplo, discos são a opção de armazenamento recomendada quando você executa um banco de dados em um computador virtual Lightsail for Research.

Um disco se comporta-se como um dispositivo de blocos externo não formatado que você pode fixar a um único computador virtual. O volume persiste independentemente da vida útil em execução de um computador. Depois de fixar um disco a um computador, você pode usá-lo como qualquer outro disco rígido físico.

Você pode fixar vários discos a um computador. Você também pode desconectar um disco de um computador e fixá-lo a outro computador.

Para manter uma cópia de backup dos seus dados, crie um snapshot do disco. Você pode criar um novo disco a partir de um snapshot e fixá-lo a outro computador.

Tópicos

Crie um disco de armazenamento no console do Lightsail for Research

Conclua as etapas a seguir para criar um disco para seu computador virtual Lightsail for Research.

1. Faça login no console do Lightsail for Research.
2. Escolha Armazenamento no painel de navegação.

3. Selecione Criar disco.
4. Insira um nome para o disco. Caracteres válidos incluem caracteres alfanuméricos, números, pontos, hífens e sublinhados.

   Os nomes de discos devem atender aos seguintes requisitos:

   - Seja único Região da AWS em cada um em sua conta do Lightsail for Research.
   - Contêm de 2 a 255 caracteres.
   - Comece e termine com um caractere alfanumérico ou com um número.
5. Escolha um Região da AWS para o seu disco.

   O disco deve estar na mesma Região que o computador virtual ao qual você o fixará.
6. Escolha o tamanho do disco em GB.
7. Continue até a seção Fixar um disco para obter informações sobre como conectar discos ao seu computador virtual.

Veja os detalhes do disco de armazenamento no console do Lightsail for Research

Conclua as etapas a seguir para visualizar os discos em sua conta do Lightsail for Research e seus detalhes.

1. Faça login no console do Lightsail for Research.
2. Escolha Armazenamento no painel de navegação.

   A página Armazenamento fornece uma visão abrangente dos discos em sua conta do Lightsail for Research.

   As seguintes informações são exibidas na página:

   - Nome — O nome do seu disco de armazenamento.
   - Tamanho — O tamanho do seu disco (em GB).
   - Região da AWS— O Região da AWS seu disco foi criado em.
   - Conectado a — O computador Lightsail ao qual seu disco está conectado.
   - Data de criação — A data em que seu disco foi criado.

Adicione armazenamento a um computador virtual no Lightsail for Research

Conclua as etapas a seguir para conectar um disco a um computador virtual no Lightsail for Research. É possível fixar até 15 discos a um computador virtual. Quando você conecta um disco ao seu computador virtual usando o console do Lightsail for Research, ele é automaticamente formatado e montado pelo serviço. Esse processo leva alguns minutos, portanto, você deve confirmar que o disco atingiu o status de Montagem antes de começar a usá-lo. Por padrão, o Lightsail for Research monta discos no diretório; `<disk-name>` onde está `/home/lightsail-user/<disk-name>` o nome que você deu ao seu disco.

> **Important**
>
> Antes de fixar um disco a um computador virtual, o computador virtual deve estar em um estado em Execução. Se você fixar um disco a um computador virtual enquanto ele estiver no estado Parado, o disco será conectado, mas falhará na montagem. Se o status de Montagem do disco estiver como Falha, você deverá desconectar o disco e fixá-lo quando o computador virtual estiver em Execução.

1. Faça login no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação.
3. Escolha o computador ao qual fixar o disco.
4. Escolha a guia Armazenamento.
5. Escolha Fixar disco.
6. Selecione o nome do disco a ser fixado ao computador.
7. Escolha Fixar .

Separe um disco de um computador virtual no Lightsail for Research

Conclua as etapas a seguir para separar um disco de um computador.

1. Faça login no console do Lightsail for Research.

2. Escolha Armazenamento no painel de navegação.
3. Encontre o disco a ser separado. Na coluna Fixado a, escolha o nome do computador ao qual o disco está fixado.
4. Escolha Parar para parar o computador. Você deve parar o computador antes de poder separar o disco.
5. Confirme que você deseja parar o computador e escolha Parar computador.
6. Escolha a guia Armazenamento.
7. Selecione o disco a ser separado e, em seguida, escolha Separar.
8. Confirme que você deseja separar o disco do computador e escolha Separar.

Exclua discos de armazenamento não utilizados no Lightsail for Research

Complete as seguintes etapas para excluir um disco de armazenamento quando você não precisar mais dele. Você interrompe a geração de cobranças para o disco assim que ele é excluído.

Se o disco estiver fixado a um computador, você deverá primeiro separá-lo para poder excluí-lo. Para obter mais informações, consulte Separe um disco de um computador virtual no Lightsail for Research.

1. Faça login no console do Lightsail for Research.
2. Escolha Armazenamento no painel de navegação.
3. Encontre e selecione o disco a ser excluído.
4. Escolha Excluir disco.
5. Confirme que deseja excluir o seu disco. Em seguida, selecione Excluir.

Faça backup de computadores e discos virtuais com instantâneos do Lightsail for Research

Os instantâneos são uma point-in-time cópia dos seus dados. Você pode criar snapshots dos seus computadores virtuais e discos de armazenamento do Amazon Lightsail for Research e usá-los como linhas de base para criar novos computadores ou fazer backup de dados.

Um snapshot contém todos os dados necessários para restaurar o computador (a partir do momento em que o snapshot foi criado). Quando você cria um novo computador virtual a partir de um snapshot, ele começa como uma réplica exata do computador original que foi utilizado para criar o snapshot.

Como seus recursos podem falhar a qualquer momento, recomendamos criar snapshots frequentes para evitar perda permanente de dados.

Tópicos

Crie instantâneos dos computadores ou discos virtuais do Lightsail for Research

Conclua as etapas a seguir para criar um instantâneo do seu computador ou disco virtual do Lightsail for Research.

1. Faça login no console do Lightsail for Research.
2. Selecione Snapshots no painel de navegação.
3. Conclua uma das seguintes etapas:

    - Em Snapshots do computador virtual, localize o nome do computador que você deseja capturar e escolha Criar snapshot.
    - Em Snapshots do computador virtual, localize o nome do computador que você deseja capturar e escolha Criar snapshot.

4. Insira um nome do seu snapshot. Caracteres válidos incluem caracteres alfanuméricos, números, pontos, hífens e sublinhados.

   Os nomes de snapshots devem atender aos seguintes requisitos:

   - Seja único Região da AWS em cada um em sua conta do Lightsail for Research.
   - Contêm de 2 a 255 caracteres.
   - Comece e termine com um caractere alfanumérico ou com um número.
5. Escolha Criar snapshot.

Visualize e gerencie instantâneos de disco e computadores virtuais no Lightsail for Research

Conclua as etapas a seguir para visualizar instantâneos de seus computadores e discos virtuais.

1. Faça login no console do Lightsail for Research.
2. Selecione Snapshots no painel de navegação.

   A página Snapshots exibe snapshots do computador virtual e do disco que você criou.

   Os snapshots também estão localizados nesta página. Snapshots arquivados são snapshots de recursos que foram excluídos da sua conta.

Crie um computador ou disco virtual a partir de um snapshot

Conclua as etapas a seguir para criar um novo computador ou disco virtual do Lightsail for Research a partir de um snapshot.

Ao criar um computador virtual a partir de um snapshot, use um plano do mesmo tamanho ou maior do que o usado no computador original. Você não pode usar um plano menor do que o computador virtual original.

Ao criar um disco a partir de um snapshot, escolha um tamanho de disco maior que o disco original. Você não pode usar um disco menor que o original.

1. Faça login no console do Lightsail for Research.
2. Selecione Snapshots no painel de navegação.

3. Na página Snapshots, localize o nome do snapshot do computador ou disco que você usará para criar o novo computador ou disco. Escolha o menu suspenso Snapshots para exibir uma lista dos instantâneos disponíveis para esse recurso.
4. Selecione o snapshot que deseja usar para criar o computador virtual.
5. Escolha no menu suspenso Ações. Em seguida, escolha Criar computador virtual ou Criar disco.

Excluir um instantâneo no console do Lightsail for Research

Complete as seguintes etapas para excluir um snapshot.

1. Faça login no console do Lightsail for Research.
2. Selecione Snapshots no painel de navegação.
3. Na página Snapshots, localize o nome do computador ou do snapshot do disco que você deseja excluir. Escolha o menu suspenso Snapshots para exibir uma lista dos instantâneos disponíveis para esse recurso.
4. Selecione o snapshot que você deseja excluir.
5. Escolha o menu suspenso Ações. Em seguida, escolha Excluir snapshot.
6. Verifique se o nome do snapshot está correto. Em seguida, escolha Excluir snapshot.

Estimativas de custo e uso no Lightsail for Research

O Amazon Lightsail for Research oferece estimativas de custo e uso para seus recursos. AWS Você pode usar essas estimativas para ajudá-lo a planejar seus gastos, encontrar oportunidades de redução de custos e tomar decisões informadas ao usar o Lightsail for Research.

Quando você cria um computador ou disco virtual, são exibidas estimativas de custo e uso para esse recurso. Uma estimativa de custo e uso começa a ser monitorada assim que um recurso é criado e está em um estado Disponível ou Executando. A estimativa aparecerá no AWS Management Console em até 15 minutos após a criação do recurso. Os recursos que foram excluídos não estão incluídos em uma estimativa.

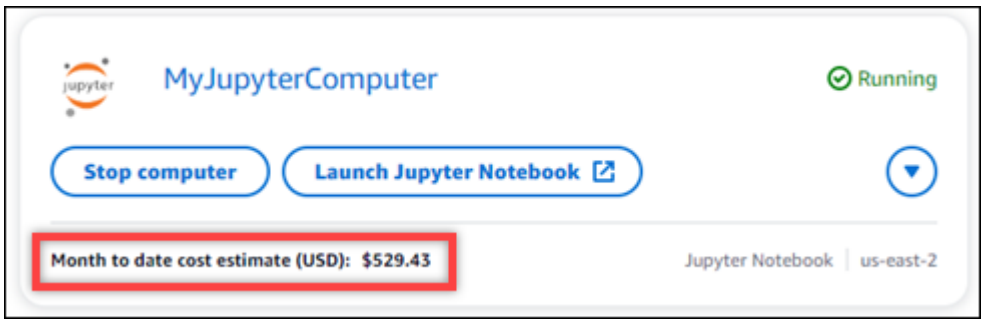
> **Important**
>
> Uma estimativa é um custo estimado com base no uso do recurso. Seu custo real será baseado no uso real de seus recursos, não na estimativa mostrada no console do Lightsail for Research. Os custos reais são mostrados no extrato AWS Billing da sua conta. Faça login no AWS Management Console e abra o AWS Billing console em https://console.aws.amazon.com/billing/.

Tópicos

Veja estimativas de custo e uso de seus recursos no Lightsail for Research

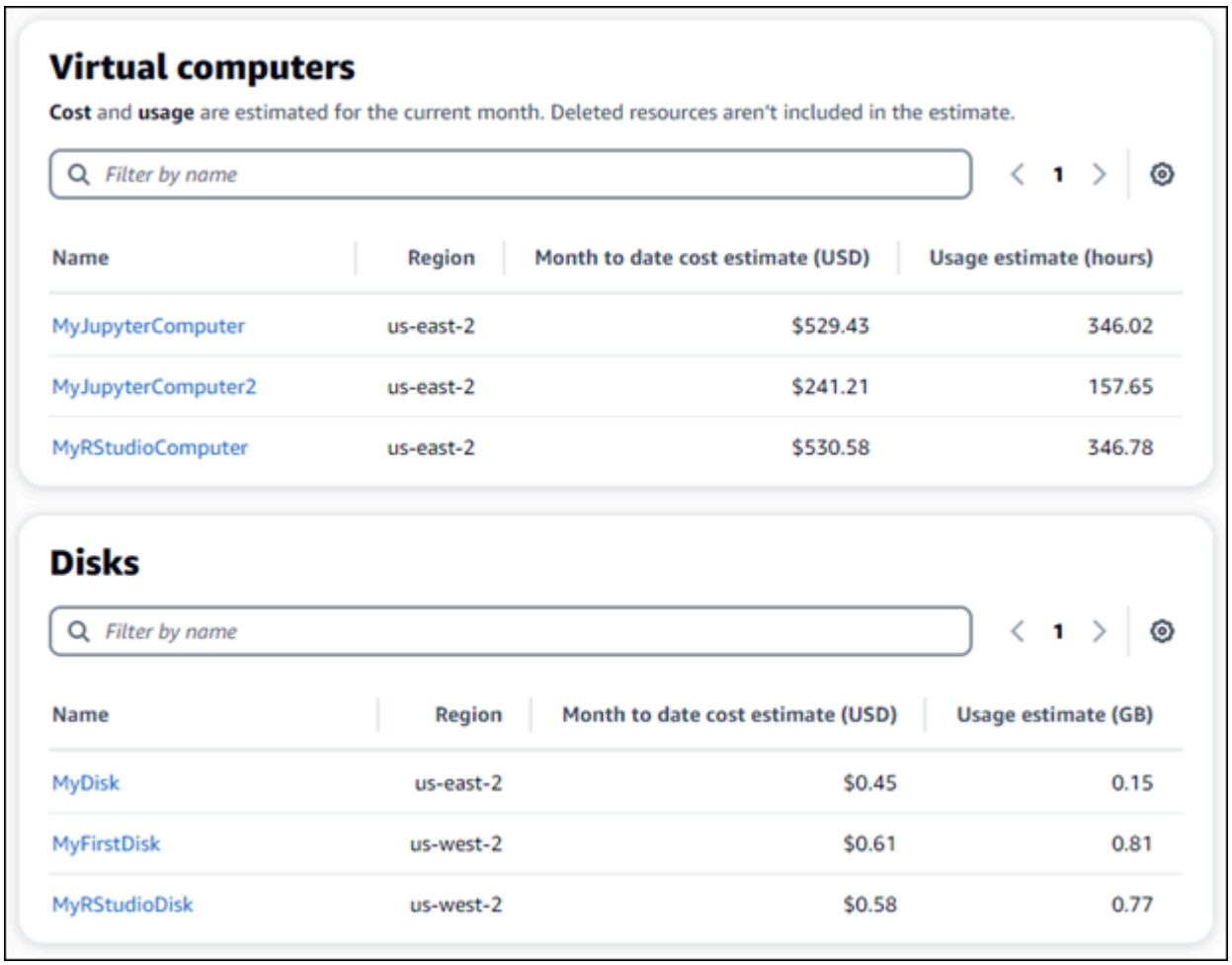
As estimativas mensais de custo e uso de seus recursos do Lightsail for Research são exibidas nas seguintes áreas do console do Lightsail for Research.

1. Escolha Computadores virtuais no painel de navegação do console do Lightsail for Research. A estimativa de custo mensal para seus computadores virtuais está listada em cada computador virtual em execução.



2. Para ver a CPU utilização de um computador virtual, escolha o nome do computador virtual e, em seguida, escolha a guia Painel.

3. Para ver as estimativas de custo e uso do mês para todos os seus recursos do Lightsail for Research, escolha Uso no painel de navegação.


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

Gerencie as regras de controle de custos no Lightsail for Research

O controle de custos usa regras que você define para ajudar a gerenciar o uso e o custo de seus computadores virtuais do Lightsail for Research.

Você pode criar uma regra de Parar computador virtual em inatividade que interrompe um computador em execução quando ele atinge uma porcentagem especificada de sua CPU utilização durante um determinado período. Por exemplo, uma regra pode parar automaticamente um computador específico quando sua CPU utilização for igual ou inferior a 5% durante um período de 30 minutos. Isso significa que o computador está ocioso e o Lightsail for Research interrompe o computador. Você não incorre mais nas cobranças horárias padrão depois que o computador virtual é interrompido.

Tópicos

Crie regras de controle de custos para seus computadores virtuais do Lightsail for Research

Conclua as etapas a seguir para criar uma regra para seu computador virtual Lightsail for Research.

> **Note**
>
> A única ação de regra compatível no momento é parar um computador virtual. CPUa utilização é a única métrica atualmente monitorada por regras, e a única operação suportada é menor ou igual a.

1. Faça login no console do Lightsail for Research.
2. No painel de navegação, selecione Executar comando.
3. Escolha Criar Regra.
4. Selecione o recurso ao qual aplicar a regra.

5. Especifique a porcentagem CPU de utilização e o período em que a regra deve ser executada.

   Por exemplo, você pode especificar 5 por cento e 30 minutos. O Lightsail for Research interrompe automaticamente o computador quando CPU sua utilização é menor ou igual a 5% durante um período de 30 minutos.
6. Escolha Criar Regra.
7. Confirme se as informações da sua nova regra estão corretas e escolha Confirmar.

Exclua regras de controle de custos para seus computadores virtuais do Lightsail for Research

Conclua as etapas a seguir para excluir uma regra do seu computador virtual Lightsail for Research.

1. Faça login no console do Lightsail for Research.
2. No painel de navegação, selecione Executar comando.
3. Selecione a regra a ser excluída.
4. Escolha Excluir.
5. Escolha Delete (Excluir) para a regra que você deseja excluir.

Organize os recursos do Lightsail for Research com tags

Com o Amazon Lightsail for Research, você pode atribuir tags aos seus recursos. Cada tag é uma etiqueta que consiste em uma chave e um valor opcional, o que pode tornar eficiente a gestão dos seus recursos. Uma chave sem um valor é chamada de tag apenas com chave (key-only tag), e uma chave com um valor é chamada de tag chave-valor (key-value tag). Embora não haja tipos de tags inerentes, elas permitem categorizar seus recursos do por finalidade, proprietário, ambiente ou outros critérios. Isso é útil quando você tem muitos recursos do mesmo tipo. Identifique rapidamente um recurso específico com base nas tags atribuídas a ele. Por exemplo, você pode definir um conjunto de tags que o ajudem a rastrear o projeto ou a prioridade de cada recurso.

Os seguintes recursos podem ser marcados no console do Amazon Lightsail for Research:

- Computadores virtuais
- Discos de armazenamento
- Snapshots

As restrições a seguir se aplicam às tags:

- O número máximo de tags por recurso é 50.
- Para cada recurso, cada chave de tag deve ser única. Cada chave de tag pode ter apenas um valor.
- O tamanho máximo da chave é 128 caracteres Unicode em UTF -8.
- O tamanho máximo do valor é 256 caracteres Unicode em UTF -8.
- Se o seu esquema de tags é usado em vários serviços e recursos , lembre-se de que outros serviços talvez tenham restrições em caracteres permitidos. Em geral, os caracteres permitidos são letras, números, espaços e os seguintes caracteres: `+ - = . _ : / @` .
- As chaves e os valores de tags diferenciam maiúsculas de minúsculas.
- Não use o prefixo `aws:` para chaves ou valores. Esse prefixo está reservado para AWS uso.

Tópicos

- Tag: recursos do Lightsail for Research
- Remover tags dos recursos do Lightsail for Research

Tag: recursos do Lightsail for Research

Conclua as etapas a seguir para criar uma tag para seu computador virtual Lightsail for Research. As etapas são semelhantes para discos e instantâneos do Lightsail for Research.

1. Faça login no console do Lightsail for Research no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação.
3. Escolha o computador virtual para o qual você deseja criar uma tag.
4. Escolha a guia Tags.
5. Selecione Gerenciar tags.
6. Selecione Adicionar nova tag.
7. Insira um nome de chave no campo Chave. Por exemplo, Projeto.
8. (Opcional) Insira o nome do valor no campo do valor. Por exemplo, Blog.
9. Escolha Salvar alterações para salvar a chave em seu computador virtual.

Remover tags dos recursos do Lightsail for Research

Conclua as etapas a seguir para excluir uma tag do seu computador virtual Lightsail for Research. As etapas são semelhantes para discos e instantâneos do Lightsail for Research.

1. Faça login no console do Lightsail for Research no console do Lightsail for Research.
2. Escolha Computadores virtuais no painel de navegação.
3. Escolha o computador virtual do qual você deseja excluir a tag.
4. Escolha a guia Tags.
5. Selecione Gerenciar tags.
6. Escolha Remover para excluir a tag do recurso.

> **Note**
>
> Se você quiser remover apenas o Valor da tag, localize o valor e escolha o ícone X ao lado dele.

7. Escolha Salvar alterações.

Segurança no Amazon Lightsail for Research

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Lightsail for Research, AWS consulte Services in Scope by Compliance Program Services in Scope by Compliance AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Essa documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Lightsail for Research. Os tópicos a seguir mostram como configurar o Lightsail for Research para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus recursos do Lightsail for Research.

Tópicos

Proteção de dados no Amazon Lightsail for Research

O modelo de responsabilidade AWS compartilhada O modelo se aplica à proteção de dados no Amazon Lightsail for Research. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Lightsail for Research ou Serviços da AWS outro usando o consoleAPI,,, AWS CLI ou. AWS SDKs Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou

de diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Identity and Access Management para Amazon Lightsail for Research

AWS Identity and Access Management (IAM) é uma ferramenta Serviço da AWS que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar os recursos do Lightsail for Research. IAMé um Serviço da AWS que você pode usar sem custo adicional.

> **Note**
>
> O Amazon Lightsail e o Lightsail for Research compartilham os mesmos parâmetros de política. IAM As alterações feitas nas políticas do Lightsail for Research também afetarão as políticas do Lightsail. Por exemplo, se um usuário tiver permissão para criar um disco no Lightsail for Research, esse mesmo usuário também poderá criar um disco no Lightsail.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Lightsail for Research.

Usuário do serviço — Se você usa o serviço Lightsail for Research para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você

usa mais recursos do Lightsail for Research para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Lightsail for Research, consulte. Solução de problemas de identidade e acesso ao Amazon Lightsail for Research

Administrador de serviços — Se você é responsável pelos recursos do Lightsail for Research em sua empresa, provavelmente tem acesso total ao Lightsail for Research. É seu trabalho determinar quais recursos e recursos do Lightsail for Research seus usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar o IAM Lightsail for Research, consulte. Como o Amazon Lightsail for Research trabalha com IAM

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Lightsail for Research. Para ver exemplos de políticas baseadas em identidade do Lightsail for Research que você pode usar, consulte. IAM Exemplos de políticas baseadas em identidade para o Amazon Lightsail for Research

Autenticando com identidades

A autenticação é como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como IAM usuário ou assumindo uma IAM função. Usuário raiz da conta da AWS

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as

solicitações. Para obter mais informações sobre como usar o método recomendado para você mesmo assinar solicitações, consulte Assinar AWS API solicitações no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Uso da autenticação multifator (MFA) AWS no Guia do IAMusuário.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter informações sobre o IAM Identity Center, consulte O que é o IAM Identity Center? no Guia do AWS IAM Identity Center usuário.

Grupos e usuários do IAM

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Usando IAM funções no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM

Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .

- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.
  - Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância

e fazendo AWS CLI AWS API solicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console AWS CLI, do ou do AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições.

Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber maisACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Como o Amazon Lightsail for Research trabalha com IAM

Antes de usar IAM para gerenciar o acesso ao Lightsail for Research, saiba IAM quais recursos estão disponíveis para uso com o Lightsail for Research.

IAMrecursos que você pode usar com o Amazon Lightsail for Research

IAMrecurso	Suporte do Lightsail for Research
Políticas baseadas em identidade	Sim
Políticas baseadas em recursos	Não
Ações das políticas	Sim
Atributos de políticas	Sim
Chaves de condição de política (específicas do serviço)	Sim
ACLs	Não
ABAC(tags nas políticas)	Parcial
Credenciais temporárias	Sim
Permissões de entidade principal	Não
Perfis de serviço	Não
Funções vinculadas ao serviço	Não

Para ter uma visão geral de como o Lightsail for Research e AWS outros serviços funcionam com a IAM maioria dos recursos, AWS consulte os serviços com os quais o Lightsail for Research funciona IAM no Guia do usuário. IAM

Políticas baseadas em identidade para o Lightsail for Research

Compatível com políticas baseadas em identidade: Sim

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para o Lightsail for Research

Para ver exemplos de políticas baseadas em identidade do Lightsail for Research, consulte. Exemplos de políticas baseadas em identidade para o Amazon Lightsail for Research

Políticas baseadas em recursos no Lightsail for Research

Suporte a políticas baseadas em recursos: não

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para habilitar o acesso entre contas, você pode especificar uma conta ou IAM entidades inteiras em outra conta como principal em uma política baseada em recursos. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um IAM administrador na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Ações políticas para o Lightsail for Research

Compatível com ações de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente com permissão que não têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do Lightsail for Research, consulte Ações definidas pelo Amazon Lightsail for Research na Referência de autorização de serviço.

As ações políticas no Lightsail for Research usam o seguinte prefixo antes da ação:

```
lightsail
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

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

Para ver exemplos de políticas baseadas em identidade do Lightsail for Research, consulte. Exemplos de políticas baseadas em identidade para o Amazon Lightsail for Research

Recursos de políticas para o Lightsail for Research

Compatível com recursos de políticas: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (ARN). Isso pode ser feito para ações

que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

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

Para ver uma lista dos tipos de recursos do Lightsail for Research e ARNs seus, consulte Recursos definidos pelo Amazon Lightsail for Research na Referência de autorização de serviço. Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas pelo Amazon Lightsail for Research. ARN

Para ver exemplos de políticas baseadas em identidade do Lightsail for Research, consulte. Exemplos de políticas baseadas em identidade para o Amazon Lightsail for Research

Chaves de condições de política para o Lightsail for Research

Compatível com chaves de condição de política específicas de serviço: Sim

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia IAM do usuário.

Para ver uma lista das chaves de condição do Lightsail for Research, consulte Chaves de condição do Amazon Lightsail for Research na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações definidas pelo Amazon Lightsail for Research.

Para ver exemplos de políticas baseadas em identidade do Lightsail for Research, consulte. Exemplos de políticas baseadas em identidade para o Amazon Lightsail for Research

ACLsno Lightsail for Research

SuportesACLs: Não

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

ABACcom o Lightsail for Research

Suportes ABAC (tags nas políticas): Parciais

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a muitos AWS recursos. Marcar entidades e recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

ABACé útil em ambientes que estão crescendo rapidamente e ajuda em situações em que o gerenciamento de políticas se torna complicado.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAMusuário.

Usando credenciais temporárias com o Lightsail for Research

Compatível com credenciais temporárias: Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS esse trabalho IAM no Guia do IAM usuário.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias emIAM.

Permissões principais entre serviços para o Lightsail for Research

Suporta sessões de acesso direto (FAS): Não

Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um Serviço da AWS, combinadas com a solicitação Serviço da AWS para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.

Funções de serviço do Lightsail for Research

Compatível com perfis de serviço: não

Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma Serviço da AWS no Guia do IAM usuário.

> **Warning**
>
> Alterar as permissões de uma função de serviço pode interromper a funcionalidade do Lightsail for Research. Edite funções de serviço somente quando o Lightsail for Research fornecer orientação para fazer isso.

Funções vinculadas a serviços do Lightsail for Research

Compatível com perfis vinculados ao serviço: Não

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. Serviço da AWS O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte AWS serviços que funcionam com. IAM Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para o Amazon Lightsail for Research

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Lightsail for Research. Eles também não podem realizar tarefas usando o AWS Management Console, AWS Command Line Interface (AWS CLI) ou AWS API. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos de JSON política, consulte Criação de IAM políticas no Guia do IAMusuário.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Lightsail for Research, incluindo o formato de cada um ARNs dos tipos de recursos, consulte Ações, recursos e chaves de condição do Amazon Lightsail for Research na Referência de autorização de serviço.

Tópicos

- Melhores práticas de política
- Usando o console do Lightsail for Research
- Permitir que usuários visualizem suas próprias permissões

Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Lightsail for Research em sua conta. Essas ações podem incorrer em custos para seus Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte políticas AWS gerenciadas ou políticas AWS gerenciadas para funções de trabalho no Guia IAM do usuário.
- Aplique permissões com privilégios mínimos — Ao definir permissões com IAM políticas, conceda somente as permissões necessárias para realizar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre IAM como usar para aplicar permissões, consulte Políticas e permissões IAM no Guia IAM do usuário.
- Use condições nas IAM políticas para restringir ainda mais o acesso — Você pode adicionar uma condição às suas políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usandoSSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica Serviço da AWS, como AWS CloudFormation. Para obter mais informações, consulte Elementos IAM JSON da política: Condição no Guia IAM do usuário.
- Use o IAM Access Analyzer para validar suas IAM políticas e garantir permissões seguras e funcionais — o IAM Access Analyzer valida políticas novas e existentes para que as políticas

sigam a linguagem da IAM política (JSON) e as melhores práticas. IAM IAMO Access Analyzer fornece mais de 100 verificações de políticas e recomendações práticas para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação da política do IAM Access Analyzer no Guia do IAM Usuário.

- Exigir autenticação multifatorial (MFA) — Se você tiver um cenário que exija IAM usuários ou um usuário root Conta da AWS, ative MFA para obter segurança adicional. Para exigir MFA quando API as operações são chamadas, adicione MFA condições às suas políticas. Para obter mais informações, consulte Configurando o API acesso MFA protegido no Guia do IAMusuário.

Para obter mais informações sobre as melhores práticas emIAM, consulte as melhores práticas de segurança IAM no Guia IAM do usuário.

Usando o console do Lightsail for Research

Para acessar o console do Amazon Lightsail for Research, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Lightsail for Research em seu. Conta da AWS Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para AWS CLI o. ou AWS API o. Em vez disso, permita o acesso somente às ações que correspondam à API operação que eles estão tentando realizar.

Para garantir que usuários e funções ainda possam usar o console do Lightsail for Research, anexe também o Lightsail for `ConsoleAccess` Research ou a política gerenciada às entidades. `ReadOnly` AWS Para obter mais informações, consulte Adicionar permissões a um usuário no Guia do IAM usuário.

Permitir que usuários visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permita IAM aos usuários visualizar as políticas embutidas e gerenciadas que estão anexadas à identidade do usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando o AWS CLI ou. AWS API

```
{
    "Version": "2012-10-17",
```

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

Solução de problemas de identidade e acesso ao Amazon Lightsail for Research

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Lightsail for Research e. IAM

Tópicos

- Não estou autorizado a realizar uma ação no Lightsail for Research

- Quero permitir que pessoas fora da minha casa acessem meus Conta da AWS recursos do Lightsail for Research

Não estou autorizado a realizar uma ação no Lightsail for Research

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta usar o console para ver detalhes sobre um *`my-example-widget`* recurso fictício, mas não tem as permissões fictícias`lightsail:`*`GetWidget`*.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `lightsail:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha casa acessem meus Conta da AWS recursos do Lightsail for Research

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Lightsail for Research é compatível com esses recursos, consulte. Como o Amazon Lightsail for Research trabalha com IAM
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Fornecer acesso a um IAM usuário em outro Conta da AWS de sua propriedade no Guia do IAM usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecer Contas da AWS acesso a terceiros no Guia do IAM usuário.

- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAMusuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.

Validação de conformidade para o Amazon Lightsail for Research

Para saber se um Serviço da AWS está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para HIPAA segurança e conformidade na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos qualificados.

> **Note**
>
> Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a Referência de serviços HIPAA elegíveis.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização ()). ISO

- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso Serviço da AWS fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso Serviço da AWS detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, por exemplo PCIDSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso Serviço da AWS ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Resiliência no Amazon Lightsail para pesquisa

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Além da infraestrutura AWS global, o Lightsail for Research oferece vários recursos para ajudar a suportar suas necessidades de resiliência e backup de dados. Para ter mais informações, consulte Faça backup de computadores e discos virtuais com instantâneos do Lightsail for Research e Crie instantâneos dos computadores ou discos virtuais do Lightsail for Research.

Segurança da infraestrutura no Amazon Lightsail for Research

Como um serviço gerenciado, o Amazon Lightsail for Research é protegido pela segurança AWS da rede global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa API chamadas AWS publicadas para acessar o Lightsail for Research por meio da rede. Os clientes devem oferecer suporte para:

- Segurança da camada de transporte (TLS). Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Suítes de criptografia com sigilo direto perfeito (), como (Ephemeral PFS Diffie-Hellman) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Análise de configuração e vulnerabilidade no Amazon Lightsail for Research

A configuração e os controles de TI são uma responsabilidade compartilhada entre você AWS e você, nosso cliente. Para obter mais informações, consulte o modelo de responsabilidade AWS compartilhada.

Melhores práticas de segurança para o Amazon Lightsail for Research

O Lightsail for Research fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Para evitar possíveis eventos de segurança associados ao seu uso do Lightsail for Research, siga estas melhores práticas:

- Acesse o console do Lightsail for Research autenticando-se no primeiro. AWS Management Console Não compartilhe, compartilhe suas credenciais pessoais do console. Qualquer pessoa na internet pode acessar o console, mas não pode fazer login ou iniciar uma sessão a menos que tenha credenciais válidas para o console.

Histórico do documento para o guia do usuário do Lightsail para Pesquisa

A tabela a seguir descreve as versões de documentação para o Lightsail para Pesquisa.

Alteração	Descrição	Data
Versão inicial	Versão inicial do Guia do usuário do Lightsail para Pesquisa.	28 de fevereiro de 2023

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.