Guida per l'utente

Amazon Lightsail per la ricerca

Amazon Lightsail per la ricerca: Guida per l’utente

Table of Contents

Cos'è Amazon Lightsail for Research?

Con Amazon Lightsail for Research, accademici e ricercatori possono creare potenti computer virtuali nel cloud Amazon Web Services ().AWS Questi computer virtuali sono dotati di applicazioni di ricerca preinstallate, come Scilab. RStudio

Con Lightsail for Research, puoi caricare i dati direttamente da un browser web per iniziare il tuo lavoro. Puoi creare ed eliminare i tuoi computer virtuali in qualsiasi momento, e questo ti consente di accedere su richiesta a potenti risorse di elaborazione.

Paghi solo per il tempo in cui hai bisogno del computer virtuale. Lightsail for Research offre controlli per la gestione del budget che possono arrestare automaticamente il computer quando raggiunge un limite di costo preconfigurato, in modo da non doversi preoccupare di addebiti aggiuntivi.

Tutto ciò che fai nella console Lightsail for Research è supportato da un'API disponibile pubblicamente. Scopri come installare e utilizzare l'API AWS CLIand per Amazon Lightsail.

Prezzi

Con Lightsail for Research, paghi solo per le risorse che crei e utilizzi. Per ulteriori informazioni, consulta i prezzi di Lightsail for Research.

Disponibilità

Lightsail for Research è disponibile nelle AWS stesse regioni di Amazon Lightsail, ad eccezione della regione Stati Uniti orientali (Virginia settentrionale). Lightsail for Research utilizza anche gli stessi endpoint di Lightsail. Per visualizzare le AWS regioni e gli endpoint attualmente supportati per Lightsail, consulta Lightsail Endpoints and Quotas nella Guida generale.AWS

Configurazione di Amazon Lightsail for Research

Se sei un nuovo AWS cliente, completa i prerequisiti di configurazione elencati in questa pagina prima di iniziare a utilizzare Amazon Lightsail for Research.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi Console di gestione AWScome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Tutorial: Inizia a usare i computer virtuali di Lightsail for Research

Usa questo tutorial per iniziare a usare i computer virtuali Amazon Lightsail for Research. Imparerai a creare, connettere e utilizzare un computer virtuale. In Lightsail for Research, un computer virtuale è una workstation di ricerca che puoi creare e gestire in. Cloud AWS I computer virtuali sono basati su istanze Lightsail Linux con sistema operativo Ubuntu. Sul tuo computer virtuale, puoi preconfigurare un'applicazione di ricerca come JupyterLab Scilab e altre. RStudio

Il computer virtuale che crei in questo tutorial comporterà costi di utilizzo dal momento in cui lo crei fino a quando lo elimini. L'eliminazione è il passaggio finale di questo tutorial. Per ulteriori informazioni sui prezzi, consulta la pagina dei prezzi di Lightsail for Research.

Argomenti

Fase 1: completamento dei prerequisiti

Se sei un nuovo AWS cliente, completa i prerequisiti di configurazione prima di iniziare a utilizzare Amazon Lightsail for Research. Per ulteriori informazioni, consulta Configurazione di Amazon Lightsail for Research.

Fase 2: crea un computer virtuale

È possibile creare un computer virtuale utilizzando la console Lightsail for Research come descritto nella procedura seguente. La finalità di questo tutorial è aiutarti ad avviare in modo semplice e rapido il tuo primo computer virtuale. Ti consigliamo inoltre di esplorare le applicazioni e i piani hardware

disponibili. Per ulteriori informazioni, consulta Scegli le immagini delle applicazioni e i piani hardware per Lightsail for Research e Crea un computer virtuale Lightsail for Research.

1. Accedi alla console Lightsail for Research.
2. Nella home page, scegli Crea computer virtuale.
3. Selezionane uno Regione AWS per il tuo computer virtuale.

   Scegli Regione AWS quello più vicino alla tua posizione fisica per ridurre la latenza.
4. Scegli un'applicazione, nota anche come modello nell'API Lightsail.

   L'applicazione scelta viene installata e configurata sul computer virtuale al momento della creazione.
5. Scegli un piano hardware, noto anche come pacchetto nell'API Lightsail.

   I piani hardware offrono diverse quantità di potenza di elaborazione, tra cui core vCPU, memoria, storage e trasferimento dati mensile. Lightsail for Research offre piani standard e piani GPU per computer virtuali. Scegli un piano standard quando i requisiti computazionali dell'attività sono bassi. Scegli un piano GPU quando tale requisito è elevato, ad esempio quando esegui modelli di machine learning o altre attività ad alta intensità di calcolo.
6. Inserisci un nome per il computer virtuale.
7. Scegli Crea computer virtuale nel pannello Riepilogo.

Una volta che il nuovo computer virtuale è attivo e funzionante, procedi con la fase successiva di questo tutorial per scoprire come avviare l'applicazione del computer.

Fase 3: avvio dell'applicazione di un computer virtuale

Dopo aver creato un computer virtuale ed averlo messo In esecuzione, puoi avviare una sessione virtuale nel tuo browser web. Con la sessione, puoi interagire e gestire l'applicazione installata sul tuo computer virtuale.

1. Scegli Computer virtuali nel pannello di navigazione della console Lightsail for Research.
2. Individua il nome del computer virtuale che hai creato nella Fase 1 e scegli Avvia l'applicazione. Ad esempio, Launch. JupyterLab La sessione dell'applicazione si apre in una nuova finestra del browser Web.

> **Important**
>
> Se nel tuo browser web è installato un blocco pop-up, potresti dover consentire i popup dal dominio aws.amazon.com prima di aprire la sessione.

Per informazioni su come connettersi al computer virtuale, continua alla fase successiva di questo tutorial.

Fase 4: collegati al computer virtuale

È possibile connettersi al computer virtuale utilizzando i metodi seguenti:

- Utilizza il client Amazon DCV basato su browser disponibile nella console Lightsail for Research. Con Amazon DCV, puoi utilizzare un'interfaccia utente grafica (GUI) per interagire con la tua applicazione di ricerca e il sistema operativo del tuo computer virtuale.

  Puoi anche accedere all'interfaccia a riga di comando del tuo computer virtuale e trasferire file utilizzando il client Amazon DCV basato su browser.
- Usa un client Secure Shell (SSH) come OpenSSH, PuTTY o Windows Subsystem per Linux per accedere all'interfaccia a riga di comando del tuo computer virtuale. Con un client SSH, puoi modificare script e file di configurazione.
- Utilizza Secure Copy (SCP) per trasferire in modo sicuro i file dal tuo computer locale al tuo computer virtuale. Con SCP, puoi iniziare a lavorare localmente e continuare sul tuo computer virtuale. Puoi anche scaricare file dal tuo computer virtuale per copiare il tuo lavoro sul tuo computer locale.

È necessario fornire la coppia di chiavi del computer virtuale per connettersi ad esso tramite SSH o per trasferire file tramite SCP. Una key pair è un set di credenziali di sicurezza che utilizzi per dimostrare la tua identità quando ti connetti a un computer virtuale Lightsail for Research. Una coppia di chiavi è composta da una chiave privata e una chiave pubblica.

Per ulteriori informazioni sulla connessione al computer virtuale, consulta la documentazione che segue:

- Stabilisci una connessione al protocollo di visualizzazione remota:

  - Accedi a un'applicazione per computer virtuale Lightsail for Research
  - Accedi al sistema operativo del tuo computer virtuale Lightsail for Research
- Stabilisci una connessione SSH o trasferisci i file usando SCP:
  - Richiedi una key pair per un computer virtuale Lightsail for Research
  - Connect a un computer virtuale Lightsail for Research tramite Secure Shell
  - Trasferisci file sui computer virtuali di Lightsail for Research utilizzando Secure Copy

Per ulteriori informazioni sullo storage del computer virtuale, continua alla fase successiva di questo tutorial.

Fase 5: aggiunta di storage al computer virtuale

Lightsail for Research fornisce volumi di archiviazione a livello di blocco (dischi) che è possibile collegare a un computer virtuale. Anche se il computer virtuale è dotato di un disco di sistema, è possibile collegare dischi di archiviazione aggiuntivi in base alle esigenze. È inoltre possibile scollegare un disco da un computer virtuale e collegarlo a un altro computer virtuale.

Quando colleghi un disco al tuo computer virtuale utilizzando la console, Lightsail for Research formatta e monta automaticamente il disco nel tuo sistema operativo. Questo processo richiede alcuni minuti, quindi è necessario verificare che il disco sia nello stato di montaggio Montato prima di iniziare a utilizzarlo.

Per informazioni sulla creazione, il collegamento e la gestione di un disco, consulta la documentazione che segue:

- Crea un disco di archiviazione nella console Lightsail for Research
- Visualizza i dettagli del disco di archiviazione nella console Lightsail for Research
- Aggiungi spazio di archiviazione a un computer virtuale in Lightsail for Research
- Scollegare un disco da un computer virtuale in Lightsail for Research
- Eliminare i dischi di archiviazione inutilizzati in Lightsail for Research

Per ulteriori informazioni sul backup del computer virtuale, continua alla fase successiva di questo tutorial.

Fase 6: Creazione di una snapshot DB

Le istantanee sono una point-in-time copia dei tuoi dati. È possibile creare snapshot dei computer virtuali e utilizzarli come linee di base per creare nuovi computer o per il backup dei dati. Uno snapshot contiene tutti i dati necessari per ripristinare il computer (dal momento in cui lo snapshot è stato acquisito).

Per informazioni sulla creazione e la gestione di snapshot, consulta la documentazione che segue:

- Crea istantanee dei computer o dei dischi virtuali di Lightsail for Research
- Visualizza e gestisci istantanee di computer e dischi virtuali in Lightsail for Research
- Crea un computer o un disco virtuale da uno snapshot
- Eliminare un'istantanea nella console Lightsail for Research

Per ulteriori informazioni sulla cancellazione delle risorse del computer virtuale, continua alla fase successiva di questo tutorial.

Passaggio 7: eseguire l'eliminazione

Dopo aver creato il computer virtuale per questo tutorial, puoi eliminarlo. In questo modo eviti di incorrere in addebiti per il computer virtuale se non ne hai bisogno.

L'eliminazione di un computer virtuale non comporta l'eliminazione degli snapshot associati o dei dischi collegati. Se hai creato snapshot e dischi, dovresti eliminarli manualmente per evitare di incorrere in costi aggiuntivi.

Per salvare il computer virtuale per utilizzarlo in un secondo momento, ma evitare di incorrere in addebiti a tariffe orarie standard, puoi arrestare il computer virtuale anziché eliminarlo. Potrai quindi riavviarlo in un secondo momento. Per ulteriori informazioni, consulta Visualizza i dettagli del computer virtuale di Lightsail for Research. Per ulteriori informazioni sui prezzi, consulta la pagina dei prezzi di Lightsail for Research.

> **Important**
>
> L'eliminazione di una risorsa Lightsail for Research è un'azione permanente. I dati eliminati non possono essere ripristinati. Se pensi che potresti aver bisogno dei dati in un secondo

momento, è consigliabile creare uno snapshot del computer virtuale prima di eliminarli. Per ulteriori informazioni, consulta Creazione di uno snapshot.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Computer virtuali.
3. Seleziona il computer virtuale da eliminare.
4. Scegli Azioni, quindi scegli Elimina computer virtuale.
5. Digita conferma nel blocco di testo. Quindi, scegli Elimina computer virtuale.

Inizia a usare le applicazioni di data science su Lightsail for Research

I seguenti tutorial forniscono informazioni aggiuntive su come iniziare a usare applicazioni specifiche disponibili in Lightsail for Research.

Argomenti

- Avvio e utilizzo JupyterLab su Lightsail for Research
- Avvio e utilizzo RStudio su Lightsail for Research

> **Note**
>
> Un tutorial approfondito per iniziare a usare Lightsail for Research RStudio , pubblicato sul Public Sector Blog. AWS Per ulteriori informazioni, consulta Guida introduttiva ad Amazon Lightsail for Research: un tutorial sull'utilizzo. RStudio

Avvio e utilizzo JupyterLab su Lightsail for Research

In questo tutorial, ti mostriamo come iniziare a gestire e utilizzare il tuo computer JupyterLab virtuale in Amazon Lightsail for Research.

Argomenti

- Fase 1: completamento dei prerequisiti
- Fase 2: (facoltativa) aggiunta di spazio di archiviazione
- Fase 3: caricamento e download di file
- Fase 4: Avviare l' JupyterLab applicazione
- Fase 5: Leggi la JupyterLab documentazione
- Fase 6: (facoltativa) monitoraggio dell'utilizzo e dei costi
- Fase 7: (facoltativa) creazione di una regola di controllo dei costi
- Fase 8: (facoltativa) creazione di uno snapshot
- Fase 9: (facoltativa) arrestare o eliminare il computer virtuale

Fase 1: completamento dei prerequisiti

Crea un computer virtuale utilizzando l' JupyterLab applicazione se non l'hai già fatto. Per ulteriori informazioni, consulta Crea un computer virtuale Lightsail for Research.

Una volta che il nuovo computer virtuale sarà operativo, continua con la sezione di avvio dell' JupyterLab applicazione di questo tutorial.

Fase 2: (facoltativa) aggiunta di spazio di archiviazione

Il computer virtuale è dotato di un disco di sistema. Tuttavia, man mano che le esigenze di archiviazione cambiano, puoi collegare dischi aggiuntivi al computer virtuale per aumentarne lo spazio di archiviazione.

Puoi, inoltre, archiviare i file di lavoro su un disco collegato. È quindi possibile scollegare il disco e collegarlo a un altro computer virtuale per spostare rapidamente i file da un computer all'altro.

In alternativa, puoi creare uno snapshot di un disco collegato contenente i file di lavoro e quindi creare un disco duplicato a partire dallo snapshot. È quindi possibile collegare il nuovo disco duplicato a un altro computer per duplicare il lavoro su diversi computer virtuali. Per ulteriori informazioni, consultare Crea un disco di archiviazione nella console Lightsail for Research e Aggiungi spazio di archiviazione a un computer virtuale in Lightsail for Research.

> **Note**
>
> Quando colleghi un disco al computer virtuale utilizzando la console, Lightsail for Research formatta e monta automaticamente il disco. Questo processo richiede alcuni minuti, quindi è necessario verificare che il disco abbia raggiunto lo stato di montaggio Montato prima di iniziare a utilizzarlo. Per impostazione predefinita, Lightsail for Research monta i dischi nella directory. `/home/lightsail-user/<disk-name>` `<disk-name>`è il nome che hai dato al disco.

Fase 3: caricamento e download di file

Puoi caricare file sul tuo computer JupyterLab virtuale e scaricare file da esso. Per fare ciò, completa la seguente procedura:

1. Procurati una coppia di chiavi da Amazon Lightsail. Per ulteriori informazioni, consulta Richiedi una key pair per un computer virtuale Lightsail for Research.

2. Dopo aver ottenuto la coppia di chiavi, puoi utilizzarla per stabilire una connessione utilizzando l'utilità Secure Copy (SCP). SCP ti consente di caricare e scaricare file utilizzando il prompt dei comandi o il terminale. Per ulteriori informazioni, consulta Trasferisci file sui computer virtuali di Lightsail for Research utilizzando Secure Copy.
3. (Facoltativo) Puoi anche usare la coppia di chiavi per connetterti al tuo computer virtuale con SSH. Per ulteriori informazioni, consulta Connect a un computer virtuale Lightsail for Research tramite Secure Shell.

> **Note**
>
> Puoi anche accedere all'interfaccia a riga di comando del tuo computer virtuale e trasferire file utilizzando il client Amazon DCV basato su browser. Amazon DCV è disponibile nella console Lightsail for Research. Per ulteriori informazioni, consultare Accedi a un'applicazione per computer virtuale Lightsail for Research e Accedi al sistema operativo del tuo computer virtuale Lightsail for Research.

Per gestire i file di progetto in un disco di archiviazione collegato, assicurati di caricarli nella directory di montaggio corretta per il disco collegato. Quando colleghi un disco al tuo computer virtuale utilizzando la console, Lightsail for Research formatta e monta automaticamente il disco nella directory. `/home/lightsail-user/<disk-name>` *`<disk-name>`*è il nome che hai dato al disco.

Fase 4: Avviare l' JupyterLab applicazione

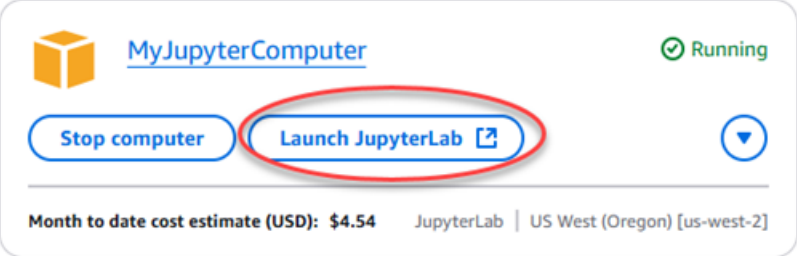
Completa la seguente procedura per avviare l' JupyterLab applicazione sul tuo nuovo computer virtuale.

> **Important**
>
> Non aggiornate il sistema operativo o l' JupyterLab applicazione anche se vi viene richiesto di farlo. Scegli invece l'opzione per chiudere o ignorare queste istruzioni. Inoltre, non modificate nessuno dei file che si trovano nella directory /home/lightsail-admin/. Queste azioni potrebbero rendere il computer virtuale inutilizzabile.

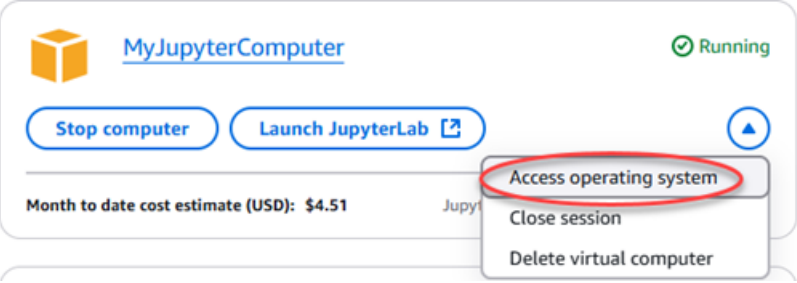
1. Accedi alla console Lightsail for Research.
2. Seleziona Computer virtuali nel riquadro di navigazione per visualizzare i computer virtuali disponibili nell'account.

3. Nella pagina Computer virtuali, trova il tuo computer virtuale e scegli una delle seguenti opzioni per connetterti ad esso:

   a. (Consigliato) Scegliete Avvia JupyterLab per avviare l' JupyterLab applicazione in modalità focalizzata. Se di recente non ti sei connesso al tuo computer virtuale, potresti dover attendere qualche minuto mentre Lightsail for Research prepara la sessione.



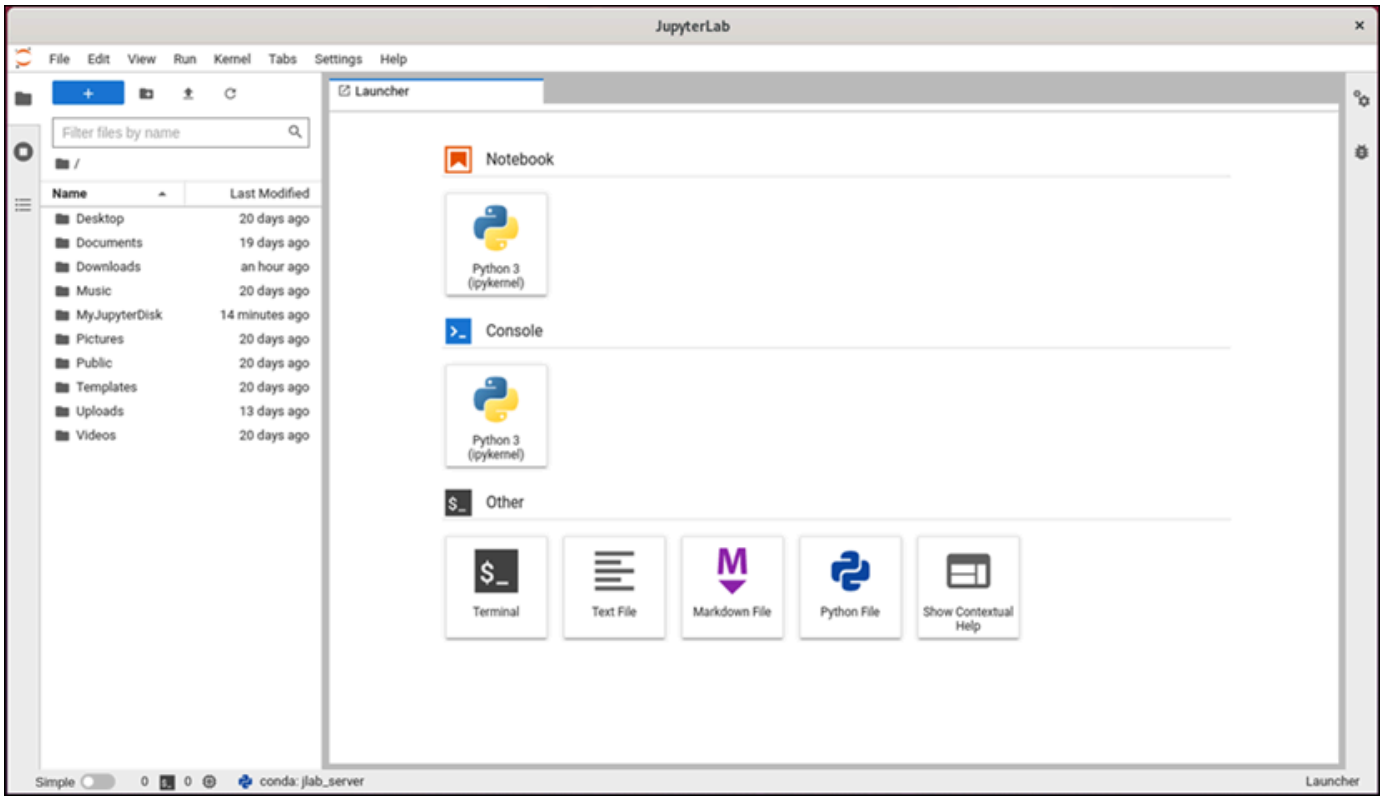
   b. Scegli il menu a discesa per il computer, quindi scegli Accedi al sistema operativo per accedere al desktop del tuo computer virtuale.



Lightsail for Research esegue alcuni comandi per avviare la connessione al protocollo di visualizzazione remota. Dopo alcuni istanti, si apre una nuova finestra della scheda del browser con una connessione desktop virtuale stabilita al computer virtuale. Se avete scelto l'opzione Avvia applicazione, passate al passaggio successivo di questa procedura per aprire un file nell'applicazione. JupyterLab Se hai scelto l'opzione Accedi al sistema operativo, puoi aprire altre applicazioni tramite il desktop di Ubuntu.

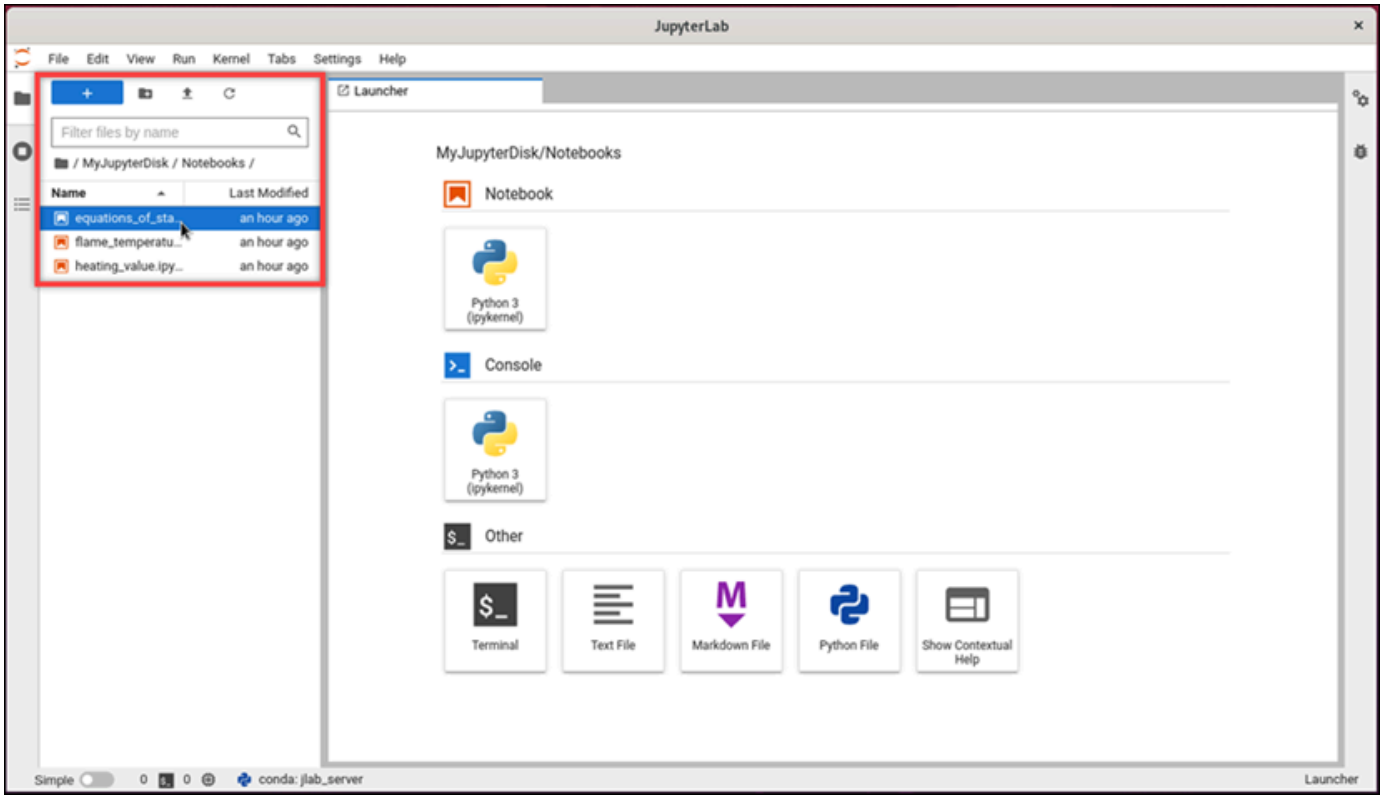
> **Note**
>
> Il tuo browser potrebbe chiederti di autorizzare la condivisione degli appunti. Consentendo ciò, è possibile copiare e incollare tra il computer locale e il computer virtuale.
>
> Ubuntu potrebbe anche richiedere una configurazione iniziale. Segui le istruzioni fino al completamento della configurazione e potrai utilizzare il sistema operativo.

4. L' JupyterLab applicazione si apre. Nel menu di avvio, puoi creare un nuovo notebook, avviare la console, avviare il terminale e creare vari file.

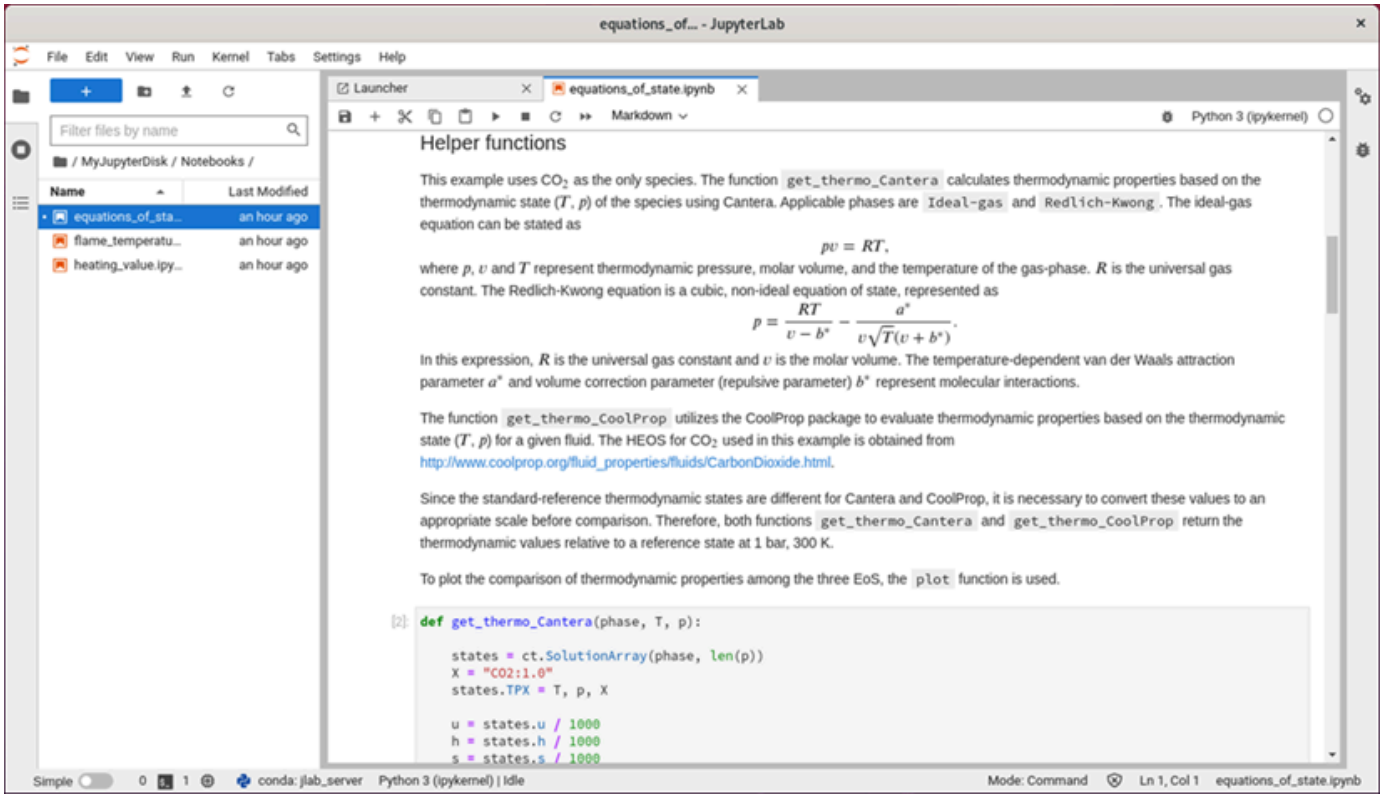


5. Per aprire un file JupyterLab, nel riquadro File Browser, scegliete la directory o la cartella in cui sono archiviati i file del progetto. Quindi scegli il file da aprire.

   Se hai caricato i file di progetto su un disco collegato, cerca la directory in cui è montato il disco. Per impostazione predefinita, Lightsail for Research monta i dischi nella directory. `/home/lightsail-user/<disk-name>` `<disk-name>`è il nome che hai dato al disco. Nell'esempio seguente, la directory `MyJupyterDisk` rappresenta il disco montato e la sottodirectory `Notebooks` contiene i file del nostro notebook Jupyter.



Nell'esempio seguente, abbiamo aperto il file del notebook Jupyter `equations_of_state.ipynb`.



Per ulteriori informazioni sulle nozioni di base, vai alla sezione Fase 5: Leggi la JupyterLab documentazione di questo tutorial.

Fase 5: Leggi la JupyterLab documentazione

Se non li conosci JupyterLab, ti consigliamo di leggere la loro documentazione ufficiale. Sono disponibili le seguenti risorse JupyterLab online:

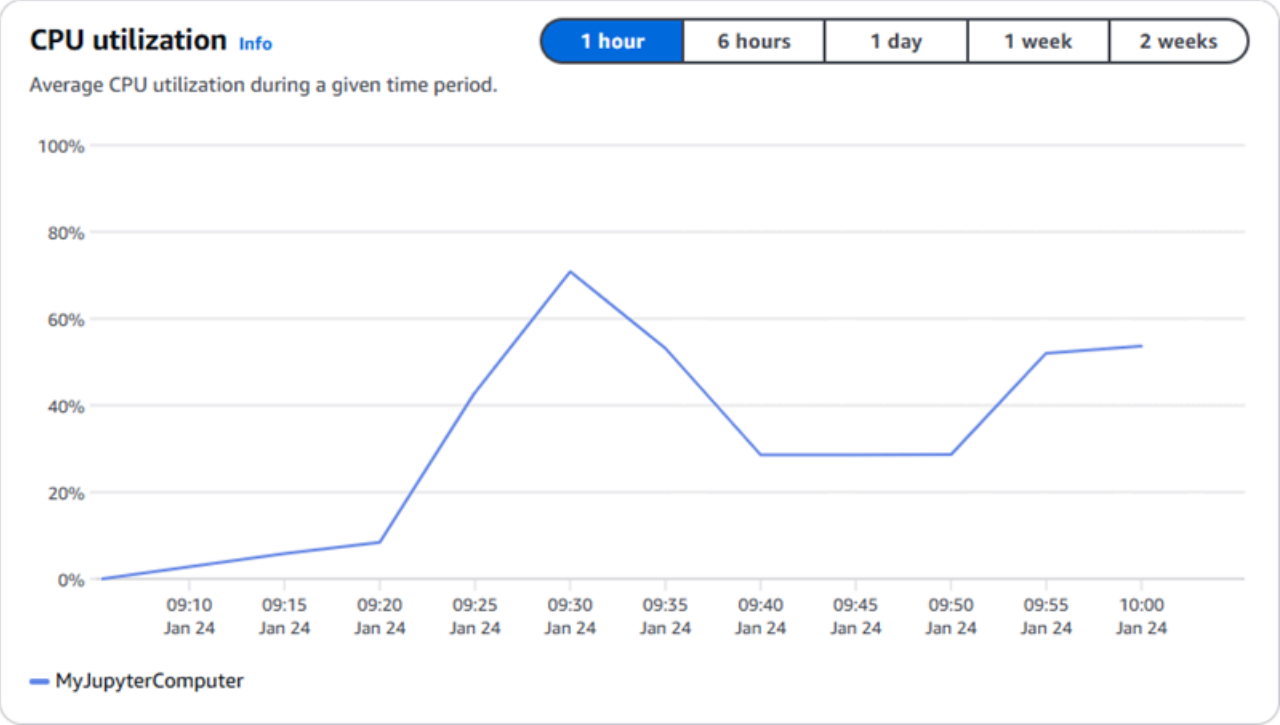
- Documentazione di JupyterLab
- Forum di discussione di Jupyter
- JupyterLab su StackOverflow
- JupyterLab su GitHub

Fase 6: (facoltativa) monitoraggio dell'utilizzo e dei costi

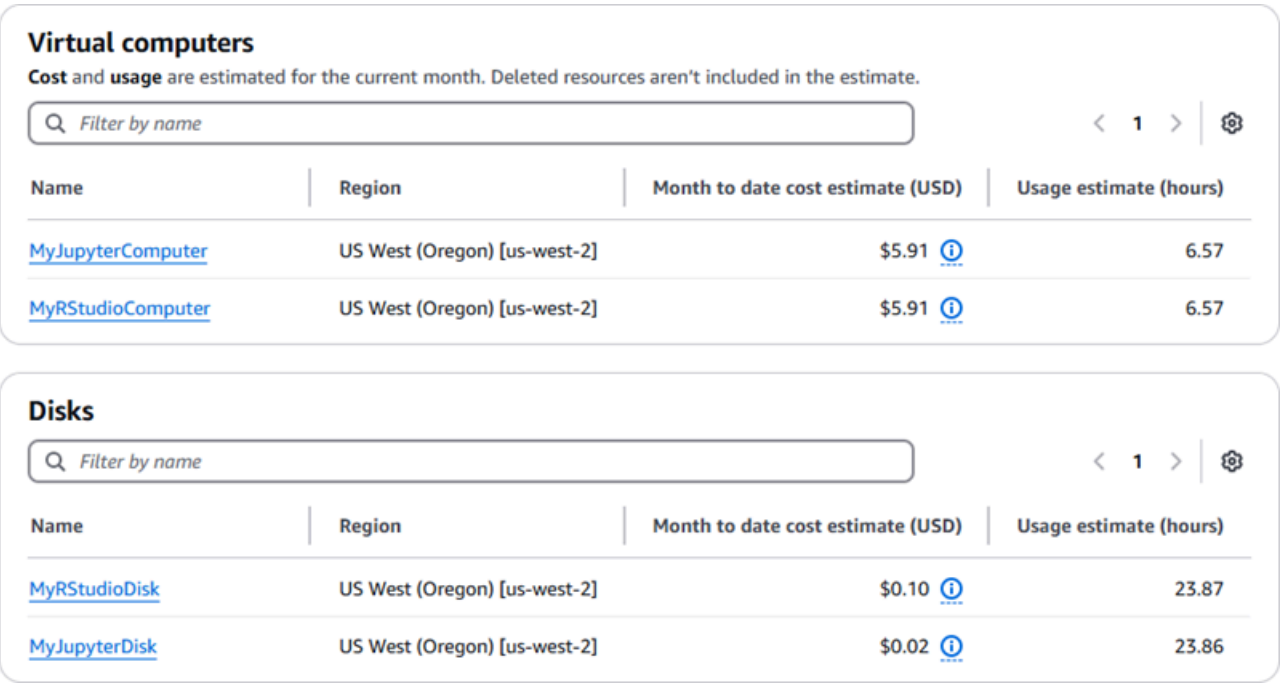
Le stime mensili dei costi e dell'utilizzo delle risorse Lightsail for Research sono visualizzate nelle seguenti aree della console Lightsail for Research.

1. Scegli Computer virtuali nel pannello di navigazione della console Lightsail for Research. La stima dei costi mensili ad oggi per i computer virtuali è elencata sotto ogni computer virtuale in esecuzione.

2. Per visualizzare l'utilizzo della CPU per un computer virtuale, scegli il nome del computer virtuale, quindi scegli la scheda Pannello di controllo.



3. Per visualizzare le stime di costo e utilizzo mensili per tutte le risorse di Lightsail for Research, scegli Utilizzo nel pannello di navigazione.



Fase 7: (facoltativa) creazione di una regola di controllo dei costi

Gestisci l'utilizzo e i costi dei tuoi computer virtuali creando regole di controllo dei costi. È possibile creare una regola Arresta computer virtuale su inattivo che arresta un computer in esecuzione quando raggiunge una determinata percentuale di utilizzo della CPU durante un determinato periodo. Ad esempio, una regola può arrestare automaticamente un computer specifico quando l'utilizzo della CPU è pari o inferiore al 5% per un periodo di 30 minuti. Ciò potrebbe significare che il computer è inattivo e Lightsail for Research lo arresta in modo da non incorrere in addebiti per una risorsa inattiva.

> **Important**
>
> Prima di creare una regola per arrestare il computer virtuale in stato di inattività, ti consigliamo di monitorarne l'utilizzo della CPU per alcuni giorni. Prendi nota dell'utilizzo della CPU quando il computer virtuale è sottoposto a carichi diversi. Ad esempio, durante la compilazione del codice, l'elaborazione di un'operazione e l'inattività. Questo ti aiuterà a determinare una soglia precisa per la regola. Per ulteriori informazioni, consulta la sezione Fase 6: (facoltativa) monitoraggio dell'utilizzo e dei costi di questo tutorial.
>
> Se crei una regola con una soglia di utilizzo della CPU superiore al carico di lavoro, la regola può arrestare consecutivamente il computer virtuale. Ad esempio, se avvii il computer virtuale immediatamente dopo l'interruzione di una regola, la regola si riattiva e il computer si arresta nuovamente.

Le istruzioni dettagliate per la creazione e la gestione delle regole di controllo dei costi sono disponibili nelle seguenti guide:

- Gestisci le regole di controllo dei costi in Lightsail for Research
- Crea regole di controllo dei costi per i tuoi computer virtuali Lightsail for Research
- Eliminare le regole di controllo dei costi per i computer virtuali Lightsail for Research

Fase 8: (facoltativa) creazione di uno snapshot

Le istantanee sono una copia dei tuoi dati. point-in-time È possibile creare snapshot dei computer virtuali e utilizzarli come linee di base per creare nuovi computer o per il backup dei dati. Uno snapshot contiene tutti i dati necessari per ripristinare il computer (dal momento in cui lo snapshot è stato acquisito).

Le istruzioni dettagliate per la creazione e la gestione di snapshot sono disponibili nelle seguenti guide:

- Crea istantanee dei computer o dei dischi virtuali di Lightsail for Research
- Visualizza e gestisci istantanee di computer e dischi virtuali in Lightsail for Research
- Crea un computer o un disco virtuale da uno snapshot
- Eliminare un'istantanea nella console Lightsail for Research

Fase 9: (facoltativa) arrestare o eliminare il computer virtuale

Dopo aver creato il computer virtuale per questo tutorial, puoi eliminarlo. In questo modo eviti di incorrere in addebiti per il computer virtuale se non ne hai bisogno.

L'eliminazione di un computer virtuale non comporta l'eliminazione degli snapshot associati o dei dischi collegati. Se hai creato snapshot e dischi, dovresti eliminarli manualmente per evitare di incorrere in costi aggiuntivi.

Per salvare il computer virtuale per utilizzarlo in un secondo momento, ma evitare di incorrere in addebiti a tariffe orarie standard, puoi arrestare il computer virtuale anziché eliminarlo. Potrai quindi riavviarlo in un secondo momento. Per ulteriori informazioni, consulta Visualizza i dettagli del computer virtuale di Lightsail for Research. Per ulteriori informazioni sui prezzi, consulta la pagina dei prezzi di Lightsail for Research.

> **Important**
>
> L'eliminazione di una risorsa Lightsail for Research è un'azione permanente. I dati eliminati non possono essere ripristinati. Se pensi che potresti aver bisogno dei dati in un secondo momento, è consigliabile creare uno snapshot del computer virtuale prima di eliminarli. Per ulteriori informazioni, consulta Creazione di uno snapshot.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Computer virtuali.
3. Seleziona il computer virtuale da eliminare.
4. Scegli Azioni, quindi scegli Elimina computer virtuale.
5. Digita conferma nel blocco di testo. Quindi, scegli Elimina computer virtuale.

Avvio e utilizzo RStudio su Lightsail for Research

In questo tutorial, ti mostriamo come iniziare a gestire e utilizzare il tuo computer RStudio virtuale in Amazon Lightsail for Research.

> **Note**
>
> Un tutorial approfondito per iniziare a usare Lightsail for Research RStudio , pubblicato sul Public Sector Blog. AWS Per ulteriori informazioni, consulta Guida introduttiva ad Amazon Lightsail for Research: un tutorial sull'utilizzo. RStudio

Argomenti

Fase 1: completamento dei prerequisiti

Crea un computer virtuale utilizzando l' RStudio applicazione, se non l'hai già fatto. Per ulteriori informazioni, consulta Crea un computer virtuale Lightsail for Research.

Fase 2: (facoltativa) aggiunta di spazio di archiviazione

Il computer virtuale è dotato di un disco di sistema. Tuttavia, man mano che le esigenze di archiviazione cambiano, puoi collegare dischi aggiuntivi al computer virtuale per aumentarne lo spazio di archiviazione.

Puoi, inoltre, archiviare i file di lavoro su un disco collegato. È quindi possibile scollegare il disco e collegarlo a un altro computer virtuale per spostare rapidamente i file da un computer all'altro.

In alternativa, puoi creare uno snapshot di un disco collegato contenente i file di lavoro e quindi creare un disco duplicato a partire dall'snapshot. È quindi possibile collegare il nuovo disco duplicato a un altro computer per duplicare il lavoro su diversi computer virtuali. Per ulteriori informazioni, consultare Crea un disco di archiviazione nella console Lightsail for Research e Aggiungi spazio di archiviazione a un computer virtuale in Lightsail for Research.

> **Note**
>
> Quando colleghi un disco al computer virtuale utilizzando la console, Lightsail for Research formatta e monta automaticamente il disco. Questo processo richiede alcuni minuti, quindi è necessario verificare che il disco abbia raggiunto lo stato di montaggio Montato prima di iniziare a utilizzarlo. Per impostazione predefinita, Lightsail for Research monta i dischi `<disk-name>` nella directory con `/home/lightsail-user/<disk-name>` il nome che hai assegnato al disco.

Fase 3: caricamento e download di file

Puoi caricare file sul tuo computer RStudio virtuale e scaricare file da esso. Per fare ciò, completa la seguente procedura:

1. Procurati una coppia di chiavi da Amazon Lightsail. Per ulteriori informazioni, consulta Richiedi una key pair per un computer virtuale Lightsail for Research.
2. Dopo aver ottenuto la coppia di chiavi, puoi utilizzarla per stabilire una connessione utilizzando l'utilità Secure Copy (SCP). SCP ti consente di caricare e scaricare file utilizzando il prompt dei comandi o il terminale. Per ulteriori informazioni, consulta Trasferisci file sui computer virtuali di Lightsail for Research utilizzando Secure Copy.
3. (Facoltativo) Puoi anche usare la coppia di chiavi per connetterti al tuo computer virtuale con SSH. Per ulteriori informazioni, consulta Connect a un computer virtuale Lightsail for Research tramite Secure Shell.

   > **Note**
   >
   > Puoi anche accedere all'interfaccia a riga di comando del tuo computer virtuale e trasferire file utilizzando il client Amazon DCV basato su browser. Amazon DCV è disponibile nella console Lightsail for Research. Per ulteriori informazioni, consultare Accedi a

un'applicazione per computer virtuale Lightsail for Research e Accedi al sistema operativo del tuo computer virtuale Lightsail for Research.

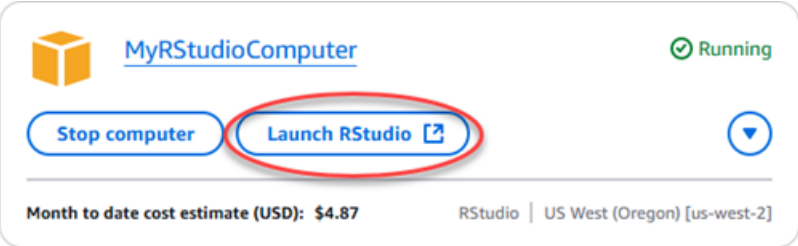
Fase 4: Avvia l'applicazione RStudio

Completa la seguente procedura per avviare l' RStudio applicazione sul tuo nuovo computer virtuale.

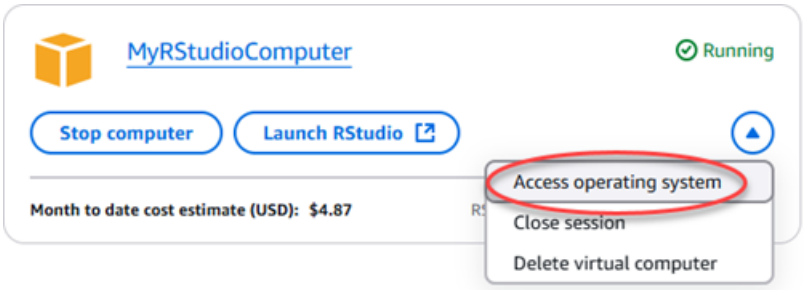
> **Important**
>
> Non aggiornate il sistema operativo o l' RStudio applicazione anche se vi viene richiesto di farlo. Scegli invece l'opzione per chiudere o ignorare queste istruzioni. Inoltre, non modificate nessuno dei file che si trovano nella directory /home/lightsail-admin/. Queste azioni potrebbero rendere il computer virtuale inutilizzabile.

1. Accedi alla console Lightsail for Research.
2. Seleziona Computer virtuali nel riquadro di navigazione per visualizzare i computer virtuali disponibili nell'account.
3. Nella pagina Computer virtuali, trova il tuo computer virtuale e scegli una delle seguenti opzioni per connetterti ad esso:

   a. (Consigliato) Scegliete Avvia RStudio per avviare l' RStudio applicazione in modalità focalizzata. Se di recente non ti sei connesso al tuo computer virtuale, potresti dover attendere qualche minuto mentre Lightsail for Research prepara la sessione.

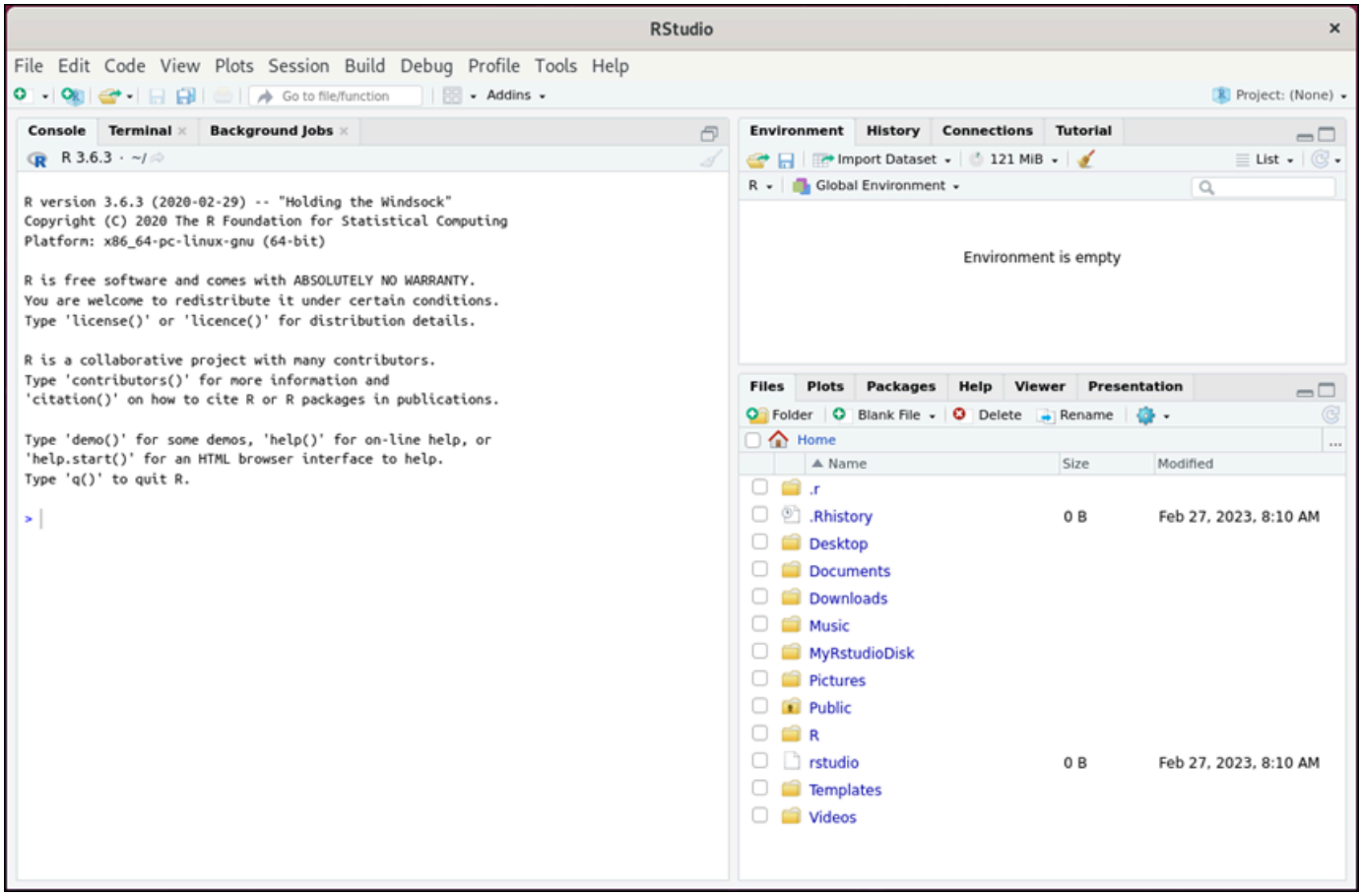
   b. Scegli il menu a discesa per il computer, quindi scegli il Accedi al sistema operativo per accedere al desktop del tuo computer virtuale. Esegui questa operazione se desideri installare un'applicazione diversa sul sistema operativo.



Lightsail for Research esegue alcuni comandi per avviare la connessione al protocollo di visualizzazione remota. Dopo alcuni istanti, si apre una nuova finestra della scheda del browser con una connessione desktop virtuale stabilita al computer virtuale. Se avete scelto l'opzione Avvia applicazione, passate al passaggio successivo di questa procedura per aprire un file nell'applicazione. RStudio Se hai scelto l'opzione Accedi al sistema operativo, puoi aprire altre applicazioni tramite il desktop di Ubuntu.

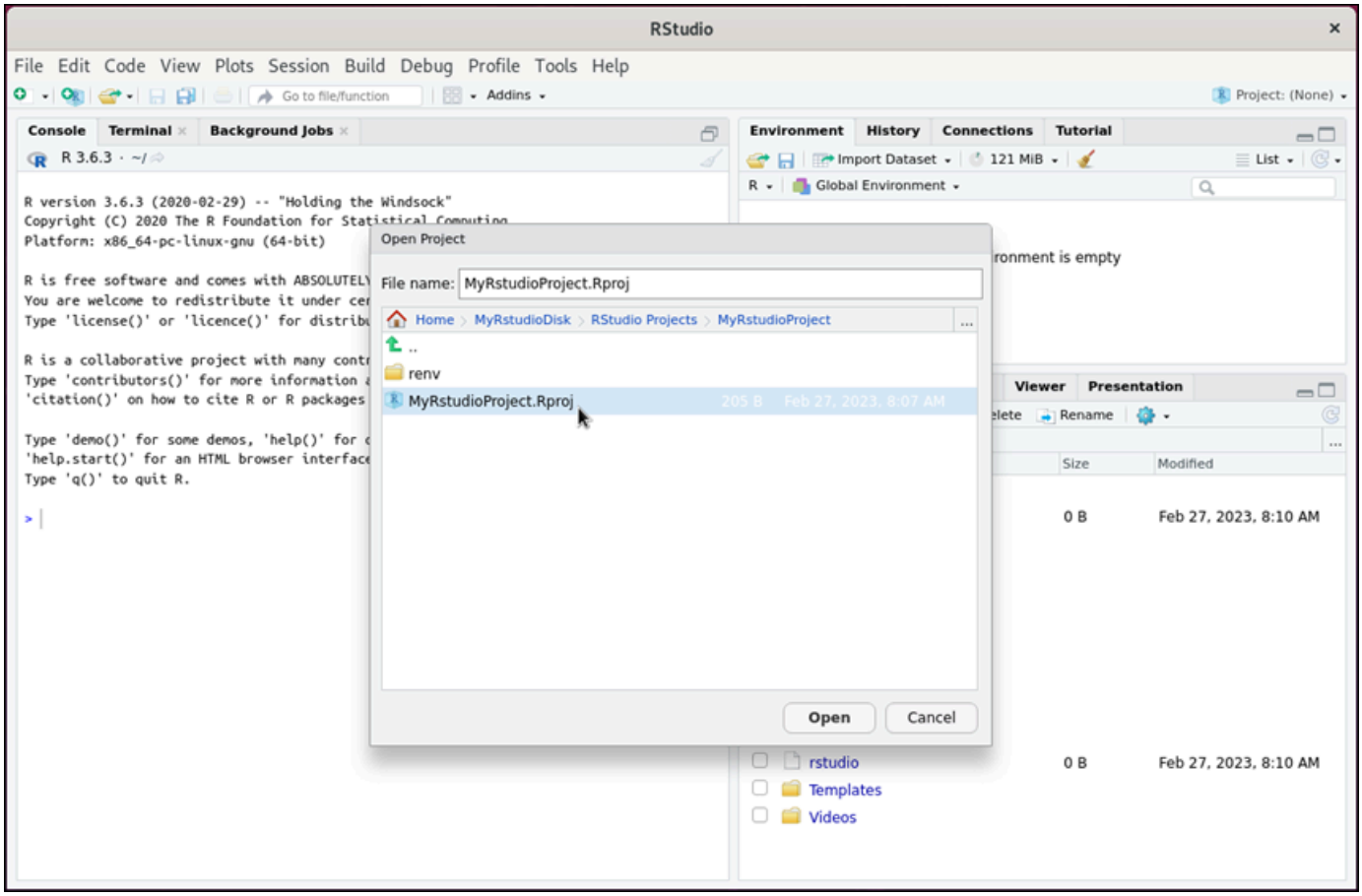
> **Note**
>
> Il tuo browser potrebbe chiederti di autorizzare la condivisione degli appunti. Consentendo ciò, è possibile copiare e incollare tra il computer locale e il computer virtuale.
> Ubuntu potrebbe anche richiedere una configurazione iniziale. Segui le istruzioni fino al completamento della configurazione e potrai utilizzare il sistema operativo.

4. L' RStudio applicazione si apre.

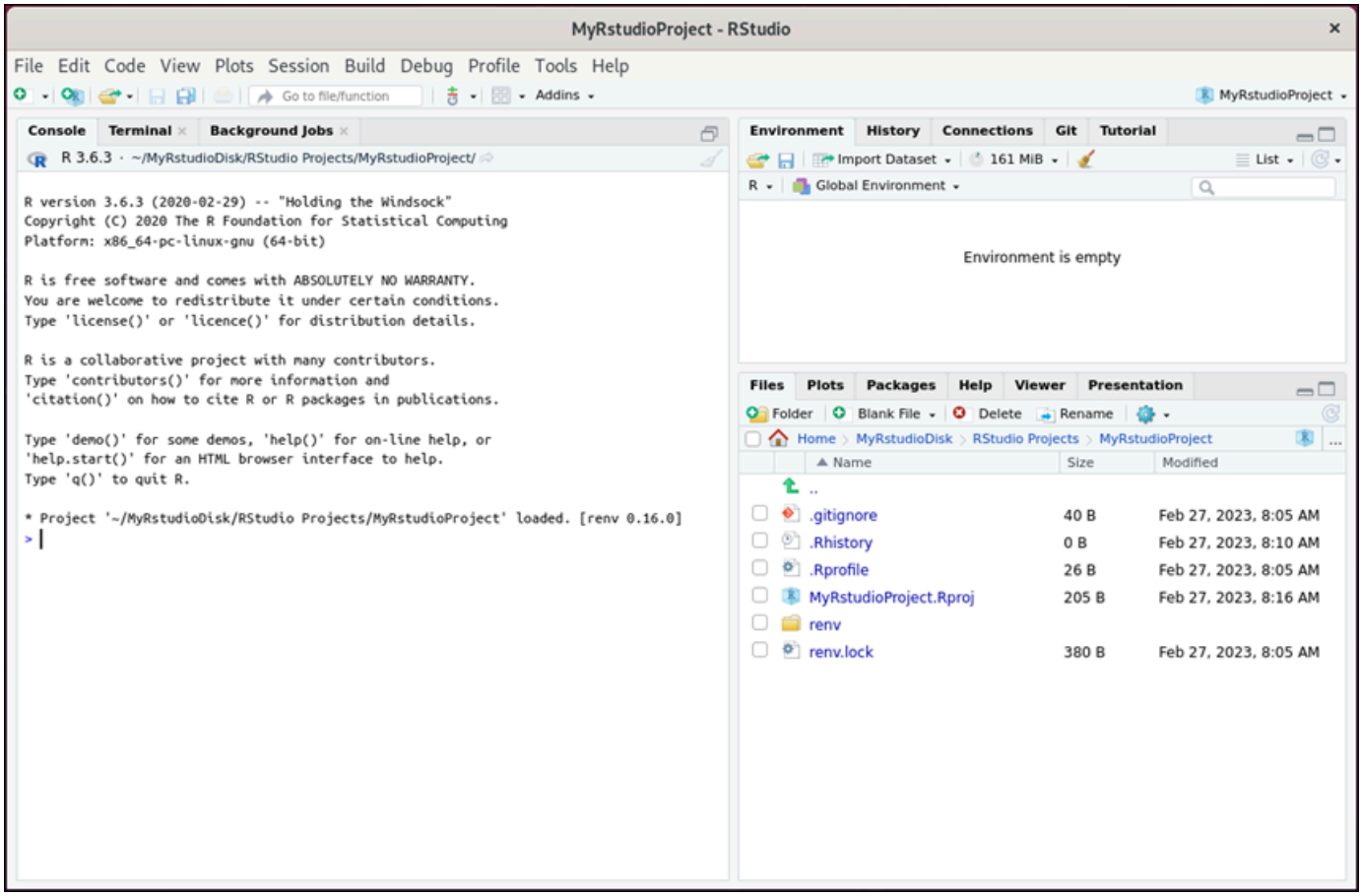


5. Per aprire un progetto in RStudio, scegliete il menu File, quindi scegliete Apri progetto. Seleziona la directory o la cartella in cui sono archiviati i file del progetto. Quindi scegli il file da aprire.

   Se hai caricato i file di progetto su un disco collegato, cerca la directory in cui è montato il disco. Per impostazione predefinita, Lightsail for Research monta i dischi nella directory. `/home/lightsail-user/<disk-name>` `<disk-name>`è il nome che hai dato al disco. Nell'esempio seguente, la `MyRstudioDisk` directory rappresenta il disco montato e la `Projects` sottodirectory contiene i nostri file di RStudio progetto.



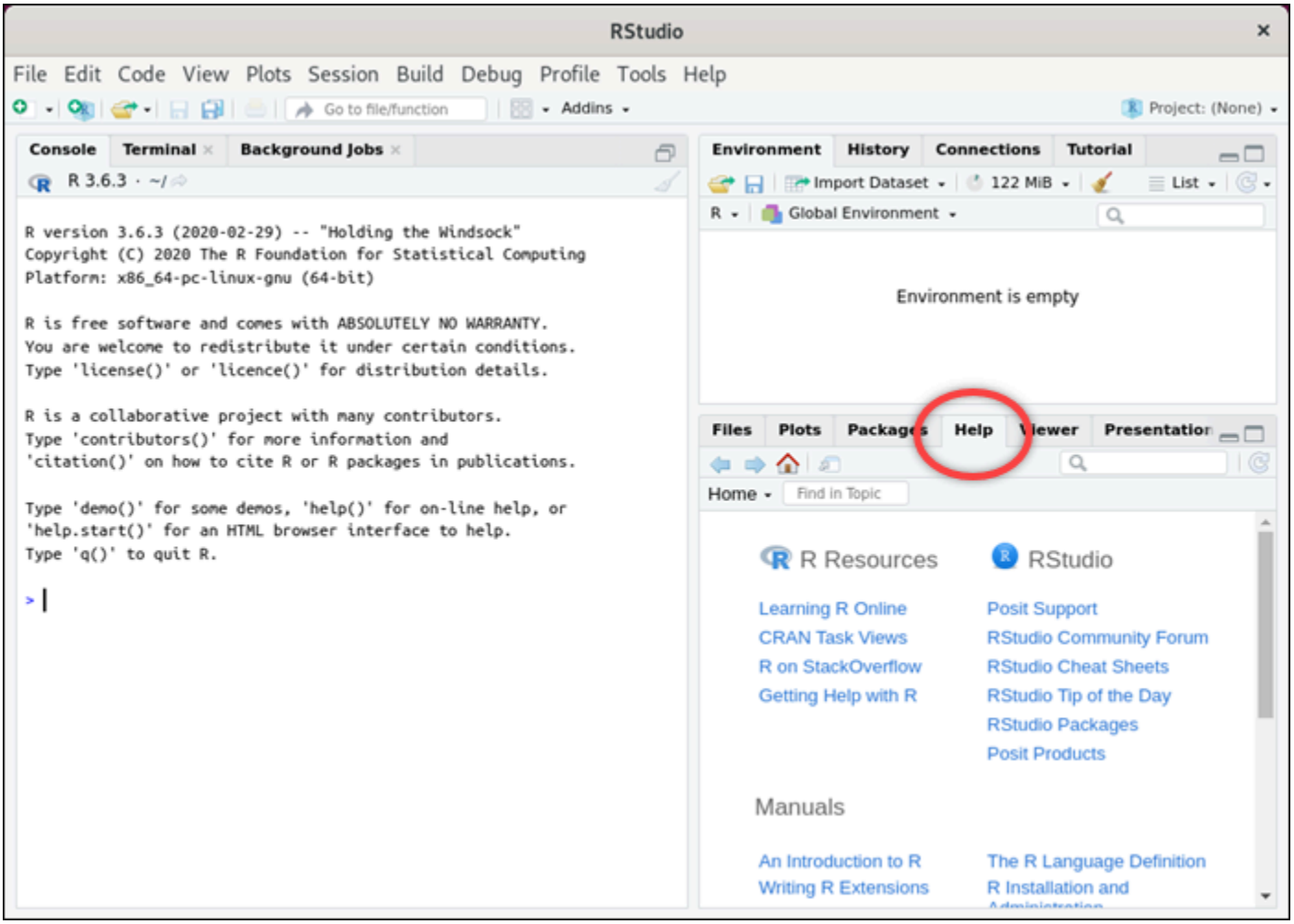
Nell'esempio seguente, abbiamo aperto il file di progetto `MyRstudioProject.Rproj`.



Per informazioni su come iniziare RStudio, continua con la Fase 5: Leggi la RStudio documentazione sezione di questo tutorial.

Fase 5: Leggi la RStudio documentazione

L' RStudio applicazione è fornita in bundle con un pacchetto di documentazione completo. Per iniziare a imparare RStudio, ti consigliamo di accedere alla scheda Aiuto RStudio come mostrato nell'esempio seguente.



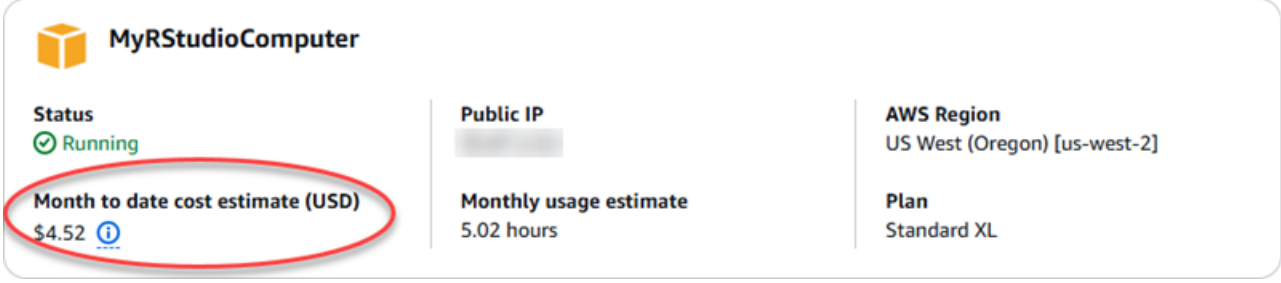
Sono disponibili anche le seguenti risorse RStudio online:

- Imparare R online
- R su StackOverflow
- Utilizzo della Guida con R
- Supporto Posit
- RStudioForum della comunità
- RStudio Cheat sheet
- RStudio Suggerimento del giorno (Twitter)
- RStudioPacchetti

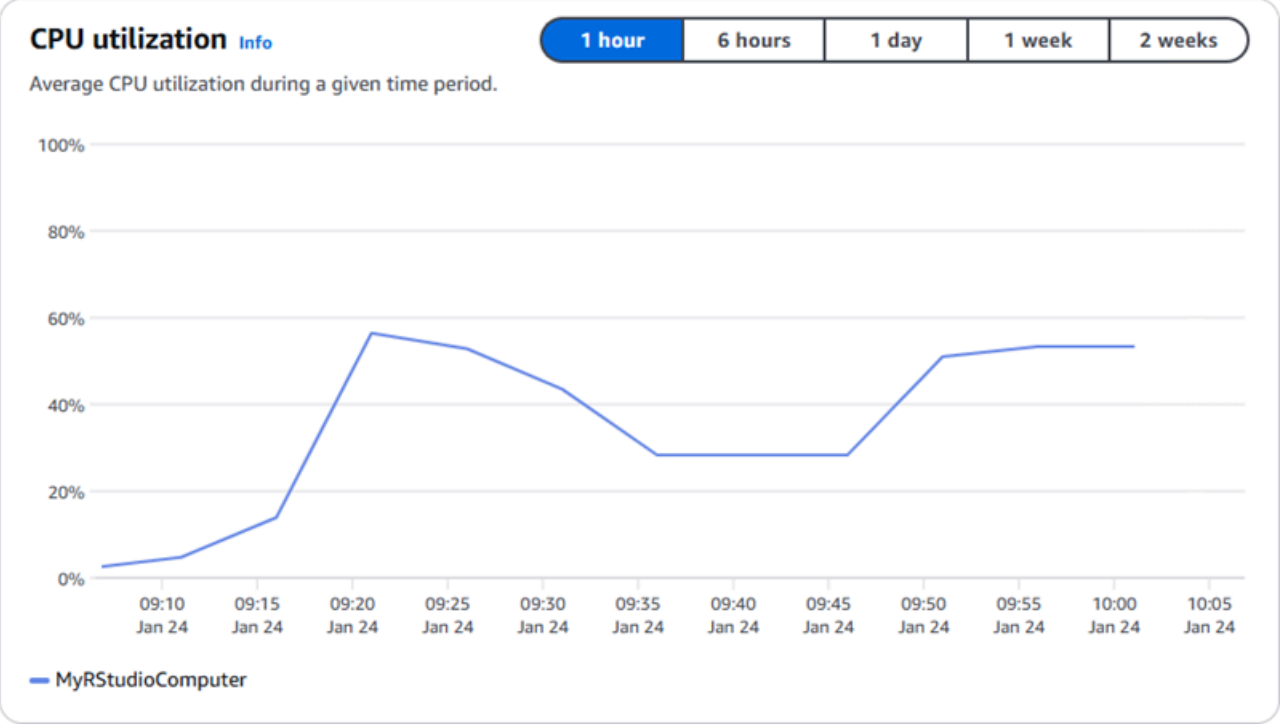
Fase 6: (facoltativa) monitoraggio dell'utilizzo e dei costi

Le stime mensili dei costi e dell'utilizzo delle risorse Lightsail for Research sono visualizzate nelle seguenti aree della console Lightsail for Research.

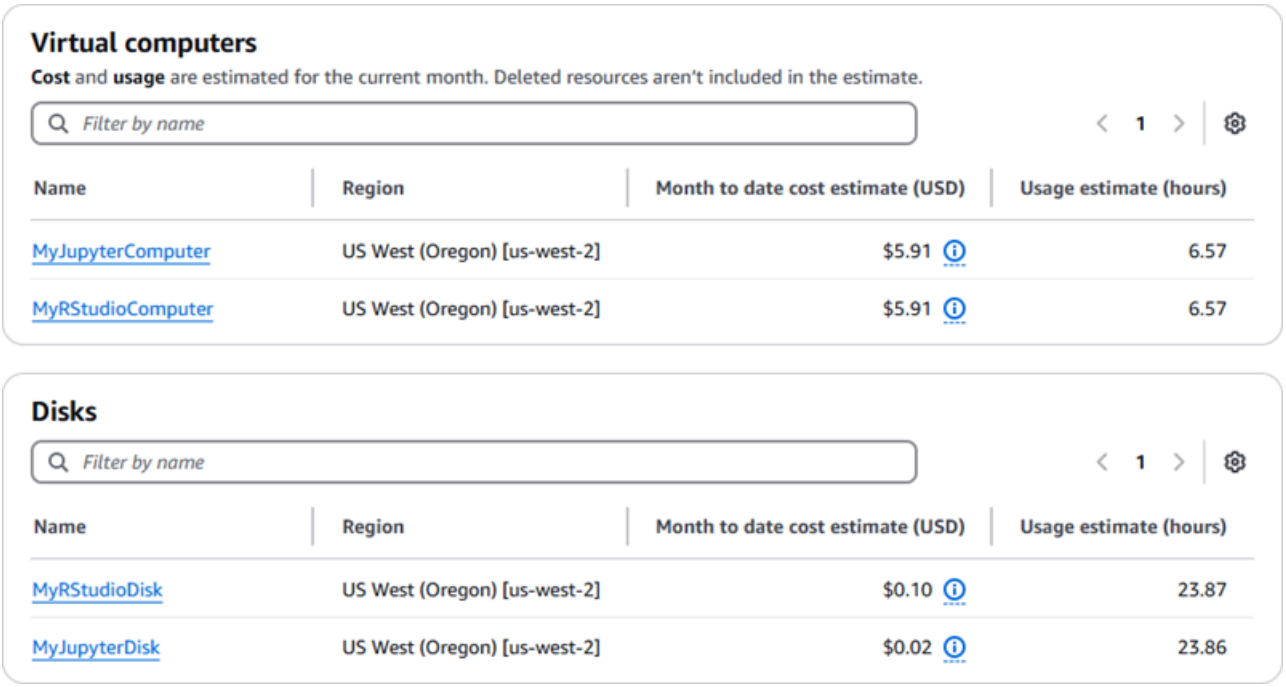
1. Scegli Computer virtuali nel pannello di navigazione della console Lightsail for Research. La stima dei costi mensili ad oggi per i computer virtuali è elencata sotto ogni computer virtuale in esecuzione.



2. Per visualizzare l'utilizzo della CPU per un computer virtuale, scegli il nome del computer virtuale, quindi scegli la scheda Pannello di controllo.



3. Per visualizzare le stime di costo e utilizzo mensili per tutte le risorse di Lightsail for Research, scegli Utilizzo nel pannello di navigazione.



Fase 7: (facoltativa) creazione di una regola di controllo dei costi

Gestisci l'utilizzo e i costi dei tuoi computer virtuali creando regole di controllo dei costi. È possibile creare una regola Arresta computer virtuale su inattivo che arresta un computer in esecuzione quando raggiunge una determinata percentuale di utilizzo della CPU durante un determinato periodo. Ad esempio, una regola può arrestare automaticamente un computer specifico quando l'utilizzo della CPU è pari o inferiore al 5% per un periodo di 30 minuti. Ciò potrebbe significare che il computer è inattivo e Lightsail for Research lo arresta in modo da non incorrere in addebiti per una risorsa inattiva.

Important

Prima di creare una regola per arrestare il computer virtuale in stato di inattività, ti consigliamo di monitorarne l'utilizzo della CPU per alcuni giorni. Prendi nota dell'utilizzo della CPU quando il computer virtuale è sottoposto a carichi diversi. Ad esempio, durante la compilazione del codice, l'elaborazione di un'operazione e l'inattività. Questo ti aiuterà a determinare una soglia precisa per la regola. Per ulteriori informazioni, consulta la sezione Fase 6: (facoltativa) monitoraggio dell'utilizzo e dei costi di questo tutorial.

Se crei una regola con una soglia di utilizzo della CPU superiore al carico di lavoro, la regola può arrestare consecutivamente il computer virtuale. Ad esempio, se avvii il computer virtuale

immediatamente dopo l'interruzione di una regola, la regola si riattiva e il computer si arresta nuovamente.

Le istruzioni dettagliate per la creazione e la gestione delle regole di controllo dei costi sono disponibili nelle seguenti guide:

- Gestisci le regole di controllo dei costi in Lightsail for Research
- Crea regole di controllo dei costi per i tuoi computer virtuali Lightsail for Research
- Eliminare le regole di controllo dei costi per i computer virtuali Lightsail for Research

Fase 8: (facoltativa) creazione di uno snapshot

Le istantanee sono una copia dei tuoi dati. point-in-time È possibile creare snapshot dei computer virtuali e utilizzarli come linee di base per creare nuovi computer o per il backup dei dati. Uno snapshot contiene tutti i dati necessari per ripristinare il computer (dal momento in cui lo snapshot è stato acquisito).

Le istruzioni dettagliate per la creazione e la gestione di snapshot sono disponibili nelle seguenti guide:

- Crea istantanee dei computer o dei dischi virtuali di Lightsail for Research
- Visualizza e gestisci istantanee di computer e dischi virtuali in Lightsail for Research
- Crea un computer o un disco virtuale da uno snapshot
- Eliminare un'istantanea nella console Lightsail for Research

Fase 9: (facoltativa) arrestare o eliminare il computer virtuale

Dopo aver creato il computer virtuale per questo tutorial, puoi eliminarlo. In questo modo eviti di incorrere in addebiti per il computer virtuale se non ne hai bisogno.

L'eliminazione di un computer virtuale non comporta l'eliminazione degli snapshot associati o dei dischi collegati. Se hai creato snapshot e dischi, dovresti eliminarli manualmente per evitare di incorrere in costi aggiuntivi.

Per salvare il computer virtuale per utilizzarlo in un secondo momento, ma evitare di incorrere in addebiti a tariffe orarie standard, puoi arrestare il computer virtuale anziché eliminarlo. Potrai

quindi riavviarlo in un secondo momento. Per ulteriori informazioni, consulta Visualizza i dettagli del computer virtuale di Lightsail for Research. Per ulteriori informazioni sui prezzi, consulta la pagina dei prezzi di Lightsail for Research.

> **Important**
>
> L'eliminazione di una risorsa Lightsail for Research è un'azione permanente. I dati eliminati non possono essere ripristinati. Se pensi che potresti aver bisogno dei dati in un secondo momento, è consigliabile creare uno snapshot del computer virtuale prima di eliminarli. Per ulteriori informazioni, consulta Creazione di uno snapshot.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Computer virtuali.
3. Seleziona il computer virtuale da eliminare.
4. Scegli Azioni, quindi scegli Elimina computer virtuale.
5. Digita conferma nel blocco di testo. Quindi, scegli Elimina computer virtuale.

Crea e gestisci computer virtuali su Lightsail for Research

Con Amazon Lightsail for Research, puoi creare computer virtuali in. Cloud AWS

Quando si crea un computer virtuale, si sceglie un'applicazione e un piano hardware da utilizzare. È possibile impostare un limite di spesa per il computer virtuale e scegliere cosa succede quando il computer virtuale raggiunge tale limite. Ad esempio, puoi scegliere di arrestare automaticamente il computer virtuale in modo che non ti venga addebitato un importo superiore al budget configurato.

> **Important**
>
> A partire dal 22 marzo 2024, i computer virtuali di Lightsail for Research verranno IMDSv2 applicati per impostazione predefinita.

Argomenti

Scegli le immagini delle applicazioni e i piani hardware per Lightsail for Research

Quando crei un computer virtuale Amazon Lightsail for Research, selezioni un'applicazione e un piano hardware (piano) per esso.

Un'applicazione fornisce una configurazione software (ad esempio, un'applicazione e un sistema operativo). Un piano fornisce l'hardware del computer virtuale, ad esempio il numero di v, la memoriaCPUs, lo spazio di archiviazione e l'indennità mensile per il trasferimento dei dati. Insieme, l'applicazione e il piano costituiscono la configurazione del computer virtuale.

> **Note**
>
> Non è possibile modificare l'applicazione o il piano del computer virtuale dopo la creazione. Tuttavia, è possibile creare uno snapshot del computer virtuale e quindi scegliere un nuovo piano quando si crea un nuovo computer virtuale dallo snapshot. Per ulteriori informazioni sugli snapshot, consulta Backup di computer e dischi virtuali con le istantanee di Lightsail for Research.

Argomenti

Applicazioni

Amazon Lightsail for Research fornisce e gestisce immagini di macchine che contengono l'applicazione e il sistema operativo necessari per avviare un computer virtuale. Puoi scegliere da un elenco di applicazioni quando crei un computer virtuale in Lightsail for Research. Tutte le immagini delle applicazioni Lightsail for Research utilizzano il sistema operativo Ubuntu (Linux).

Le seguenti applicazioni sono disponibili in Lightsail for Research:

- JupyterLab— JupyterLab è un ambiente di sviluppo integrato (IDE) basato sul web per notebook, codice e dati. Con la sua interfaccia flessibile è possibile configurare e organizzare i flussi di lavoro nell'ambito del data science, del calcolo scientifico, del giornalismo computazionale e del machine learning. Per ulteriori informazioni, consulta la documentazione del progetto Jupyter.
- RStudio— RStudio è un ambiente di sviluppo integrato (IDE) open source per R, un linguaggio di programmazione per calcolo statistico e grafica e Python. Combina un editor di codice sorgente, strumenti di automazione delle build e un debugger, oltre a strumenti per il plottaggio e la gestione dell'area di lavoro. Per ulteriori informazioni, consulta l'RStudioIDE.
- VSCodium— VSCodium è una distribuzione binaria gestita dalla comunità dell'editor VS Code di Microsoft. Per ulteriori informazioni, consulta VSCodium.

- Scilab — Scilab è un pacchetto computazionale numerico open source e un linguaggio di programmazione di alto livello orientata al numero. Per ulteriori informazioni, consulta Scilab.
- Ubuntu 20.04 LTS — Ubuntu è una distribuzione Linux open source basata su Debian. Snello, veloce e potente, Ubuntu Server offre servizi in modo affidabile, prevedibile ed economico. È un'ottima base su cui costruire i tuoi computer virtuali. Per ulteriori informazioni, consulta Rilasci Ubuntu.

Piani

Un piano fornisce le specifiche hardware e determina il prezzo del computer virtuale Lightsail for Research. Un piano include una quantità fissa di memoria (RAM), elaborazione (v), spazio per il volume di archiviazione (discoCPUs) basato su SSD e un'indennità mensile per il trasferimento dei dati. I piani vengono addebitati su base oraria e su richiesta, quindi paghi solo per il tempo in cui il computer virtuale è in esecuzione.

Il piano scelto può dipendere dalle risorse richieste dal carico di lavoro. Lightsail for Research offre i seguenti tipi di piani:

- Standard: i piani standard sono a calcolo ottimizzato e rappresentano la soluzione ideale per le applicazioni basate su calcolo che usano processori a prestazioni elevate.
- GPU: i piani GPU offrono una piattaforma economica, a elevate prestazioni e per l'elaborazione generale su GPU. Puoi utilizzare questi piani per accelerare le applicazioni e i carichi di lavoro scientifici, tecnici e di rendering.

Piani standard

Di seguito sono riportate le specifiche hardware dei piani standard disponibili in Lightsail for Research.

Nome del piano	v CPUs	Memoria	Spazio di archiviazione	Indennità mensile per il trasferimento dei dati
Standard XL	4	8 GB	50 GB	512 GB
Standard 2XL	8	16 GB	50 GB	512 GB

Standard 4XL	16	32 GB	50 GB	512 GB

Piani GPU

Di seguito sono riportate le specifiche hardware dei piani GPU disponibili in Lightsail for Research.

Nome del piano	v CPUs	Memoria	Spazio di archiviazione	Indennità mensile per il trasferimento dei dati
GPU XL	4	16 GB	50 GB	1 TB
GPU 2XL	8	32 GB	50 GB	1 TB
GPU 4XL	16	64 GB	50 GB	1 TB

Crea un computer virtuale Lightsail for Research

Completa i seguenti passaggi per creare un computer virtuale Lightsail for Research che esegue un'applicazione.

1. Accedi alla console Lightsail for Research.
2. Nella home page, scegli Crea computer virtuale.
3. Selezionane uno Regione AWS per il tuo computer virtuale vicino alla tua posizione fisica.
4. Scegli un'applicazione e un piano hardware. Per ulteriori informazioni, consulta Scegli le immagini delle applicazioni e i piani hardware per Lightsail for Research.
5. Inserisci un nome per il computer virtuale. I caratteri validi includono caratteri alfanumerici, numeri, punti, trattini e trattini bassi.

   I nomi dei computer virtuali devono inoltre soddisfare i seguenti requisiti:

   - Sii unico Regione AWS in ognuno dei tuoi account Lightsail for Research.
   - Devono contenere da 2 a 255 caratteri.
   - Devono iniziare e terminare con un carattere alfanumerico o un numero.

6. Scegli Crea computer virtuale nel pannello Riepilogo.

In pochi minuti, il tuo computer virtuale Lightsail for Research è pronto e puoi connetterti ad esso tramite una sessione di interfaccia grafica utente (GUI). Per ulteriori informazioni sulla connessione al computer virtuale Lightsail for Research, consulta. Accedi a un'applicazione per computer virtuale Lightsail for Research

> **Important**
>
> Per impostazione predefinita, i computer virtuali appena creati dispongono di una serie di porte firewall aperte. Per ulteriori informazioni su queste porte, consulta Gestione delle porte firewall per i computer virtuali Lightsail for Research.

Visualizza i dettagli del computer virtuale di Lightsail for Research

Completa i seguenti passaggi per visualizzare un elenco di computer virtuali e i relativi dettagli nel tuo account Lightsail for Research.

1. Accedi alla console Lightsail for Research.
2. Scegli Computer virtuali nel riquadro di navigazione per visualizzare un elenco dei computer virtuali presenti nel tuo account.

Scegli il nome di un computer virtuale per accedere alla relativa pagina di gestione. Di seguito sono riportate le informazioni fornite dalla pagina di gestione:

- Nome del computer virtuale: il nome del computer virtuale.
- Stato: il computer virtuale può avere uno dei seguenti codici di stato:
  - Creazione in corso
  - In esecuzione
  - In arresto
  - Arrestato
  - Sconosciuto
- Regione AWS— Il Regione AWS computer virtuale in cui è stato creato.
- Applicazione e hardware: l'applicazione e il piano hardware del computer virtuale.

- Stima dell'utilizzo mensile: l'utilizzo orario stimato per questo computer virtuale, per il ciclo di fatturazione corrente.
- Stima dei costi da inizio mese: il costo stimato (in USD) per il computer virtuale per il ciclo di fatturazione corrente.
- Pannello di controllo: dalla scheda Dashboard, è possibile avviare una sessione per accedere all'applicazione del computer virtuale. È inoltre possibile visualizzare l'utilizzo della CPU. L'utilizzo della CPU identifica la potenza di elaborazione utilizzata dalle applicazioni del computer virtuale. Ogni punto dati mostrato nel grafico rappresenta l'utilizzo medio della CPU in un periodo di tempo.
- Regole di controllo dei costi: regole definite dall'utente per aiutare a gestire l'utilizzo e i costi del computer virtuale.
- Utilizzo del computer virtuale: una stima dei costi e dell'utilizzo per un determinato ciclo di fatturazione. Puoi filtrarlo per data e ora.
- Archiviazione: crea, collega e scollega i dischi dei computer virtuali dalla scheda Archiviazione. Un disco è un volume di archiviazione che puoi collegare a un computer virtuale e montare come disco rigido.
- Tag: gestisci i tag del tuo computer virtuale dalla scheda Tag. Un tag è un'etichetta che si assegna a una AWS risorsa. Ciascun tag è formato da una chiave e da un valore facoltativo. Puoi utilizzare i tag per cercare e filtrare le tue risorse o tenere traccia AWS dei costi.

Accedi a un'applicazione per computer virtuale Lightsail for Research

Completa i seguenti passaggi per avviare l'applicazione in esecuzione sul tuo computer virtuale Lightsail for Research.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Computer virtuali.
3. Individua il nome del computer virtuale da cui desideri avviare l'applicazione.

> **Note**
>
> Se il computer virtuale è fermo, scegli innanzitutto il pulsante Avvia computer per accenderlo.

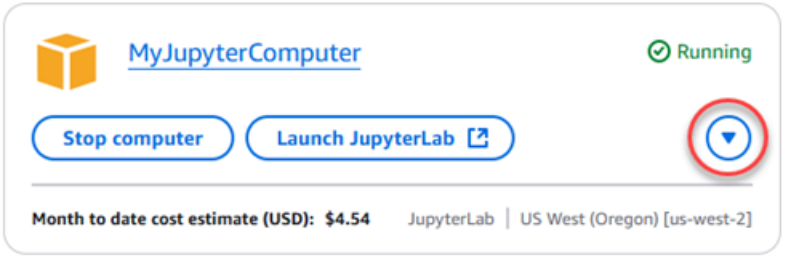
4. Scegli Avvia l'applicazione. Ad esempio, Launch. JupyterLab Una sessione dell'applicazione si aprirà in una nuova finestra del browser Web.

> **Important**
>
> Se nel tuo browser web è installato un blocco pop-up, potresti dover consentire i popup dal dominio aws.amazon.com prima di aprire la sessione.

Accedi al sistema operativo del tuo computer virtuale Lightsail for Research

Completa i seguenti passaggi per accedere al sistema operativo del tuo computer virtuale Lightsail for Research.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Computer virtuali.
3. Individua il nome del tuo computer virtuale, quindi scegli il menu a discesa del pulsante delle azioni sotto lo stato del computer.



> **Note**
>
> Se il computer virtuale è fermo, scegli prima il pulsante Avvio per accenderlo.

4. Scegli il Accedi al sistema operativo. Una sessione del sistema operativo si apre in una nuova finestra del browser.

> **Important**
>
> Se nel tuo browser web è installato un blocco pop-up, potresti dover consentire i popup dal dominio aws.amazon.com prima di aprire la sessione.

Gestione delle porte firewall per i computer virtuali Lightsail for Research

Un firewall in Amazon Lightsail for Research controlla il traffico autorizzato a connettersi al tuo computer virtuale. Aggiungi regole al firewall del tuo computer virtuale che specificano il protocollo, le porte e la fonte IPv4 o IPv6 gli indirizzi a cui è consentito connettersi. Le regole dei gruppi di sicurezza sono sempre permissive; non è possibile creare regole che negano l'accesso. Puoi aggiungere regole al firewall del computer virtuale per consentire al traffico di raggiungere il computer virtuale. Ogni computer virtuale dispone di due firewall, uno per IPv4 gli indirizzi e l'altro per IPv6 gli indirizzi. I firewall sono indipendenti l'uno dall'altro e contengono un set preconfigurato di regole che filtrano il traffico in entrata nell'istanza.

Protocolli

Un protocollo è il formato in cui i dati vengono trasmessi tra due computer. Puoi specificare i seguenti protocolli in una regola del firewall:

- Il protocollo TCP (Transmission Contact Protocol) viene utilizzato principalmente per stabilire e mantenere una connessione tra i client e l'applicazione in esecuzione sul computer virtuale. Si tratta di un protocollo ampiamente utilizzato e che è possibile specificare spesso nelle regole del firewall.
- UDP (User Datagram Protocol) viene utilizzato principalmente per stabilire connessioni a bassa latenza e tolleranza delle perdite tra i client e l'applicazione in esecuzione sul computer virtuale. È ideale per applicazioni di rete in cui la latenza percepita è fondamentale, come giochi, voce e comunicazioni video.
- Internet Control Message Protocol (ICMP) viene utilizzato principalmente per diagnosticare problemi di comunicazione di rete, ad esempio per determinare se i dati raggiungono la destinazione desiderata in modo tempestivo. È ideale per l'utilità Ping, che è possibile utilizzare per testare la velocità della connessione tra il computer locale e quello virtuale. Riporta quanto tempo impiegano i dati per raggiungere il computer virtuale e tornare al computer locale.

- Tutto viene utilizzato per consentire a tutto il traffico di protocollo di fluire nel tuo computer virtuale. Specificare questo protocollo quando non si è sicuri di quale specificare. Questo include tutti i protocolli Internet, non solo quelli specificati qui. Per ulteriori informazioni, consulta Numeri di protocollo nel sito Web Internet Assigned Numbers Authority.

Porte

Analogamente alle porte fisiche del computer, che consentono al computer di comunicare con periferiche quali tastiera e mouse, le porte firewall fungono da endpoint di comunicazione Internet per il computer virtuale. Quando un client cerca di connettersi con il computer virtuale, esporrà una porta per stabilire la comunicazione.

Le porte che è possibile specificare in una regola firewall possono variare da 0 a 65535. Quando si crea una regola firewall per consentire a un client di stabilire una connessione con il computer virtuale, si specifica il protocollo da utilizzare. È inoltre possibile specificare i numeri di porta tramite i quali è possibile stabilire la connessione e gli indirizzi IP autorizzati a stabilire una connessione.

Le seguenti porte sono aperte per impostazione predefinita per i computer virtuali appena creati.

- TCP
  - 22 - Utilizzata per Secure Shell (SSH).
  - 80 - Utilizzata per Hypertext Transfer Protocol (HTTP).
  - 443 - Utilizzata per Hypertext Transfer Protocol Secure (HTTPS).
  - 8443 - Utilizzata per Hypertext Transfer Protocol Secure (HTTPS).

Perché aprire e chiudere le porte

Quando apri le porte, consenti a un client di stabilire una connessione con il tuo computer virtuale. Quando chiudi le porte, blocchi le connessioni al computer virtuale. Ad esempio, per consentire a un client SSH di connettersi al computer virtuale, è necessario configurare una regola firewall che consenta il protocollo TCP sulla porta 22 solo a partire dall'indirizzo IP del computer che deve stabilire una connessione. In questo caso, non vuoi consentire a nessun indirizzo IP di stabilire una connessione SSH al tuo computer virtuale. Tutto ciò potrebbe comportare un rischio per la sicurezza. Se questa regola è già configurata sul firewall dell'istanza, puoi eliminarla per impedire al client SSH di connettersi al tuo computer virtuale.

Le seguenti procedure mostrano come raggiungere le porte attualmente aperte sul computer virtuale, aprirne delle nuove e chiuderne altre.

Argomenti

Completa i prerequisiti

Completare i seguenti prerequisiti prima di iniziare.

- Crea un computer virtuale in Lightsail for Research. Per ulteriori informazioni, consulta Crea un computer virtuale Lightsail for Research.
- Scarica e installa il file AWS Command Line Interface ()AWS CLI. Per ulteriori informazioni, consulta Installazione o aggiornamento della versione più recente della AWS CLI nella Guida per l'utente di AWS Command Line Interface per la versione 2.
- Configura il AWS CLI per accedere al tuo Account AWS. Per ulteriori informazioni, consulta Nozioni di base sulla configurazione nella Guida per l'utente di AWS Command Line Interface per la versione 2.

Ottieni gli stati delle porte per un computer virtuale

Completa la procedura seguente per ottenere gli stati delle porte per un computer virtuale. Questa procedura utilizza il `get-instance-port-states` AWS CLI comando per ottenere gli stati delle porte del firewall per uno specifico computer virtuale Lightsail for Research, gli indirizzi IP autorizzati a connettersi al computer virtuale tramite le porte e il protocollo. Per ulteriori informazioni, consulta get-instance-port-states nella documentazione di riferimento dei comandi della AWS CLI .

1. Questo passaggio viene determinato dal sistema operativo del computer locale.
    - Se il computer locale utilizza un sistema operativo Windows, apri una finestra del prompt dei comandi.

- Se il computer locale utilizza un sistema operativo basato su Linux o UNIX (incluso macOS), apri una finestra di Terminale.

2. Inserisci il comando seguente per ottenere gli stati delle porte del firewall e gli indirizzi IP e i protocolli consentiti. Nel comando, sostituisci *REGION* con il codice della regione AWS in cui è stato creato il computer virtuale, ad esempio `us-east-2`. Sostituisci *NAME* con il nome del tuo computer virtuale.

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

Esempio

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

La risposta mostrerà le porte e i protocolli aperti e gli intervalli IP CIDR a cui il computer virtuale può connettersi.

```
[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
```

Per informazioni su come aprire le porte, vai alla sezione successiva.

Aprire le porte per un computer virtuale

Completa la procedura seguente per aprire le porte di un computer virtuale. Questa procedura utilizza il comando. `open-instance-public-ports` AWS CLI Aprire le porte del firewall per consentire la creazione di connessioni da un indirizzo IP o da un intervallo di indirizzi IP attendibili. Ad esempio, per consentire l'indirizzo IP `192.0.2.44`, specifica `192.0.2.44` o `192.0.2.44/32`. Per consentire l'intervallo di indirizzi IP da `192.0.2.0` a `192.0.2.255`, specifica `192.0.2.0/24`. Per ulteriori informazioni, consulta open-instance-public-ports nella documentazione di riferimento dei comandi della AWS CLI .

1. Questo passaggio viene determinato dal sistema operativo del computer locale.

- Se il computer locale utilizza un sistema operativo Windows, apri una finestra del prompt dei comandi.
- Se il computer locale utilizza un sistema operativo basato su Linux o UNIX (incluso macOS), apri una finestra di Terminale.

2. Inserisci il comando seguente per aprire le porte.

   Nei comandi seguenti, sostituisci i seguenti elementi:

   - Sostituisci *REGION* con il codice della AWS regione in cui è stato creato il computer virtuale, ad esempio`us-east-2`.
   - Sostituisci *NAME* con il nome del tuo computer virtuale.
   - Sostituisci *FROM-PORT* con la prima porta in un intervallo di porte che desideri aprire.
   - Sostituisci *PROTOCOL* con il nome del protocollo IP. Ad esempio, TCP.
   - Sostituisci *TO-PORT* con l'ultima porta in un intervallo di porte che desideri aprire.
   - Sostituisci *IP* con l'indirizzo IP o l'intervallo di indirizzi IP a cui desideri che il tuo computer virtuale si connetta.

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

   Esempio

   ```
   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
   ```

   La risposta mostrerà le porte, i protocolli e gli intervalli CIDR IP appena aggiunti a cui il computer virtuale può connettersi.

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

Per informazioni su come chiudere le porte, vai alla sezione successiva.

Chiudere le porte di un computer virtuale

Completa la procedura seguente per chiudere le porte di un computer virtuale. Questa procedura utilizza il `close-instance-public-ports` AWS CLI comando. Per ulteriori informazioni, consulta close-instance-public-ports nella documentazione di riferimento dei comandi della AWS CLI .

1. Questo passaggio viene determinato dal sistema operativo del computer locale.
   - Se il computer locale utilizza un sistema operativo Windows, apri una finestra del prompt dei comandi.
   - Se il computer locale utilizza un sistema operativo basato su Linux o UNIX (incluso macOS), apri una finestra di Terminale.
2. Inserisci il comando seguente per chiudere le porte.

   Nei comandi seguenti, sostituisci i seguenti elementi:

   - Sostituisci *REGION* con il codice della AWS regione in cui è stato creato il computer virtuale, ad esempio`us-east-2`.
   - Sostituisci *NAME* con il nome del tuo computer virtuale.
   - Sostituisci *FROM-PORT* con la prima porta in un intervallo di porte che desideri chiudere.
   - Sostituisci *PROTOCOL* con il nome del protocollo IP. Ad esempio, TCP.
   - Sostituisci *TO-PORT* con l'ultima porta in un intervallo di porte che desideri chiudere.
   - Sostituisci *IP* con l'indirizzo IP o l'intervallo di indirizzi IP che desideri rimuovere.

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

Esempio

```
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
```

La risposta mostrerà le porte, i protocolli e gli intervalli CIDR IP che sono stati chiusi e non possono più connettersi al computer virtuale.

Passa alle fasi successive

Dopo aver gestito correttamente le porte del firewall del tuo computer virtuale, puoi completare gli ulteriori passaggi di seguito:

- Ottieni la coppia di chiavi del tuo computer virtuale. Con la coppia di chiavi, puoi stabilire una connessione utilizzando numerosi client SSH, come OpenSSH, PuTTY e Windows Subsystem per Linux. Per ulteriori informazioni, consulta Richiedi una key pair per un computer virtuale Lightsail for Research.
- Connettiti al computer virtuale tramite SSH per gestirlo tramite la riga di comando. Per ulteriori informazioni, consulta Trasferisci file sui computer virtuali di Lightsail for Research utilizzando Secure Copy.

- Connettiti al computer virtuale tramite SCP per trasferire file in modo sicuro. Per ulteriori informazioni, consulta Trasferisci file sui computer virtuali di Lightsail for Research utilizzando Secure Copy.

Richiedi una key pair per un computer virtuale Lightsail for Research

Una coppia di chiavi, composta da una chiave pubblica e una chiave privata, è un insieme di credenziali di sicurezza che usi per dimostrare la tua identità quando ti connetti a un computer virtuale Amazon Lightsail for Research. La chiave pubblica è memorizzata su ogni computer virtuale in Lightsail for Research e tu conservi la chiave privata sul tuo computer locale. La chiave privata consente di stabilire in modo sicuro un protocollo Secure Shell (SSH) con il computer virtuale. Chiunque possieda la tua chiave privata potrà connettersi al tuo computer virtuale, quindi è importante archiviare la chiave privata in un luogo sicuro.

Una coppia di chiavi predefinita di Amazon Lightsail (DKP) viene creata automaticamente la prima volta che crei un'istanza Lightsail o un computer virtuale Lightsail for Research. Il DKP è specifico per ogni AWS regione in cui crei un'istanza o un computer virtuale. Ad esempio, il DKP di Lightsail per la regione Stati Uniti orientali (Ohio) (us-east-2) si applica a tutti i computer creati negli Stati Uniti orientali (Ohio) in Lightsail e Lightsail for Research configurati per utilizzare il DKP al momento della creazione. Lightsail for Research archivia automaticamente la chiave pubblica del DKP sui computer virtuali che crei. Puoi scaricare la chiave privata del DKP in qualsiasi momento effettuando una chiamata API al servizio Lightsail.

In questo documento viene illustrato come ottenere il DKP per un computer virtuale. Dopo aver ottenuto il DKP, puoi stabilire una connessione utilizzando numerosi client SSH, come OpenSSH, PuTTY e Windows Subsystem per Linux. Puoi anche utilizzare Secure Copy (SCP) per trasferire in modo sicuro i file dal tuo computer locale al tuo computer virtuale.

> **Note**
>
> Puoi anche stabilire una connessione con il protocollo di visualizzazione remota al tuo computer virtuale utilizzando il client Amazon DCV basato su browser. Amazon DCV è disponibile nella console Lightsail for Research. Quel client RDP non richiede l'ottenimento di una coppia di chiavi per il tuo computer. Per ulteriori informazioni, consultare Accedi a

un'applicazione per computer virtuale Lightsail for Research e Accedi al sistema operativo del tuo computer virtuale Lightsail for Research.

Argomenti

Completa i prerequisiti

Completare i seguenti prerequisiti prima di iniziare.

- Crea un computer virtuale in Lightsail for Research. Per ulteriori informazioni, consulta Crea un computer virtuale Lightsail for Research.
- Scarica e installa il file AWS Command Line Interface ()AWS CLI. Per ulteriori informazioni, consulta Installazione o aggiornamento della versione più recente della AWS CLI nella Guida per l'utente di AWS Command Line Interface per la versione 2.
- Configura il AWS CLI per accedere al tuo Account AWS. Per ulteriori informazioni, consulta Nozioni di base sulla configurazione nella Guida per l'utente di AWS Command Line Interface per la versione 2.
- Scarica e installa jq. È un processore JSON a riga di comando leggero e flessibile utilizzato nelle seguenti procedure per estrarre i dettagli delle coppie di chiavi dagli output JSON di AWS CLI. Per ulteriori informazioni sul download e l'installazione di jq, consulta Scarica jq sul sito Web di jq.

Procurati una coppia di chiavi per un computer virtuale

Completa una delle seguenti procedure per ottenere il DKP di Lightsail per un computer virtuale in Lightsail for Research.

Ottieni una coppia di chiavi per un computer virtuale utilizzando un computer locale Windows

Questa procedura si applica se il computer locale utilizza un sistema operativo Windows. Questa procedura utilizza il `download-default-key-pair` AWS CLI comando per ottenere il DKP di Lightsail per una regione. AWS Per ulteriori informazioni, consulta download-default-key-pair nella documentazione di riferimento dei comandi della AWS CLI .

1. Apri una finestra del prompt dei comandi.
2. Immetti il seguente comando per ottenere il DKP di Lightsail per una regione specifica. AWS Questo comando salva le informazioni in un file `dkp-details.json`. Nel comando, sostituiscilo *`region-code`* con il codice della AWS regione in cui è stato creato il computer virtuale, ad esempio. `us-east-2`

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

   Esempio

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

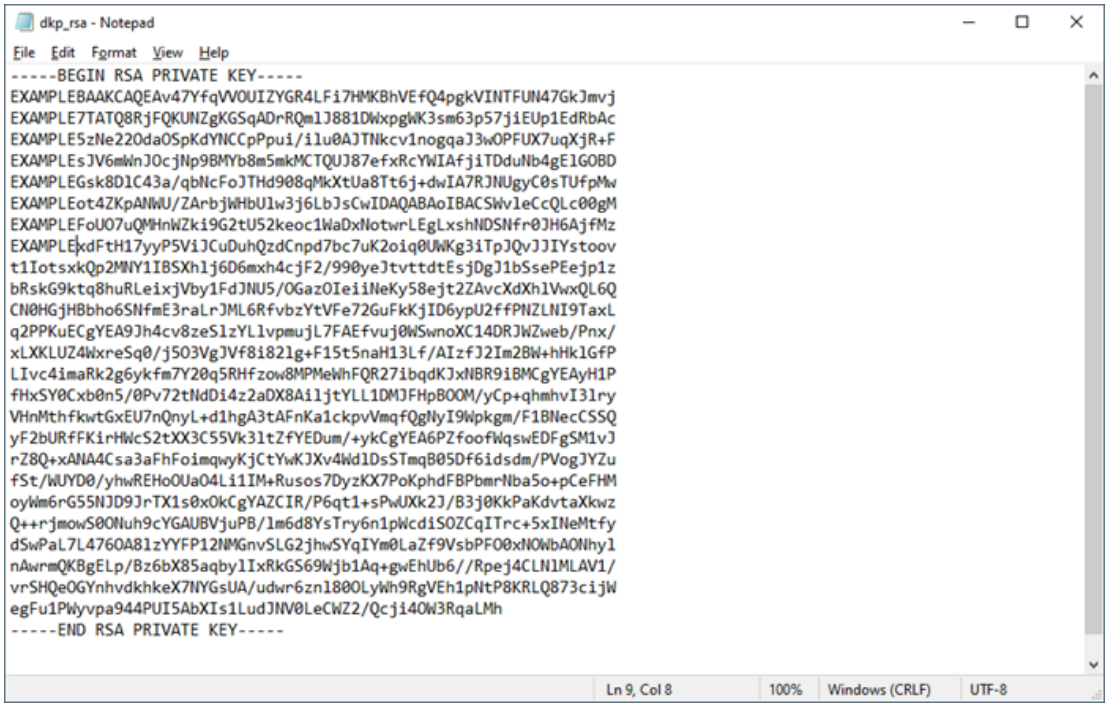
   Non c'è risposta al comando. Puoi confermare se il comando ha avuto successo aprendo il `dkp-details.json` file e verificando se le informazioni DKP di Lightsail sono state salvate. Il contenuto del file `dkp-details.json` deve corrispondere all'esempio che segue. Il comando non è riuscito se il file è vuoto.

3. Inserisci il comando seguente per estrarre le informazioni sulla chiave privata dal file `dkp-details.json` e aggiungerle a un nuovo file di chiave privata `dkp_rsa`.

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

Non c'è risposta al comando. È possibile confermare se il comando ha avuto successo aprendo il file `dkp_rsa` e verificando se contiene le informazioni. Il contenuto del file `dkp_rsa` deve corrispondere all'esempio che segue. Il comando non è riuscito se il file è vuoto.



Ora hai la chiave privata necessaria per stabilire una connessione SSH o SCP al tuo computer virtuale. Passa alla sezione successiva per ulteriori passaggi.

Ottieni una coppia di chiavi per un computer virtuale utilizzando un computer locale Linux, Unix o macOS

Questa procedura si applica se il computer locale utilizza un sistema operativo Linux, Unix o macOS. Questa procedura utilizza il `download-default-key-pair` AWS CLI comando per ottenere il DKP di Lightsail per una regione. AWS Per ulteriori informazioni, consulta download-default-key-pair nella documentazione di riferimento dei comandi della AWS CLI .

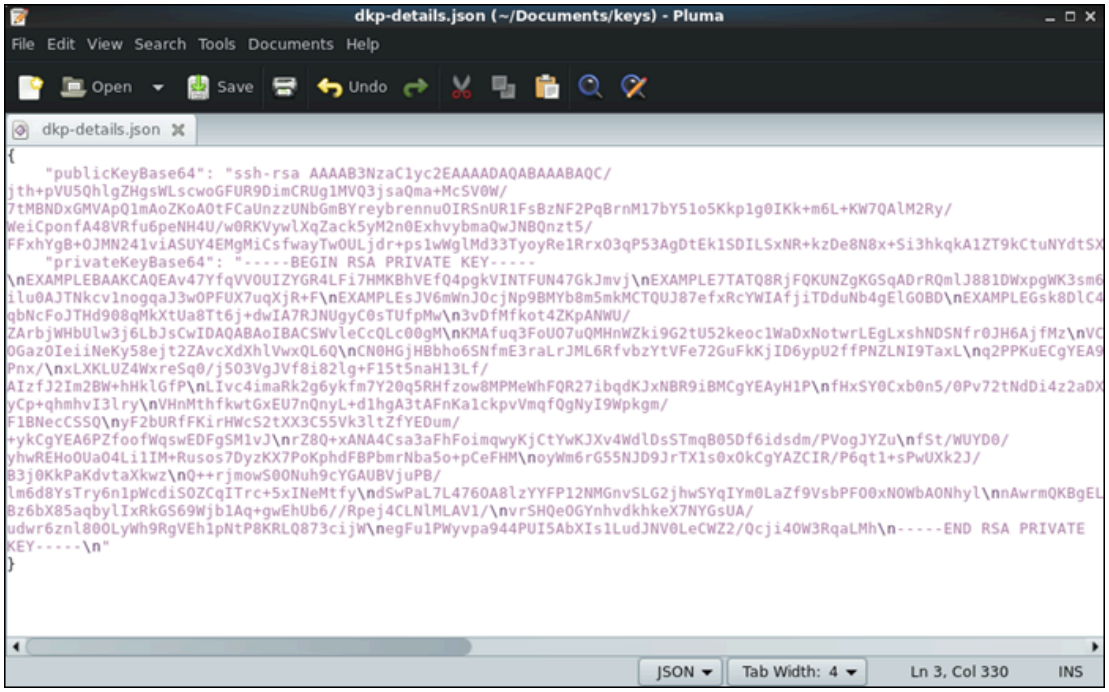
1. Apri una finestra del terminale.
2. Immetti il seguente comando per ottenere il DKP di Lightsail per una regione specifica. AWS Questo comando salva le informazioni in un file `dkp-details.json`. Nel comando, sostituiscilo *`region-code`* con il codice della AWS regione in cui è stato creato il computer virtuale, ad esempio. `us-east-2`

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

Esempio

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

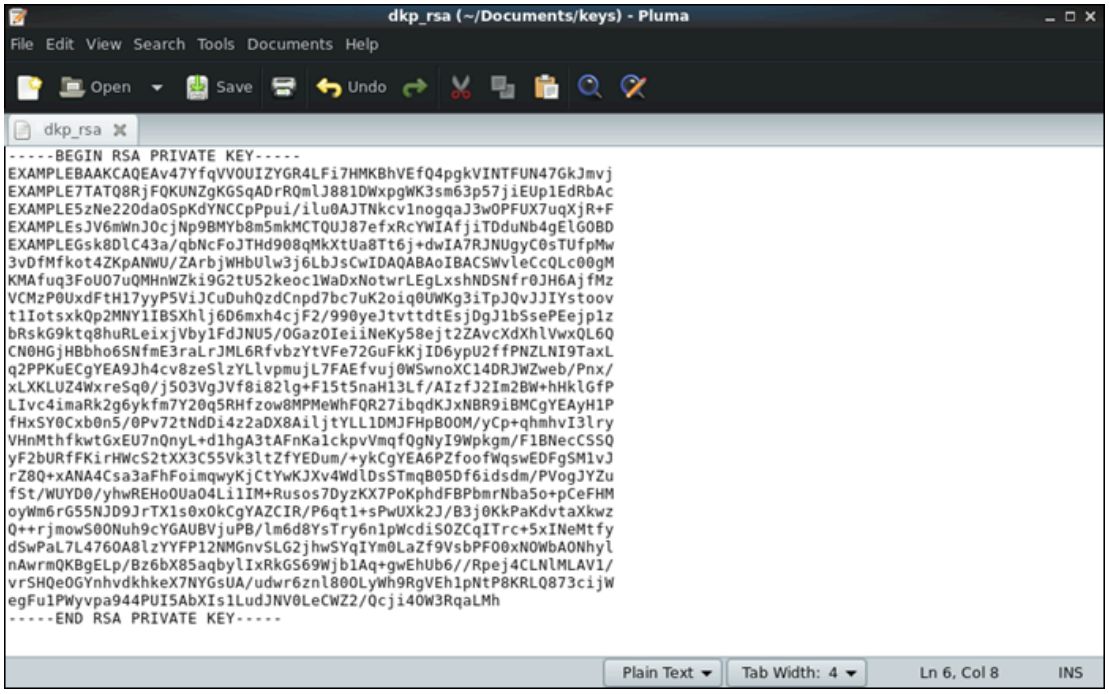
Non c'è risposta al comando. Puoi confermare se il comando ha avuto successo aprendo il `dkp-details.json` file e verificando se le informazioni DKP di Lightsail sono state salvate. Il contenuto del file `dkp-details.json` deve corrispondere all'esempio che segue. Il comando non è riuscito se il file è vuoto.



3. Inserisci il comando seguente per estrarre le informazioni sulla chiave privata dal file `dkp-details.json` e aggiungerle a un nuovo file di chiave privata `dkp_rsa`.

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

Non c'è risposta al comando. È possibile confermare se il comando ha avuto successo aprendo il file `dkp_rsa` e verificando se contiene le informazioni. Il contenuto del file `dkp_rsa` deve corrispondere all'esempio che segue. Il comando non è riuscito se il file è vuoto.



4. Per impostare le autorizzazioni sul file `dkp_rsa`, eseguire il comando seguente.

```
chmod 600 dkp_rsa
```

Ora hai la chiave privata necessaria per stabilire una connessione SSH o SCP al tuo computer virtuale. Passa alla sezione successiva per ulteriori passaggi.

Passa alle fasi successive

Dopo aver ottenuto correttamente le coppie di chiavi per il tuo computer virtuale, puoi completare gli ulteriori passaggi di seguito:

- Connettiti al computer virtuale tramite SSH per gestirlo tramite la riga di comando. Per ulteriori informazioni, consulta Connect a un computer virtuale Lightsail for Research tramite Secure Shell.
- Connettiti al computer virtuale tramite SCP per trasferire file in modo sicuro. Per ulteriori informazioni, consulta Trasferisci file sui computer virtuali di Lightsail for Research utilizzando Secure Copy.

Connect a un computer virtuale Lightsail for Research tramite Secure Shell

Puoi connetterti a un computer virtuale in Amazon Lightsail for Research utilizzando il protocollo SSH (Secure Shell Protocol). È possibile utilizzare SSH per gestire il computer virtuale in remoto in modo da poter accedere al computer tramite Internet ed eseguire comandi.

> **Note**
>
> Puoi anche stabilire una connessione con il protocollo di visualizzazione remota al tuo computer virtuale utilizzando il client Amazon DCV basato su browser. Amazon DCV è disponibile nella console Lightsail for Research. Per ulteriori informazioni, consulta Accedi al sistema operativo del tuo computer virtuale Lightsail for Research.

Argomenti

Completa i prerequisiti

Completare i seguenti prerequisiti prima di iniziare.

- Crea un computer virtuale in Lightsail for Research. Per ulteriori informazioni, consulta Crea un computer virtuale Lightsail for Research.
- Assicurati che il computer virtuale a cui desideri connetterti sia in uno stato attivo. Inoltre, annota il nome del computer virtuale e la AWS regione in cui è stato creato. Queste informazioni ti serviranno più avanti in questo processo. Per ulteriori informazioni, consulta Visualizza i dettagli del computer virtuale di Lightsail for Research.
- Assicurati che la porta 22 sia aperta sul computer virtuale a cui desideri connetterti. Questa è la porta predefinita utilizzata per SSH. È aperta per impostazione predefinita. Ma se l'hai chiusa, devi riaprirla prima di continuare. Per ulteriori informazioni, consulta Gestione delle porte firewall per i computer virtuali Lightsail for Research.

- Ottieni la coppia di chiavi predefinita di Lightsail (DKP) per il tuo computer virtuale. Per ulteriori informazioni, consulta Procurati una coppia di chiavi per un computer virtuale.

  > **Tip**
  >
  > Se intendi utilizzarla per connetterti AWS CloudShell al tuo computer virtuale, consulta la sezione Connect a un computer virtuale tramite AWS CloudShell successiva. Per ulteriori informazioni, consulta What is AWS CloudShell. Altrimenti, passa al prerequisito successivo.

- Scaricate e installate il file AWS Command Line Interface (AWS CLI). Per ulteriori informazioni, consulta Installazione o aggiornamento della versione più recente della AWS CLI nella Guida per l'utente di AWS Command Line Interface per la versione 2.
- Configura il AWS CLI per accedere al tuo Account AWS. Per ulteriori informazioni, consulta Nozioni di base sulla configurazione nella Guida per l'utente di AWS Command Line Interface per la versione 2.
- Scarica e installa jq. È un processore JSON a riga di comando leggero e flessibile utilizzato nelle seguenti procedure per estrarre i dettagli delle coppie di chiavi. Per ulteriori informazioni sul download e l'installazione di jq, consulta Scarica jq sul sito Web di jq.

Connettiti a un computer virtuale tramite Secure Shell (SSH)

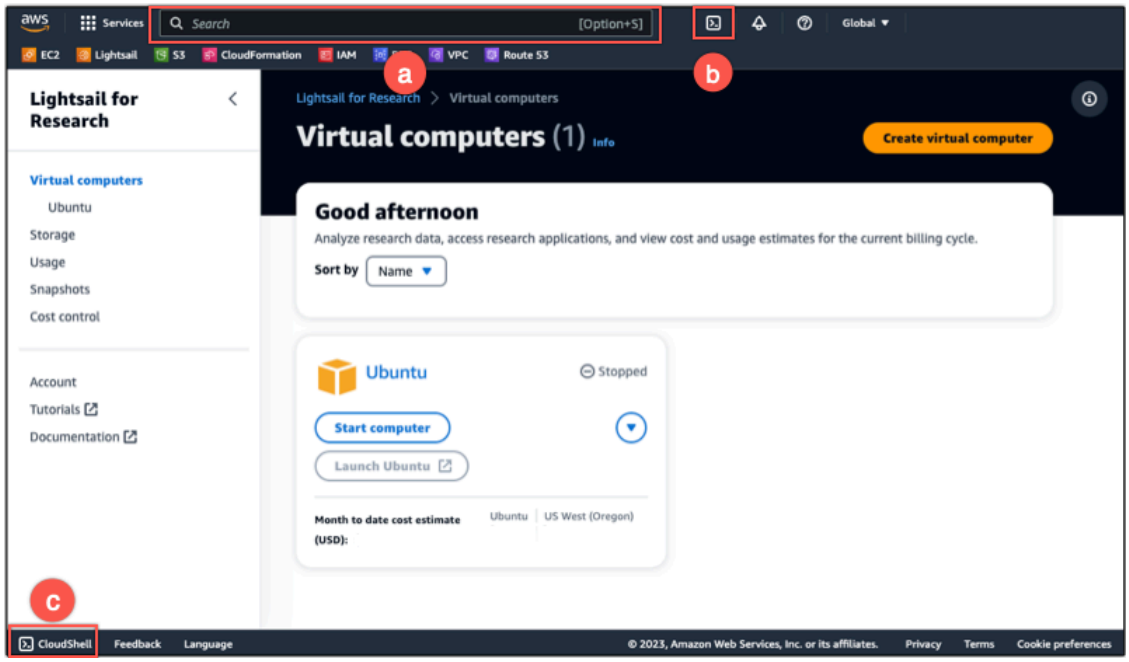
Completa una delle seguenti procedure per stabilire una connessione SSH al tuo computer virtuale in Lightsail for Research.

Connect a un computer virtuale tramite AWS CloudShell

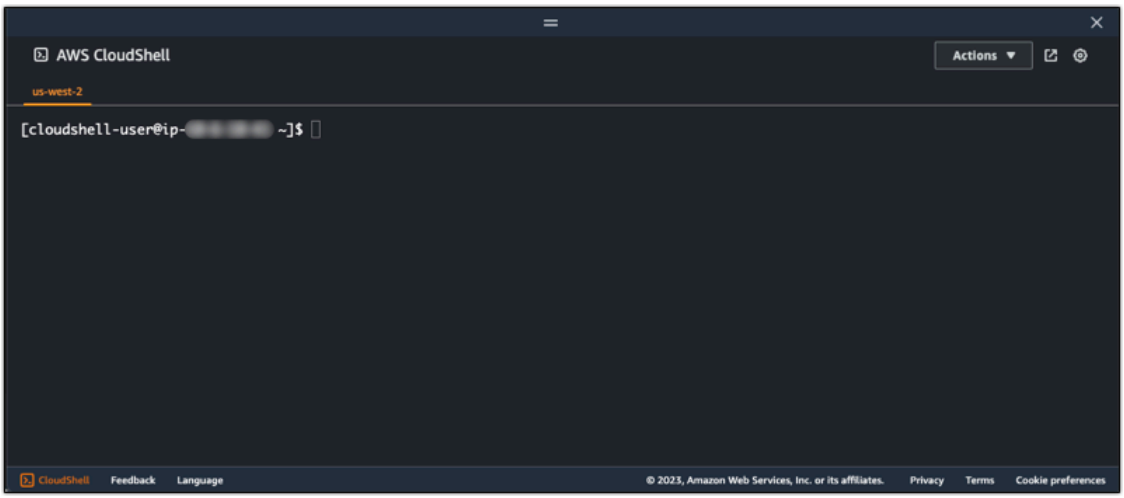
Questa procedura si applica se si preferisce una configurazione minima per la connessione al computer virtuale. AWS CloudShell utilizza una shell preautenticata basata su browser che è possibile avviare direttamente da. Console di gestione AWSÈ possibile eseguire AWS CLI i comandi utilizzando la shell preferita, ad esempio Bash o la shell Z. PowerShell E puoi farlo senza dover scaricare o installare strumenti da riga di comando. Per ulteriori informazioni, consulta Nozioni di base su AWS CloudShell nella Guida per l'utente di AWS CloudShell .

> **Important**
>
> Prima di iniziare, assicurati di avere la coppia di chiavi Lightsail predefinita (DKP) per il computer virtuale a cui ti stai connettendo. Per ulteriori informazioni, consulta Richiedi una key pair per un computer virtuale Lightsail for Research.

1. Dalla console Lightsail for Research, CloudShell avvia scegliendo una delle seguenti opzioni:
   a. Nella casella di ricerca, digita "CloudShell«, quindi scegli. CloudShell
   b. Nella barra di navigazione seleziona l'icona CloudShell.
   c. Scegli CloudShellnella barra degli strumenti della console nella parte inferiore sinistra della console.



Quando viene visualizzato il prompt dei comandi, la shell è pronta per l'interazione.



2. Scegli una shell preinstallata con cui lavorare. Per cambiare la shell predefinita, inserisci uno dei seguenti nomi di programma al prompt della riga di comando. Bashè la shell predefinita che viene eseguita all'avvio AWS CloudShell.

   Bash

   ```
   bash
   ```

   Se si passa aBash, il simbolo nella riga di comando viene aggiornato a$.

   PowerShell

   ```
   pwsh
   ```

   Se si passa a PowerShell, il simbolo visualizzato nel prompt dei comandi viene aggiornato a. `PS>`

   Z shell

   ```
   zsh
   ```

   Se si passa aZ shell, il simbolo visualizzato nel prompt dei comandi viene aggiornato a. `%`

3. Per connettersi a un computer virtuale dalla finestra del CloudShell terminale, vedereConnettiti a un computer virtuale tramite SSH su un computer locale Linux, Unix o macOS..

Per informazioni sul software preinstallato nell' CloudShellambiente, consulta l'ambiente di AWS CloudShell calcolo nella Guida per l'AWS CloudShell utente.

Connettiti a un computer virtuale tramite SSH su un computer locale Windows

Questa procedura si applica se il computer locale utilizza un sistema operativo Windows. Questa procedura utilizza il `get-instance` AWS CLI comando per ottenere il nome utente e l'indirizzo IP pubblico dell'istanza a cui si desidera connettersi. Per ulteriori informazioni, consulta get-instance nella Guida di riferimento dei comandi AWS CLI .

> **Important**
>
> Assicurati di avere la coppia di chiavi Lightsail predefinita (DKP) per il computer virtuale a cui stai tentando di connetterti prima di iniziare questa procedura. Per ulteriori informazioni, consulta Richiedi una key pair per un computer virtuale Lightsail for Research. Questa procedura invia la chiave privata del DKP di Lightsail in `dkp_rsa` un file utilizzato in uno dei seguenti comandi.

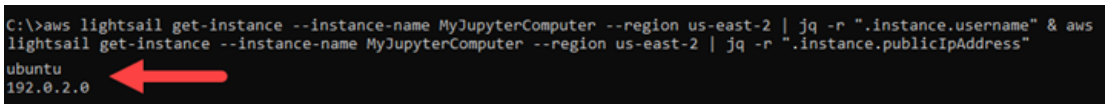
1. Apri una finestra del prompt dei comandi.
2. Inserisci il comando seguente per visualizzare l'indirizzo IP pubblico e il nome utente del computer virtuale. Nel comando, sostituiscila *`region-code`* con il codice Regione AWS in cui è stato creato il computer virtuale, ad esempio. `us-east-2` Sostituisci *`computer-name`* con il nome del computer virtuale a cui desideri connetterti.

   ```
   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"
   ```

   Esempio

   ```
   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"
   ```

   La risposta mostrerà il nome utente e l'indirizzo IP pubblico del computer virtuale, come mostrato nell'esempio seguente. Prendi nota di questi valori, perché serviranno al passaggio successivo di questa procedura.

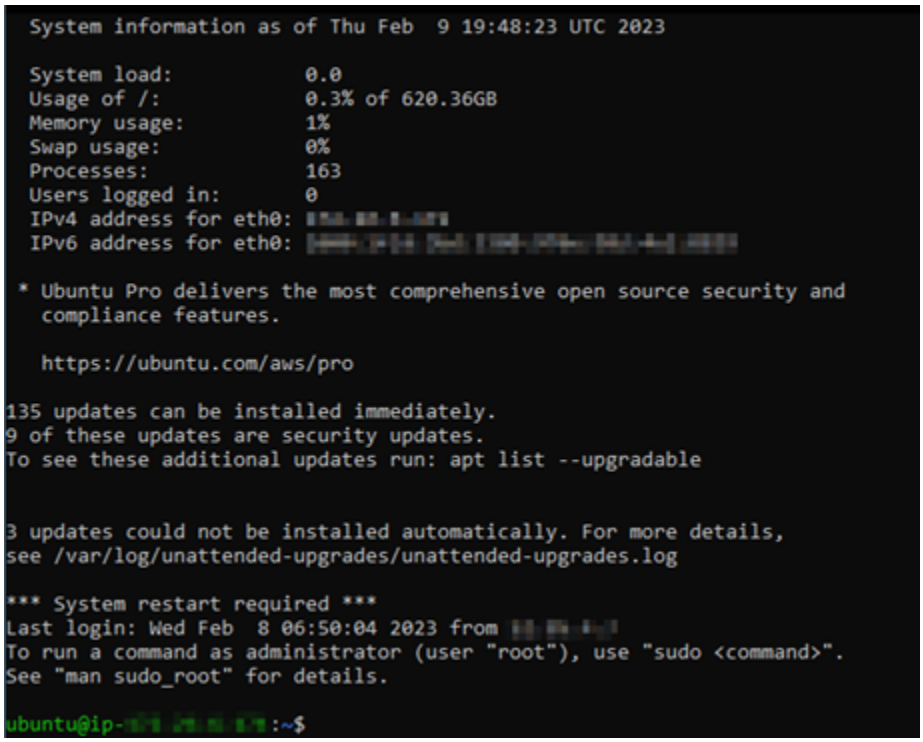
3. Inserisci il seguente comando per stabilire una connessione SSH con il tuo computer virtuale. Nel comando, sostituisci *user-name* con il nome utente di accesso e *public-ip-address* con l'indirizzo IP pubblico del tuo computer virtuale.

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

Esempio

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

Dovresti vedere una risposta simile all'esempio seguente, che mostra una connessione SSH stabilita con un computer virtuale Ubuntu in Lightsail for Research.



Ora che hai stabilito correttamente una connessione SSH al tuo computer virtuale, vai alla sezione successiva per ulteriori passaggi.

Connettiti a un computer virtuale tramite SSH su un computer locale Linux, Unix o macOS.

Questa procedura si applica se il computer locale utilizza un sistema operativo Linux, Unix o macOS. Questa procedura utilizza il `get-instance` AWS CLI comando per ottenere il nome utente e

l'indirizzo IP pubblico dell'istanza a cui desideri connetterti. Per ulteriori informazioni, consulta get-instance nella Guida di riferimento dei comandi AWS CLI .

> **Important**
>
> Assicurati di avere la coppia di chiavi Lightsail predefinita (DKP) per il computer virtuale a cui stai tentando di connetterti prima di iniziare questa procedura. Per ulteriori informazioni, consulta Richiedi una key pair per un computer virtuale Lightsail for Research. Questa procedura invia la chiave privata del DKP di Lightsail in `dkp_rsa` un file utilizzato in uno dei seguenti comandi.

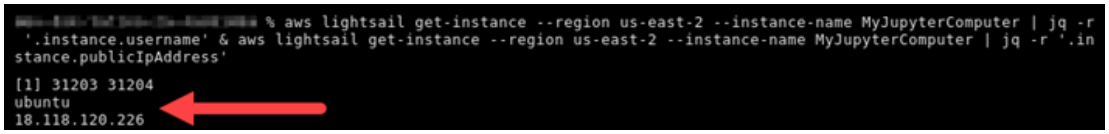
1. Apri una finestra del terminale.
2. Inserisci il comando seguente per visualizzare l'indirizzo IP pubblico e il nome utente del computer virtuale. Nel comando, sostituiscila *`region-code`* con il codice della AWS regione in cui è stato creato il computer virtuale, ad esempio. `us-east-2` Sostituisci *`computer-name`* con il nome del computer virtuale a cui desideri connetterti.

   ```
   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'
   ```

   Esempio

   ```
   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'
   ```

   La risposta mostrerà il nome utente e l'indirizzo IP pubblico del computer virtuale, come mostrato nell'esempio seguente. Prendi nota di questi valori, perché serviranno al passaggio successivo di questa procedura.

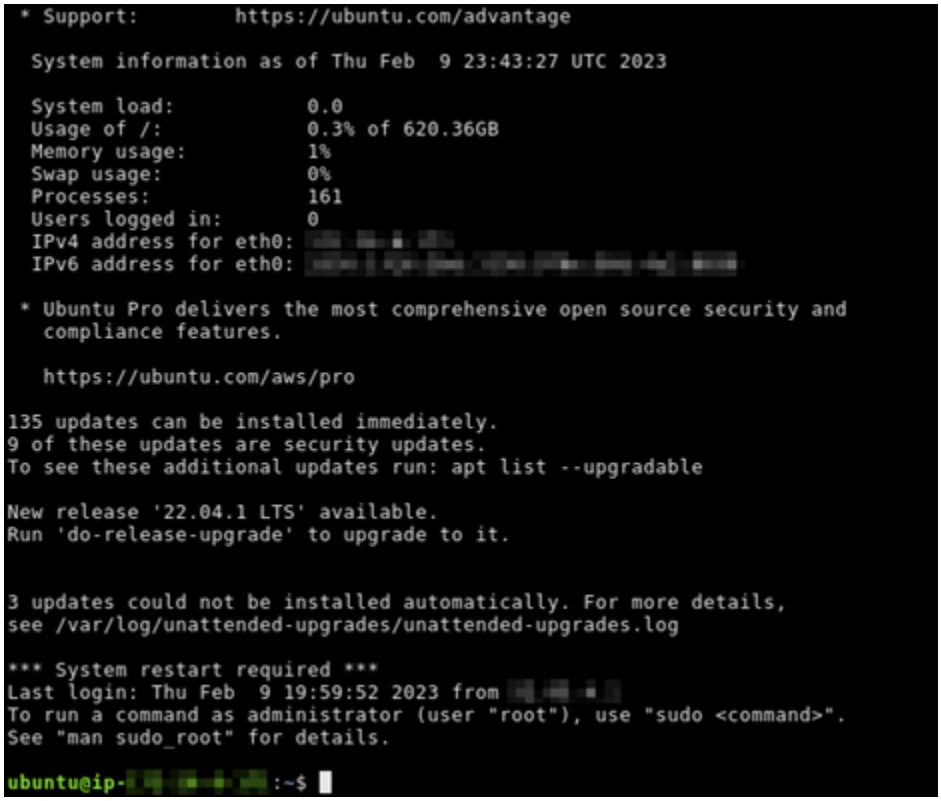
3. Inserisci il seguente comando per stabilire una connessione SSH con il tuo computer virtuale. Nel comando, sostituisci *`user-name`* con il nome utente di accesso e *`public-ip-address`* con l'indirizzo IP pubblico del tuo computer virtuale.

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

Esempio

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

Dovresti vedere una risposta simile all'esempio seguente, che mostra una connessione SSH stabilita con un computer virtuale Ubuntu in Lightsail for Research.



Ora che hai stabilito correttamente una connessione SSH al tuo computer virtuale, vai alla sezione successiva per ulteriori passaggi.

Passa alle fasi successive

Dopo aver stabilito correttamente una connessione SSH al tuo computer virtuale, puoi completare gli ulteriori passaggi di seguito:

- Connettiti al computer virtuale tramite SCP per trasferire file in modo sicuro. Per ulteriori informazioni, consulta Trasferisci file sui computer virtuali di Lightsail for Research utilizzando Secure Copy.

Trasferisci file sui computer virtuali di Lightsail for Research utilizzando Secure Copy

Puoi trasferire file dal tuo computer locale a un computer virtuale in Amazon Lightsail for Research utilizzando Secure Copy (SCP). Con questo processo, puoi trasferire più file o intere directory contemporaneamente.

> **Note**
>
> Puoi anche stabilire una connessione con protocollo di visualizzazione remota al tuo computer virtuale utilizzando il client Amazon DCV basato su browser disponibile nella console Lightsail for Research. Con il client Amazon DCV, puoi trasferire rapidamente singoli file. Per ulteriori informazioni, consulta Accedi al sistema operativo del tuo computer virtuale Lightsail for Research.

Argomenti

Completa i prerequisiti

Completare i seguenti prerequisiti prima di iniziare.

- Crea un computer virtuale in Lightsail for Research. Per ulteriori informazioni, consulta Crea un computer virtuale Lightsail for Research.
- Assicurati che il computer virtuale a cui desideri connetterti sia in uno stato attivo. Inoltre, annota il nome del computer virtuale e la regione AWS in cui è stato creato. Queste informazioni saranno necessarie più avanti in questa procedura. Per ulteriori informazioni, consulta Visualizza i dettagli del computer virtuale di Lightsail for Research.

- Scarica e installa il file AWS Command Line Interface ()AWS CLI. Per ulteriori informazioni, consulta Installazione o aggiornamento della versione più recente della AWS CLI nella Guida per l'utente di AWS Command Line Interface per la versione 2.
- Configura il AWS CLI per accedere al tuo Account AWS. Per ulteriori informazioni, consulta Nozioni di base sulla configurazione nella Guida per l'utente di AWS Command Line Interface per la versione 2.
- Scarica e installa jq. È un processore JSON a riga di comando leggero e flessibile utilizzato nelle seguenti procedure per estrarre i dettagli delle coppie di chiavi. Per ulteriori informazioni sul download e l'installazione di jq, consulta Scarica jq sul sito Web di jq.
- Assicurati che la porta 22 sia aperta sul computer virtuale a cui desideri connetterti. Questa è la porta predefinita utilizzata per SSH. È aperta per impostazione predefinita. Ma se l'hai chiusa, devi riaprirla prima di continuare. Per ulteriori informazioni, consulta Gestione delle porte firewall per i computer virtuali Lightsail for Research.
- Ottieni la coppia di chiavi predefinita di Lightsail (DKP) per il tuo computer virtuale. Per ulteriori informazioni, consulta Crea un computer virtuale Lightsail for Research.

Connettiti a un computer virtuale tramite SCP

Completa una delle seguenti procedure per connetterti al tuo computer virtuale in Lightsail for Research utilizzando SCP.

Connettiti a un computer virtuale tramite SCP su un computer locale Windows

Questa procedura si applica se il computer locale utilizza un sistema operativo Windows. Questa procedura utilizza il `get-instance` AWS CLI comando per ottenere il nome utente e l'indirizzo IP pubblico dell'istanza a cui desideri connetterti. Per ulteriori informazioni, consulta get-instance nella Guida di riferimento dei comandi AWS CLI .

> **Important**
>
> Assicurati di avere la coppia di chiavi Lightsail predefinita (DKP) per il computer virtuale a cui stai tentando di connetterti prima di iniziare questa procedura. Per ulteriori informazioni, consulta Richiedi una key pair per un computer virtuale Lightsail for Research. Questa procedura invia la chiave privata del DKP di Lightsail in `dkp_rsa` un file utilizzato in uno dei seguenti comandi.

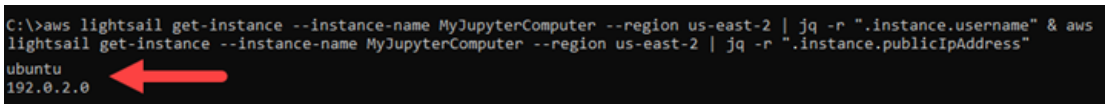
1. Apri una finestra del prompt dei comandi.
2. Inserisci il comando seguente per visualizzare l'indirizzo IP pubblico e il nome utente del computer virtuale. Nel comando, sostituiscila *region-code* con il codice della AWS regione in cui è stato creato il computer virtuale, ad esempio. `us-east-2` Sostituisci *computer-name* con il nome del computer virtuale a cui desideri connetterti.

```
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"
```

Esempio

```
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"
```

La risposta mostrerà il nome utente e l'indirizzo IP pubblico del computer virtuale, come mostrato nell'esempio seguente. Prendi nota di questi valori, perché serviranno al passaggio successivo di questa procedura.



3. Inserisci il seguente comando per stabilire una connessione SCP con il tuo computer virtuale e trasferirvi file.

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

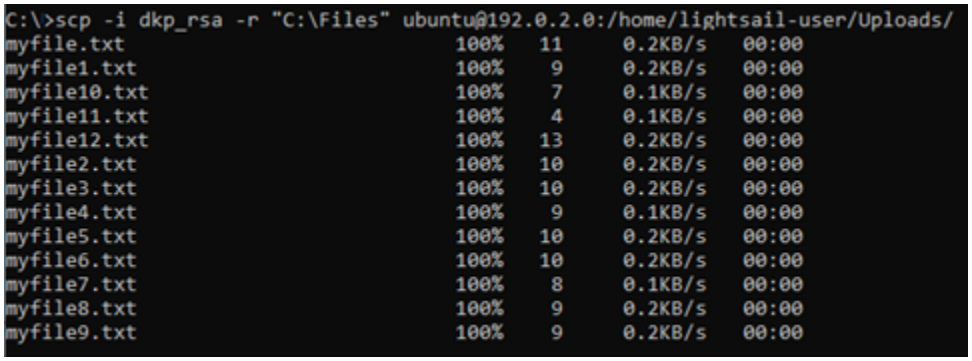
Nel comando, sostituisci:

- *source-folder* con la cartella sul computer locale che contiene i file che desideri trasferire.
- *user-name* con il nome utente utilizzato nel passaggio precedente di questa procedura (ad esempio `ubuntu`).
- *public-ip-address* con l'indirizzo IP pubblico del computer virtuale del passaggio precedente di questa procedura.
- *destination-directory* con il percorso della directory sul computer virtuale in cui copiare i file.

L'esempio seguente copia tutti i file dalla cartella `C:\Files` sul computer locale nella directory `/home/lightsail-user/Uploads/` del computer virtuale remoto.

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

La risposta dovrebbe essere analoga all'esempio seguente. Mostra ogni file che è stato trasferito dalla cartella di origine alla directory di destinazione. Ora dovrebbe essere possibile accedere a tali file sul computer virtuale.



Connettiti a un computer virtuale tramite SCP su un computer locale Linux, Unix o macOS.

Questa procedura si applica se il computer locale utilizza un sistema operativo Linux, Unix o macOS. Questa procedura utilizza il `get-instance` AWS CLI comando per ottenere il nome utente e l'indirizzo IP pubblico dell'istanza a cui desideri connetterti. Per ulteriori informazioni, consulta get-instance nella Guida di riferimento dei comandi AWS CLI .

> **Important**
>
> Assicurati di avere la coppia di chiavi Lightsail predefinita (DKP) per il computer virtuale a cui stai tentando di connetterti prima di iniziare questa procedura. Per ulteriori informazioni, consulta Richiedi una key pair per un computer virtuale Lightsail for Research. Questa procedura invia la chiave privata del DKP di Lightsail in `dkp_rsa` un file utilizzato in uno dei seguenti comandi.

1. Apri una finestra del terminale.
2. Inserisci il comando seguente per visualizzare l'indirizzo IP pubblico e il nome utente del computer virtuale. Nel comando, sostituiscila *`region-code`* con il codice della AWS regione in

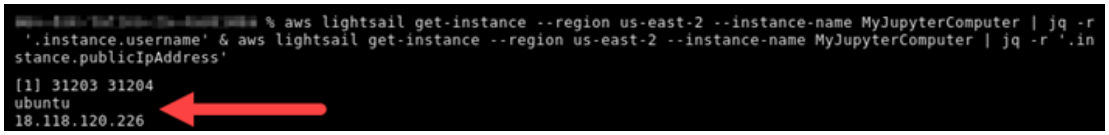
cui è stato creato il computer virtuale, ad esempio. `us-east-2` Sostituisci *`computer-name`* con il nome del computer virtuale a cui desideri connetterti.

```
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'
```

Esempio

```
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'
```

La risposta mostrerà il nome utente e l'indirizzo IP pubblico del computer virtuale, come mostrato nell'esempio seguente. Prendi nota di questi valori, perché serviranno al passaggio successivo di questa procedura.



3. Inserisci il seguente comando per stabilire una connessione SCP con il tuo computer virtuale e trasferirvi file.

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

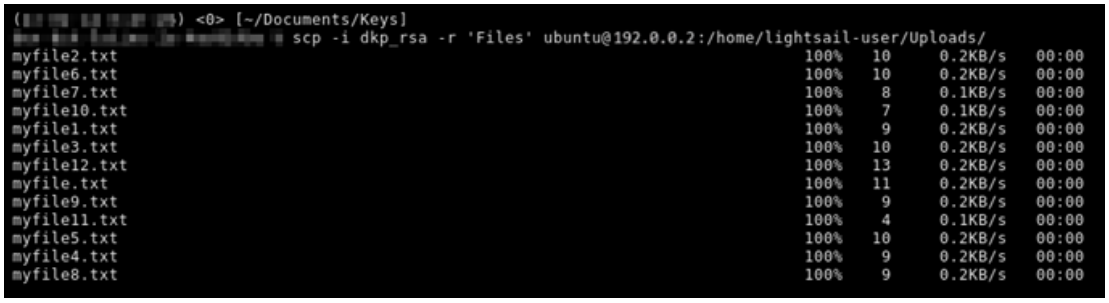
Nel comando, sostituisci:

- *`source-folder`* con la cartella sul computer locale che contiene i file che desideri trasferire.
- *`user-name`* con il nome utente utilizzato nel passaggio precedente di questa procedura (ad esempio `ubuntu`).
- *`public-ip-address`* con l'indirizzo IP pubblico del computer virtuale del passaggio precedente di questa procedura.
- *`destination-directory`* con il percorso della directory sul computer virtuale in cui copiare i file.

L'esempio seguente copia tutti i file dalla cartella `C:\Files` sul computer locale nella directory `/home/lightsail-user/Uploads/` del computer virtuale remoto.

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

La risposta dovrebbe essere analoga all'esempio seguente. Mostra ogni file che è stato trasferito dalla cartella di origine alla directory di destinazione. Ora dovrebbe essere possibile accedere a tali file sul computer virtuale.



Eliminare un computer virtuale Lightsail for Research

Completa i seguenti passaggi per eliminare il tuo computer virtuale Lightsail for Research quando non ti serve più. Non appena viene eliminato il computer virtuale, i relativi addebiti vengono bloccati. Le risorse collegate al computer eliminato, ad esempio gli snapshot, continuano a essere soggetti a costi finché non vengono eliminate.

> **Important**
>
> L'eliminazione di un computer virtuale è un'operazione permanente e il computer non può essere ripristinato. Se pensi che potresti aver bisogno dei dati in un secondo momento, è consigliabile creare uno snapshot del computer virtuale prima di eliminarli. Per ulteriori informazioni, consulta Creazione di uno snapshot.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Computer virtuali.
3. Seleziona il computer virtuale da eliminare.
4. Scegli Azioni, quindi scegli Elimina computer virtuale.
5. Digita conferma nel blocco di testo. Quindi, scegli Elimina computer virtuale.

Proteggi e archivia i dati con i volumi di Lightsail for Research

Amazon Lightsail for Research fornisce volumi di storage a livello di blocco (dischi) che puoi collegare a un computer virtuale Lightsail for Research in esecuzione. Puoi utilizzare un disco come dispositivo di storage principale per i dati che richiedono aggiornamenti frequenti e granulari. Ad esempio, i dischi sono l'opzione di archiviazione consigliata quando si esegue un database su un computer virtuale Lightsail for Research.

Un disco ha lo stesso comportamento di un dispositivo esterno a blocchi non formattati, che puoi collegare a un singolo computer virtuale. Il volume rimane persistente indipendentemente dalla durata di esecuzione di un computer. Dopo aver collegato un disco a un computer, è possibile utilizzarlo come qualsiasi altro disco rigido fisico.

È possibile collegare più dischi a un computer. Puoi anche scollegare un disco da un computer e collegarlo a un computer diverso.

Per conservare una copia di backup dei dati, crea uno snapshot del disco. Puoi anche creare un nuovo disco da uno snapshot e quindi collegarlo a un computer diverso.

Argomenti

Crea un disco di archiviazione nella console Lightsail for Research

Completa i seguenti passaggi per creare un disco per il tuo computer virtuale Lightsail for Research.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Archiviazione.
3. Scegliere Create disk (Crea disco).

4. Inserire un nome per il disco. I caratteri validi includono caratteri alfanumerici, numeri, punti, trattini e trattini bassi.

   I nomi dei dischi devono soddisfare i seguenti requisiti:

   - Sii unico Regione AWS in ognuno dei tuoi account Lightsail for Research.
   - Devono contenere da 2 a 255 caratteri.
   - Devono iniziare e terminare con un carattere alfanumerico o un numero.
5. Scegline uno Regione AWS per il tuo disco.

   Il disco deve trovarsi nella stessa regione del computer virtuale a cui verrà collegato.
6. Scegli la dimensione del disco in GB.
7. Continua alla sezione Allega un disco per informazioni su come collegare dischi al tuo computer virtuale.

Visualizza i dettagli del disco di archiviazione nella console Lightsail for Research

Completa i seguenti passaggi per visualizzare i dischi del tuo account Lightsail for Research e i relativi dettagli.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Archiviazione.

   La pagina Storage fornisce una panoramica completa dei dischi del tuo account Lightsail for Research.

   In pagina sono visualizzate le seguenti informazioni:

   - Nome: il nome del disco di archiviazione.
   - Dimensioni: la dimensione del disco (in GB).
   - Regione AWS: Il disco Regione AWS in cui è stato creato.
   - Collegato a: il computer Lightsail a cui è collegato il disco.
   - Data di creazione: la data di creazione del disco.

Aggiungi spazio di archiviazione a un computer virtuale in Lightsail for Research

Completa i seguenti passaggi per collegare un disco a un computer virtuale in Lightsail for Research. Puoi collegare fino a 15 dischi a un computer virtuale. Quando colleghi un disco al tuo computer virtuale utilizzando la console Lightsail for Research, questo viene formattato e montato automaticamente dal servizio. Questo processo richiede alcuni minuti, quindi è necessario verificare che il disco abbia raggiunto lo stato di montaggio Montato prima di iniziare a utilizzarlo. Per impostazione predefinita, Lightsail for Research monta i dischi nella directory; `<disk-name>` dov'è `/home/lightsail-user/<disk-name>` il nome che hai dato al disco.

> **Important**
>
> Prima di poter collegare un disco a un computer virtuale, è necessario che il computer virtuale sia In esecuzione. Se colleghi un disco a un computer virtuale mentre è in uno stato Arrestato, il disco verrà collegato ma non verrà montato. Se lo Stato di montaggio del disco è Non riuscito, devi scollegare il disco e ricollegarlo quando il computer virtuale è In esecuzione.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Computer virtuali.
3. Scegli il computer a cui collegare il disco.
4. Scegli la scheda Archiviazione.
5. Scegli Collega disco.
6. Seleziona il nome del disco da collegare al computer.
7. Scegli Collega.

Scollegare un disco da un computer virtuale in Lightsail for Research

Completa la seguente procedura per scollegare un disco da un computer.

1. Accedi alla console Lightsail for Research.

2. Nel riquadro di navigazione, scegli Archiviazione.
3. Individua il disco da scollegare. Nella colonna Collegato a, scegli il nome del computer a cui è collegato il disco.
4. Scegli Arresta per arrestare il computer. È necessario arrestare il computer prima di poter scollegare il disco.
5. Conferma di voler arrestare il computer, quindi scegli Arresta computer.
6. Scegli la scheda Archiviazione.
7. Seleziona il disco da scollegare, quindi scegli Scollega.
8. Conferma di voler scollegare il disco dal computer, quindi scegli Scollega.

Eliminare i dischi di archiviazione inutilizzati in Lightsail for Research

Completa la seguente procedura per eliminare un disco di archiviazione quando non è più necessario. Non appena viene eliminato, i relativi addebiti vengono interrotti.

Se il disco è collegato a un computer, è necessario innanzitutto scollegarlo prima di poterlo eliminare. Per ulteriori informazioni, consulta Scollegare un disco da un computer virtuale in Lightsail for Research.

1. Accedi alla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Archiviazione.
3. Individua e seleziona il disco da eliminare.
4. Scegli Elimina il disco.
5. Conferma di voler eliminare il disco. Quindi, scegli Elimina.

Backup di computer e dischi virtuali con le istantanee di Lightsail for Research

Le istantanee sono una point-in-time copia dei tuoi dati. Puoi creare istantanee dei tuoi computer virtuali e dischi di archiviazione Amazon Lightsail for Research e usarli come base per creare nuovi computer o per il backup dei dati.

Uno snapshot contiene tutti i dati necessari per ripristinare il computer (dal momento in cui lo snapshot è stato acquisito). Quando si crea un nuovo computer virtuale in base a uno snapshot, il computer è inizialmente l'esatta replica del computer originale utilizzato per creare la snapshot.

Considerando che le tue risorse potrebbero fallire in qualsiasi momento, ti consigliamo di creare snapshot frequenti per evitare la perdita permanente dei dati.

Argomenti

Crea istantanee dei computer o dei dischi virtuali di Lightsail for Research

Completa i seguenti passaggi per creare un'istantanea del tuo computer o disco virtuale Lightsail for Research.

1. Accedi alla console Lightsail for Research.
2. Scegliere Snapshots (Snapshot) nel riquadro di navigazione.
3. Completare una delle seguenti fasi:

    - In Snapshot di computer virtuali, trova il nome del computer di cui desideri eseguire l'istantanea e scegli Crea snapshot.
    - In Snapshot del disco, trova il nome del disco di cui vuoi creare uno snapshot e scegli Crea snapshot.

4. Immettere un nome per lo snapshot. I caratteri validi includono caratteri alfanumerici, numeri, punti, trattini e trattini bassi.

   I nomi degli snapshot devono soddisfare i seguenti requisiti:

   - Sii unico Regione AWS in ognuno dei tuoi account Lightsail for Research.
   - Devono contenere da 2 a 255 caratteri.
   - Devono iniziare e terminare con un carattere alfanumerico o un numero.
5. Scegli Create snapshot (Crea snapshot).

Visualizza e gestisci istantanee di computer e dischi virtuali in Lightsail for Research

Completa i seguenti passaggi per visualizzare gli snapshot dei tuoi dischi e computer virtuali.

1. Accedi alla console Lightsail for Research.
2. Scegliere Snapshots (Snapshot) nel riquadro di navigazione.

   La pagina Snapshot mostra gli snapshot del computer virtuale e del disco che hai creato.

   Anche gli snapshot archiviati si trovano in questa pagina. Gli snapshot archiviati sono istantanee di risorse che sono state eliminate dall'account.

Crea un computer o un disco virtuale da uno snapshot

Completa i seguenti passaggi per creare un nuovo computer o disco virtuale Lightsail for Research da un'istantanea.

Quando crei un computer virtuale da uno snapshot, utilizza un piano delle stesse dimensioni o superiori a quello utilizzato per il computer originale. Non è possibile utilizzare un piano inferiore al computer virtuale originale.

Quando crei un disco da uno snapshot, scegli una dimensione del disco superiore al disco originale. Non puoi usare un disco più piccolo dell'originale.

1. Accedi alla console Lightsail for Research.
2. Scegliere Snapshots (Snapshot) nel riquadro di navigazione.

3. Nella pagina Snapshot, individua il nome dello snapshot del computer o del disco che utilizzerai per creare il nuovo computer o disco. Scegli il menu a discesa Snapshot per visualizzare un elenco di snapshot disponibili per quella risorsa.
4. Scegli lo snapshot da utilizzare per creare il computer virtuale.
5. Scegli il menu a discesa Operazione. Quindi, scegli Crea computer virtuale o Crea disco.

Eliminare un'istantanea nella console Lightsail for Research

Per eliminare uno snapshot, completa le fasi seguenti.

1. Accedi alla console Lightsail for Research.
2. Scegliere Snapshots (Snapshot) nel riquadro di navigazione.
3. Nella pagina Snapshot, individua il nome dello snapshot del computer o del disco che desideri eliminare. Scegli il menu a discesa Snapshot per visualizzare un elenco di snapshot disponibili per quella risorsa.
4. Scegli lo snapshot da eliminare.
5. Scegli il menu a discesa Operazione. Quindi scegli Elimina snapshot.
6. Verificare che il nome dello snapshot sia corretto. Quindi scegli Elimina snapshot.

Stime dei costi e dell'utilizzo in Lightsail for Research

Amazon Lightsail for Research offre stime dei costi e dell'utilizzo delle tue risorse. AWS Puoi utilizzare queste stime per pianificare la spesa, trovare opportunità di risparmio sui costi e prendere decisioni informate quando utilizzi Lightsail for Research.

Quando si crea un computer o un disco virtuale, vengono visualizzate le stime dei costi e dell'utilizzo per quella risorsa. Una stima dei costi e dell'utilizzo inizia a essere registrata non appena una risorsa viene creata e si trova nello stato Disponibile o In esecuzione. La stima verrà visualizzata nella Console di gestione AWS entro 15 minuti dalla creazione della risorsa. Le risorse eliminate non sono incluse in una stima.

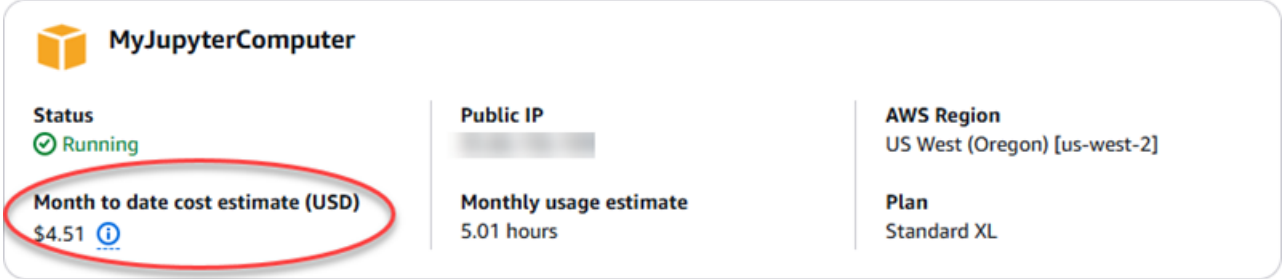
> **Important**
>
> Una stima è un costo stimato basato sull'utilizzo della risorsa. Il costo effettivo si baserà sull'uso effettivo delle risorse, non sulla stima mostrata nella console Lightsail for Research. I costi effettivi sono indicati nell'estratto AWS Billing conto.
> Accedi a Console di gestione AWS e apri la Gestione dei costi e fatturazione AWS console all'indirizzo https://console.aws.amazon.com/costmanagement/.

Argomenti

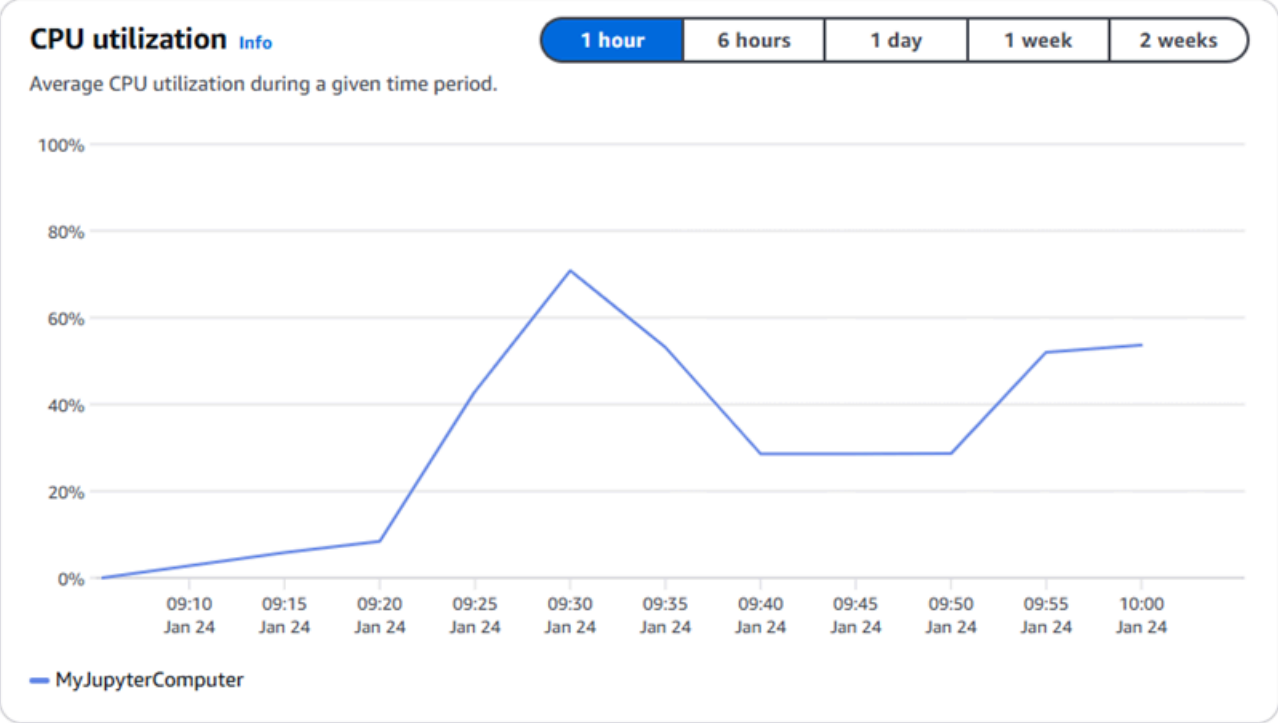
Visualizza le stime dei costi e dell'utilizzo delle tue risorse in Lightsail for Research

Le stime mensili dei costi e dell'utilizzo delle risorse Lightsail for Research sono visualizzate nelle seguenti aree della console Lightsail for Research.

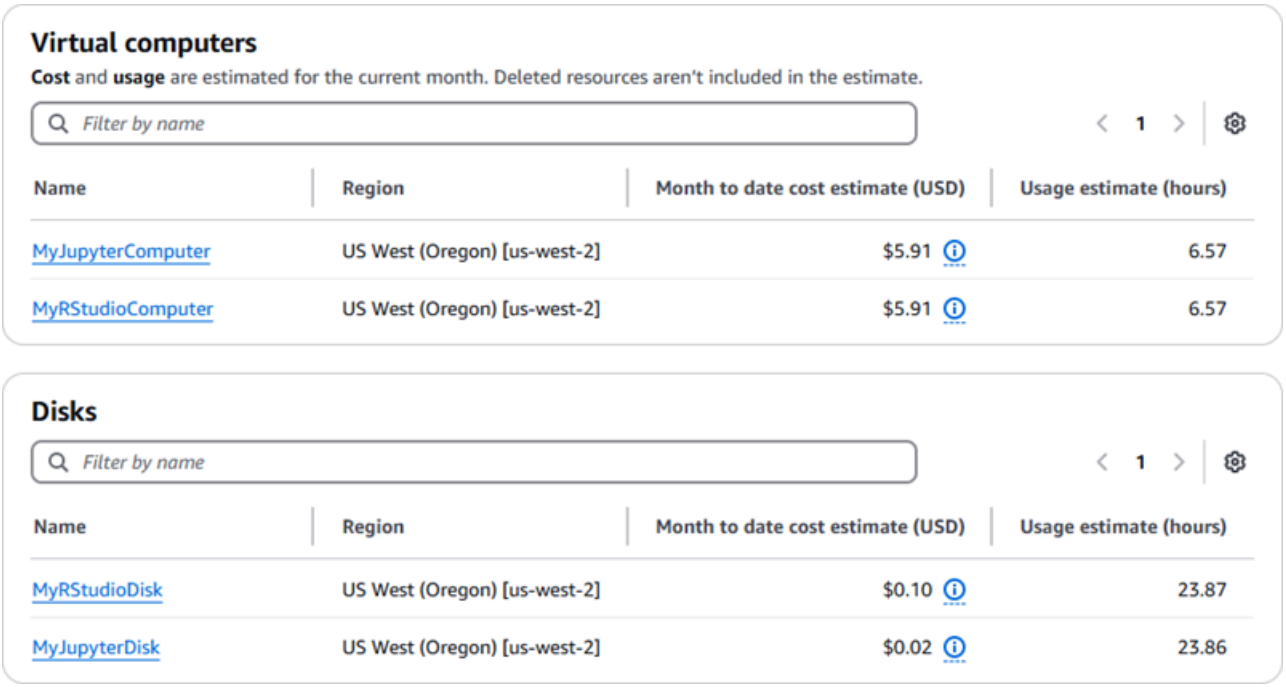
1. Scegli Computer virtuali nel pannello di navigazione della console Lightsail for Research. La stima dei costi mensili ad oggi per i computer virtuali è elencata sotto ogni computer virtuale in esecuzione.



2. Per visualizzare l'utilizzo della CPU per un computer virtuale, scegli il nome del computer virtuale, quindi scegli la scheda Pannello di controllo.



3. Per visualizzare le stime di costo e utilizzo mensili per tutte le risorse di Lightsail for Research, scegli Utilizzo nel pannello di navigazione.


Virtual computers
Cost and usage are estimated for the current month. Deleted resources aren't included in the estimate.
Filter by name
1
Name
Region
Month to date cost estimate (USD)
Usage estimate (hours)
MyJupyterComputer
US West (Oregon) [us-west-2]
$5.91
6.57
MyRStudioComputer
US West (Oregon) [us-west-2]
$5.91
6.57
Disks
Filter by name
1
Name
Region
Month to date cost estimate (USD)
Usage estimate (hours)
MyRStudioDisk
US West (Oregon) [us-west-2]
$0.10
23.87
MyJupyterDisk
US West (Oregon) [us-west-2]
$0.02
23.86

Gestisci le regole di controllo dei costi in Lightsail for Research

Il controllo dei costi utilizza regole definite dall'utente per aiutare a gestire l'utilizzo e i costi dei computer virtuali Lightsail for Research.

È possibile creare una regola Arresta computer virtuale su inattivo che arresta un computer in esecuzione quando raggiunge una determinata percentuale di utilizzo della CPU durante un determinato periodo. Ad esempio, una regola può arrestare automaticamente un computer specifico quando l'utilizzo della CPU è pari o inferiore al 5% per un periodo di 30 minuti. Ciò significa che il computer è inattivo e Lightsail for Research lo arresta. Dopo l'arresto del computer virtuale non verranno più addebitati i costi orari standard.

Argomenti

Crea regole di controllo dei costi per i tuoi computer virtuali Lightsail for Research

Completa i seguenti passaggi per creare una regola per il tuo computer virtuale Lightsail for Research.

> **Note**
>
> L'unica azione della regola supportata in questo momento è l'arresto di un computer virtuale. L'utilizzo della CPU è l'unica metrica attualmente monitorata dalle regole e l'unica operazione supportata è inferiore o uguale a.

1. Accedi alla console Lightsail for Research.
2. Scegli Controllo dei costi nel riquadro di navigazione.
3. Scegli Crea regola.
4. Seleziona la risorsa a cui applicare la regola.

5. Specifica la percentuale di utilizzo della CPU e il periodo di tempo in cui la regola deve essere eseguita.

   Ad esempio, è possibile specificare il 5% e 30 minuti. Lightsail for Research arresta automaticamente il computer quando l'utilizzo della CPU è inferiore o uguale al 5% per un periodo di 30 minuti.
6. Scegli Crea regola.
7. Conferma che le informazioni per la nuova regola siano corrette, quindi scegli Conferma.

Eliminare le regole di controllo dei costi per i computer virtuali Lightsail for Research

Completa i seguenti passaggi per eliminare una regola per il tuo computer virtuale Lightsail for Research.

1. Accedi alla console Lightsail for Research.
2. Scegli Controllo dei costi nel riquadro di navigazione.
3. Selezionare la regola da eliminare.
4. Scegli Elimina.
5. Verifica di voler eliminare la regola, quindi scegli Elimina.

Organizza le risorse di Lightsail for Research con i tag

Con Amazon Lightsail for Research, puoi assegnare tag alle tue risorse. Ogni tag è un'etichetta costituita da una chiave e un valore facoltativo che può rendere efficienti la gestione delle risorse. Una chiave senza valore viene definita tag di sola chiave, mentre una chiave con un valore viene definita tag chiave-valore. Anche se non ci sono tipi di tag inerenti, i tag consentono di suddividere le risorse in base a scopo, proprietario, ambiente o altri criteri. Questa funzione è utile quando si dispone di numerose risorse dello stesso tipo. Puoi identificare velocemente una risorsa specifica in base ai tag a questa assegnati. Ad esempio, puoi definire un set di tag che aiuti a monitorare il progetto o la priorità di ogni risorsa.

Le seguenti risorse possono essere taggate nella console Amazon Lightsail for Research:

- Computer virtuali
- Dischi di archiviazione
- Snapshot

Ai tag si applicano le limitazioni seguenti:

- Il numero massimo di tag per risorsa è 50.
- Per ogni risorsa, la chiave di ciascun tag deve essere univoca. La chiave di ogni tag può avere solo un valore.
- La lunghezza massima delle chiavi è 128 caratteri Unicode in UTF-8.
- Il valore massimo è 256 caratteri Unicode in UTF-8.
- Se lo schema di tagging viene utilizzato in più servizi e risorse, è necessario tenere presente che in altri servizi possono essere presenti limiti sui caratteri consentiti. I caratteri generalmente consentiti sono lettere, numeri, spazi e i simboli seguenti: `+ - = . _ : / @`
- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole.
- Non utilizzare il prefisso `aws:` per le chiavi o i valori. Questo prefisso è riservato all'uso. AWS

Argomenti

Tagga Lightsail for Research: risorse

Completa i seguenti passaggi per creare un tag per il tuo computer virtuale Lightsail for Research. I passaggi sono simili per i dischi e le istantanee di Lightsail for Research.

1. Accedi alla console Lightsail for Research sulla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Computer virtuali.
3. Scegli il computer virtuale per il quale desideri creare un tag.
4. Seleziona la scheda Tags (Tag).
5. Scegliere Gestisci tag.
6. Scegliere Aggiungi nuovo tag.
7. Immetti un nome chiave nel campo Chiave. Ad esempio, Progetto.
8. (Facoltativo) Immetti un nome valore nel campo valore. Ad esempio, Blog.
9. Scegli Salva modifiche per salvare la chiave sul tuo computer virtuale.

Rimuovi i tag dalle risorse di Lightsail for Research

Completa i seguenti passaggi per eliminare un tag dal tuo computer virtuale Lightsail for Research. I passaggi sono simili per i dischi e le istantanee di Lightsail for Research.

1. Accedi alla console Lightsail for Research sulla console Lightsail for Research.
2. Nel riquadro di navigazione, scegli Computer virtuali.
3. Scegli il computer virtuale da cui desideri eliminare il tag.
4. Seleziona la scheda Tags (Tag).
5. Scegliere Gestisci tag.
6. Scegli Rimuovi per eliminare il tag dalla risorsa.

> **Note**
>
> Se desideri rimuovere solo il valore del tag, individua il valore, quindi scegli l'icona X accanto ad esso.

7. Scegli Save changes (Salva modifiche).

Sicurezza in Amazon Lightsail for Research

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per informazioni sui programmi di conformità applicabili ad Amazon Lightsail for Research, AWS consulta Services in Scope by Compliance AWS Program Services in Scope by Compliance .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Lightsail for Research. I seguenti argomenti mostrano come configurare Lightsail for Research per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Lightsail for Research.

Argomenti

Protezione dei dati in Amazon Lightsail for Research

Il modello di responsabilità AWS condivisa modello si applica alla protezione dei dati in Amazon Lightsail for Research. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i. Cloud AWS L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al AWS Modello di responsabilità condivisa e GDPR nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Lightsail for Research o Servizi AWS altro utilizzando la console, l'API AWS CLI o. AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un

server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Identity and Access Management per Amazon Lightsail for Research

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (dispone delle autorizzazioni) a utilizzare le risorse di Lightsail for Research. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

> **Note**
>
> Amazon Lightsail e Lightsail for Research condividono gli stessi parametri delle policy IAM. Le modifiche apportate alle politiche di Lightsail for Research influiranno anche sulle politiche di Lightsail. Ad esempio, se un utente è autorizzato a creare un disco in Lightsail for Research, lo stesso utente può creare un disco anche in Lightsail.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Lightsail for Research)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come funziona Amazon Lightsail for Research con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità per Amazon Lightsail for Research)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon Lightsail for Research con IAM

Prima di utilizzare IAM per gestire l'accesso a Lightsail for Research, scopri quali funzionalità IAM sono disponibili per l'uso con Lightsail for Research.

Funzionalità IAM che puoi utilizzare con Amazon Lightsail for Research

Funzionalità IAM	Supporto Lightsail for Research
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì

Funzionalità IAM	Supporto Lightsail for Research
Autorizzazioni del principale	No
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una visione di alto livello di come Lightsail for Research e AWS altri servizi funzionano con la maggior parte delle funzionalità IAM, AWS consulta i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Lightsail for Research

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Esempi di policy basate sull'identità per Lightsail for Research

Per visualizzare esempi di politiche basate sull'identità di Lightsail for Research, consulta. Esempi di policy basate sull'identità per Amazon Lightsail for Research

Politiche basate sulle risorse all'interno di Lightsail for Research

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket

Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per Lightsail for Research

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di Lightsail for Research, consulta Azioni definite da Amazon Lightsail for Research nel Service Authorization Reference.

Le azioni politiche in Lightsail for Research utilizzano il seguente prefisso prima dell'azione:

```
lightsail
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

Per visualizzare esempi di politiche basate sull'identità di Lightsail for Research, consulta. Esempi di policy basate sull'identità per Amazon Lightsail for Research

Risorse politiche per Lightsail for Research

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Per visualizzare un elenco dei tipi di risorse di Lightsail for Research e ARNs relativi, consulta Resources Defined by Amazon Lightsail for Research nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon Lightsail for Research.

Per visualizzare esempi di politiche basate sull'identità di Lightsail for Research, consulta. Esempi di policy basate sull'identità per Amazon Lightsail for Research

Chiavi relative alle condizioni delle politiche per Lightsail for Research

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco dei codici di condizione di Lightsail for Research, consulta Condition Keys for Amazon Lightsail for Research nel Service Authorization Reference. Per sapere con quali azioni

e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon Lightsail for Research.

Per visualizzare esempi di politiche basate sull'identità di Lightsail for Research, consulta. Esempi di policy basate sull'identità per Amazon Lightsail for Research

ACLs in Lightsail per la ricerca

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Lightsail per la ricerca

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Lightsail for Research

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare

dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Autorizzazioni principali multiservizio per Lightsail for Research

Supporta l'inoltro delle sessioni di accesso (FAS): no

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta per effettuare richieste ai servizi Servizio AWS downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Lightsail for Research

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Lightsail for Research. Modifica i ruoli di servizio solo quando Lightsail for Research fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Lightsail for Research

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked

role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon Lightsail for Research

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare le risorse di Lightsail for Research. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Lightsail for Research, incluso il formato di per ogni tipo di ARNs risorsa, consulta Actions, Resources and Condition Keys for Amazon Lightsail for Research nel Service Authorization Reference.

Argomenti

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse Lightsail for Research nel tuo account. Queste azioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM

per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.

- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Lightsail for Research

Per accedere alla console Amazon Lightsail for Research, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Lightsail for Research presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso o l' AWS CLI API. AWS Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano continuare a utilizzare la console Lightsail for Research, allega anche la policy Lightsail for `ConsoleAccess` Research o la policy gestita alle entità.

ReadOnly AWS Per maggiori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Lightsail for Research

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Lightsail for Research e IAM.

Argomenti

Non sono autorizzato a eseguire un'azione in Lightsail for Research

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `lightsail:`*`GetWidget`* fittizie.

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

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `lightsail:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Lightsail for Research

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo.

Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Lightsail for Research supporta queste funzionalità, consulta. Come funziona Amazon Lightsail for Research con IAM
- Per scoprire come fornire l'accesso alle risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM di un altro Account AWS utente di tua proprietà nella Guida per l'utente IAM. Account AWS
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Convalida della conformità per Amazon Lightsail for Research

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta AWS la documentazione sulla sicurezza.

Resilienza in Amazon Lightsail for Research

L'infrastruttura AWS globale è costruita attorno a zone di disponibilità. Regioni AWS Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità è possibile progettare e gestire

applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Oltre all'infrastruttura AWS globale, Lightsail for Research offre diverse funzionalità per aiutarti a supportare le tue esigenze di resilienza e backup dei dati. Per ulteriori informazioni, consultare Backup di computer e dischi virtuali con le istantanee di Lightsail for Research e Crea istantanee dei computer o dei dischi virtuali di Lightsail for Research.

Sicurezza dell'infrastruttura in Amazon Lightsail for Research

In quanto servizio gestito, Amazon Lightsail for Research è protetto dalla sicurezza AWS della rete globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a Lightsail for Research attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa è possibile utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Analisi della configurazione e delle vulnerabilità in Amazon Lightsail for Research

La configurazione e i controlli IT sono una responsabilità condivisa tra te AWS e te, nostro cliente. Per ulteriori informazioni, consulta il modello di responsabilità AWS condivisa.

Best practice di sicurezza per Amazon Lightsail for Research

Lightsail for Research offre una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l’ambiente, sono da considerare come considerazioni utili anziché prescrizioni.

Per prevenire potenziali eventi di sicurezza associati all'uso di Lightsail for Research, segui queste best practice:

- Accedi alla console Lightsail for Research autenticandoti sulla prima. Console di gestione AWS Non condividere le credenziali della console personale. Tutti gli utenti di Internet possono accedere alla console, ma non possono accedere o avviare una sessione se non dispongono di credenziali valide per la console.

Cronologia dei documenti per la Guida per l'utente di Lightsail for Research

La tabella seguente descrive le versioni della documentazione per Lightsail for Research.

Modifica	Descrizione	Data
Versione iniziale	Versione iniziale della Guida per l'utente di Lightsail for Research.	28 febbraio 2023

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.