



Guida per l'utente

Amazon Lightsail per la ricerca



Amazon Lightsail per la ricerca: Guida per l'utente

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

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà delle rispettive aziende, che possono o meno essere associate, collegate o sponsorizzate da Amazon.

Table of Contents

Cos'è Amazon Lightsail for Research?	1
Prezzi	1
Disponibilità	1
Configurazione	2
Registrati per un Account AWS	2
Crea un utente con accesso amministrativo	2
Guida introduttiva	4
Fase 1: completamento dei prerequisiti	4
Fase 2: crea un computer virtuale	4
Fase 3: avvio dell'applicazione di un computer virtuale	5
Fase 4: collegati al computer virtuale	6
Fase 5: aggiunta di storage al computer virtuale	7
Fase 6: Creazione di una snapshot DB	8
Fase 7: pulire	8
Tutorial	10
Inizia con JupyterLab	10
Fase 1: completamento dei prerequisiti	11
Fase 2: (facoltativa) aggiunta di spazio di archiviazione	11
Fase 3: caricamento e download di file	11
Fase 4: Avviare l' JupyterLab applicazione	12
Fase 5: Leggi la JupyterLab documentazione	16
Fase 6: (facoltativa) monitoraggio dell'utilizzo e dei costi	16
Fase 7: (facoltativa) creazione di una regola di controllo dei costi	18
Fase 8: (facoltativa) creazione di uno snapshot	19
Fase 9: (facoltativa) arrestare o eliminare il computer virtuale	19
Inizia con RStudio	20
Fase 1: completamento dei prerequisiti	21
Fase 2: (facoltativa) aggiunta di spazio di archiviazione	21
Fase 3: caricamento e download di file	22
Fase 4: Avvia l'applicazione RStudio	22
Fase 5: Leggi la RStudio documentazione	26
Fase 6: (facoltativa) monitoraggio dell'utilizzo e dei costi	28
Fase 7: (facoltativa) creazione di una regola di controllo dei costi	29
Fase 8: (facoltativa) creazione di uno snapshot	30

Fase 9: (facoltativa) arrestare o eliminare il computer virtuale	30
Computer virtuali	32
Applicazioni e piani hardware	32
Applicazioni	33
Piani	34
Crea un computer virtuale	35
Visualizza i dettagli del computer virtuale	36
Avvia l'applicazione di un computer virtuale	37
Accedi al sistema operativo di un computer virtuale	38
Porte firewall	39
Protocolli	39
Porte	40
Perché aprire e chiudere le porte	40
Completa i prerequisiti	41
Ottieni gli stati delle porte per un computer virtuale	41
Aprire le porte per un computer virtuale	42
Chiudere le porte di un computer virtuale	44
Passa alle fasi successive	45
Procurati una coppia di chiavi per un computer virtuale	46
Completa i prerequisiti	47
Procurati una coppia di chiavi per un computer virtuale	47
Passa alle fasi successive	52
Connect a un computer virtuale tramite SSH	53
Completa i prerequisiti	53
Connect a un computer virtuale tramite SSH	54
Passa alle fasi successive	60
Trasferisci file su un computer virtuale utilizzando SCP	61
Completa i prerequisiti	61
Connect a un computer virtuale tramite SCP	62
Eliminazione di un computer virtuale	66
Storage	67
Creazione di un disco	67
Visualizza i dischi	68
Collega un disco a un computer virtuale	69
Scollega un disco da un computer virtuale	69
Eliminazione di un disco	70

Snapshot	71
Crea snapshot	71
Visualizza gli snapshot	72
Crea un computer o un disco virtuale da uno snapshot	72
Elimina lo snapshot	73
Costi e utilizzo	74
Visualizza costi e utilizzo	74
Regole di controllo dei costi	77
Creazione di una regola	77
Eliminare una regola	78
Tag	79
Creazione di un tag	80
Eliminare un tag	80
Sicurezza	81
Protezione dei dati	82
Identity and Access Management	83
Destinatari	83
Autenticazione con identità	84
Gestione dell'accesso con policy	88
Come funziona Amazon Lightsail for Research con IAM	90
Esempi di policy basate su identità	97
Risoluzione dei problemi	100
Convalida della conformità	101
Resilienza	103
Sicurezza dell'infrastruttura	103
Analisi della configurazione e delle vulnerabilità	104
Best practice di sicurezza	104
Cronologia dei documenti	105
.....	cvi

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 documento disponibile al pubblico. Scopri come installare e utilizzare [AWS CLI](#) e [API](#) 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, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene 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 [AWS Management Console](#) come 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. Attiva l'autenticazione a più fattori (MFA) per il tuo utente root.

Per istruzioni, consulta [Abilitare un MFA dispositivo virtuale per l'utente Account AWS root \(console\)](#) nella Guida per l'IAMutente.

Crea un utente con accesso amministrativo

1. Abilita IAM Identity Center.

Per istruzioni, consulta [Abilitazione di AWS IAM Identity Center](#) nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, concedi 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 i valori predefiniti IAM Identity Center directory](#) nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

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

Per informazioni sull'accesso tramite un utente di IAM Identity Center, consulta [Accesso al portale di AWS 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 che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

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](#)
- [Fase 2: crea un computer virtuale](#)
- [Fase 3: avvio dell'applicazione di un computer virtuale](#)
- [Fase 4: collegati al computer virtuale](#)
- [Fase 5: aggiunta di storage al computer virtuale](#)
- [Fase 6: Creazione di una snapshot DB](#)
- [Fase 7: pulire](#)

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. Seleziona una 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 in 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 in API Lightsail.

I piani hardware offrono diverse quantità di potenza di elaborazione, tra cui v CPU core, memoria, archiviazione e trasferimento dati mensile. Lightsail for Research offre piani standard GPU e piani per computer virtuali. Scegli un piano standard quando i requisiti computazionali dell'attività sono bassi. Scegli un GPU piano quando tale requisito è elevato, ad esempio quando esegui modelli di apprendimento automatico 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 NICE DCV client basato su browser disponibile nella console Lightsail for Research. Con NICE DCV, puoi utilizzare un'interfaccia utente grafica (GUI) per interagire con l'applicazione di ricerca e il sistema operativo del tuo computer virtuale.

È inoltre possibile accedere all'interfaccia a riga di comando del computer virtuale e trasferire file utilizzando il client basato su browser NICE DCV.

- Usa un client secure shell (SSH) come Open SSHTTY, Pu o Windows Subsystem for Linux per accedere all'interfaccia a riga di comando del tuo computer virtuale. Con un SSH client, puoi modificare script e file di configurazione.
- Utilizzate Secure Copy (SCP) per trasferire in modo sicuro i file tra il computer locale e il 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 key pair del computer virtuale per connettersi al computer virtuale SSH o per trasferire file utilizzando 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 SSH connessione o trasferisci file utilizzando: 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'istananea nella console Lightsail for Research](#)

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

Fase 7: pulire

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, consulta [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 key pair, è possibile utilizzarla per stabilire una connessione utilizzando l'utilità Secure Copy (SCP). SCP 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 key pair per connetterti al tuo computer virtuale con SSH. Per ulteriori informazioni, consulta [Connect a un computer virtuale Lightsail for Research tramite Secure Shell](#).

Note

È inoltre possibile accedere all'interfaccia a riga di comando del computer virtuale e trasferire file utilizzando il client basato su browser NICEDEV. NICEDEV è disponibile nella console Lightsail for Research. Per ulteriori informazioni, consulta [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 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

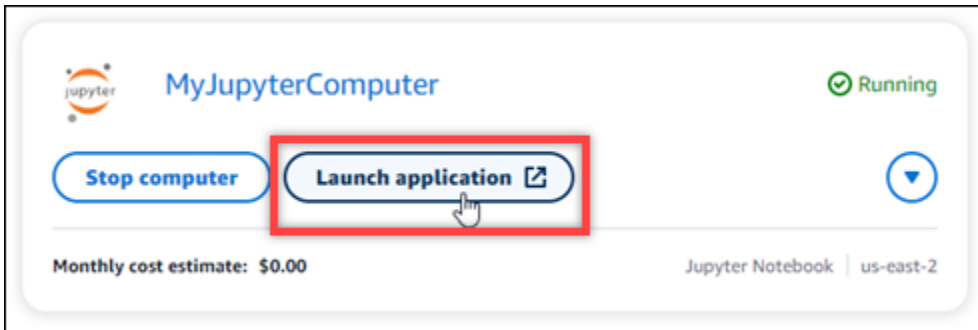
Completa la seguente procedura per avviare l' JupyterLab applicazione sul tuo nuovo computer virtuale.

Important

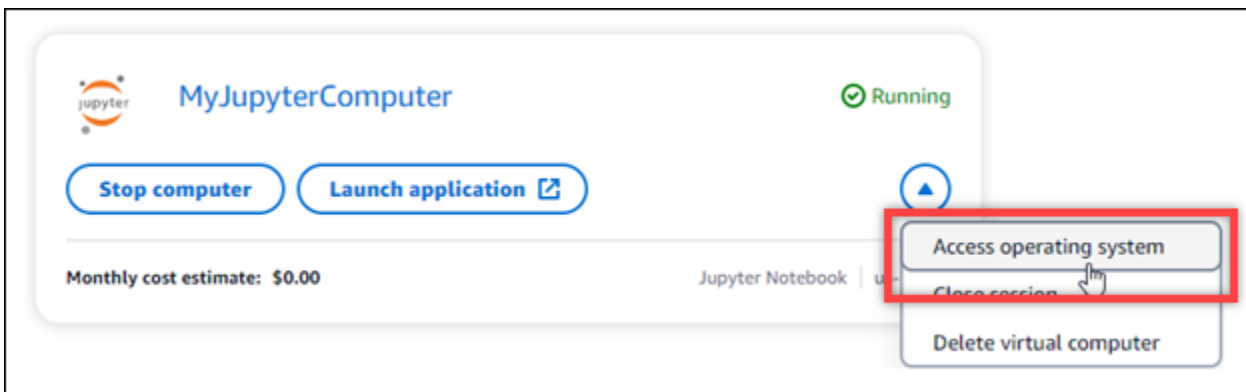
Non aggiornate il sistema operativo o l' JupyterLab applicazione anche se vi viene richiesto di farlo. Scegli invece l'opzione per chiudere o ignorare queste istruzioni. Inoltre, non modificate nessuno dei file che si trovano nella directory `/home/lightsail-admin/`. Queste azioni potrebbero rendere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



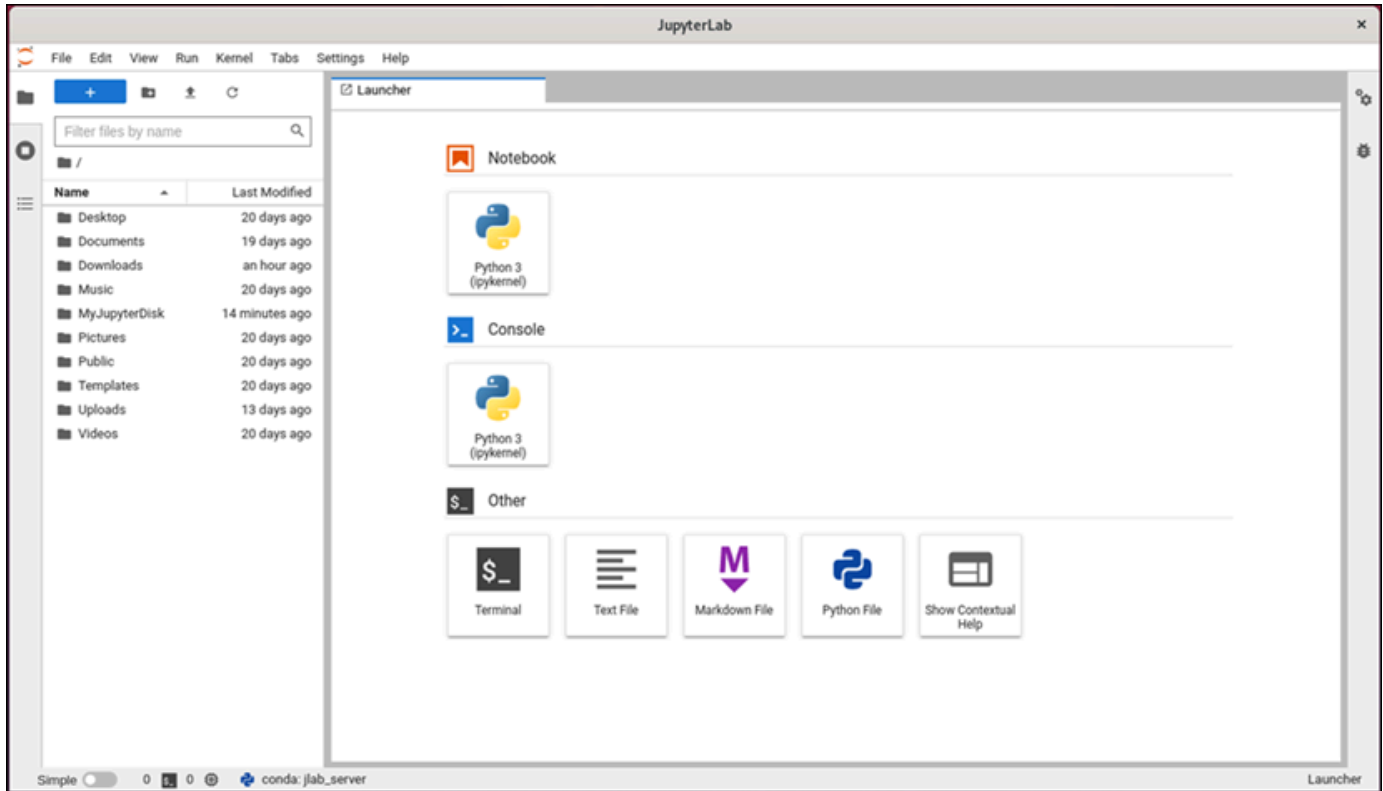
Lightsail for Research esegue alcuni comandi per avviare la connessione al protocollo di visualizzazione remota. Dopo alcuni istanti, si apre una nuova finestra della scheda del browser con una connessione desktop virtuale stabilita al computer virtuale. Se avete scelto l'opzione Avvia applicazione, 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.

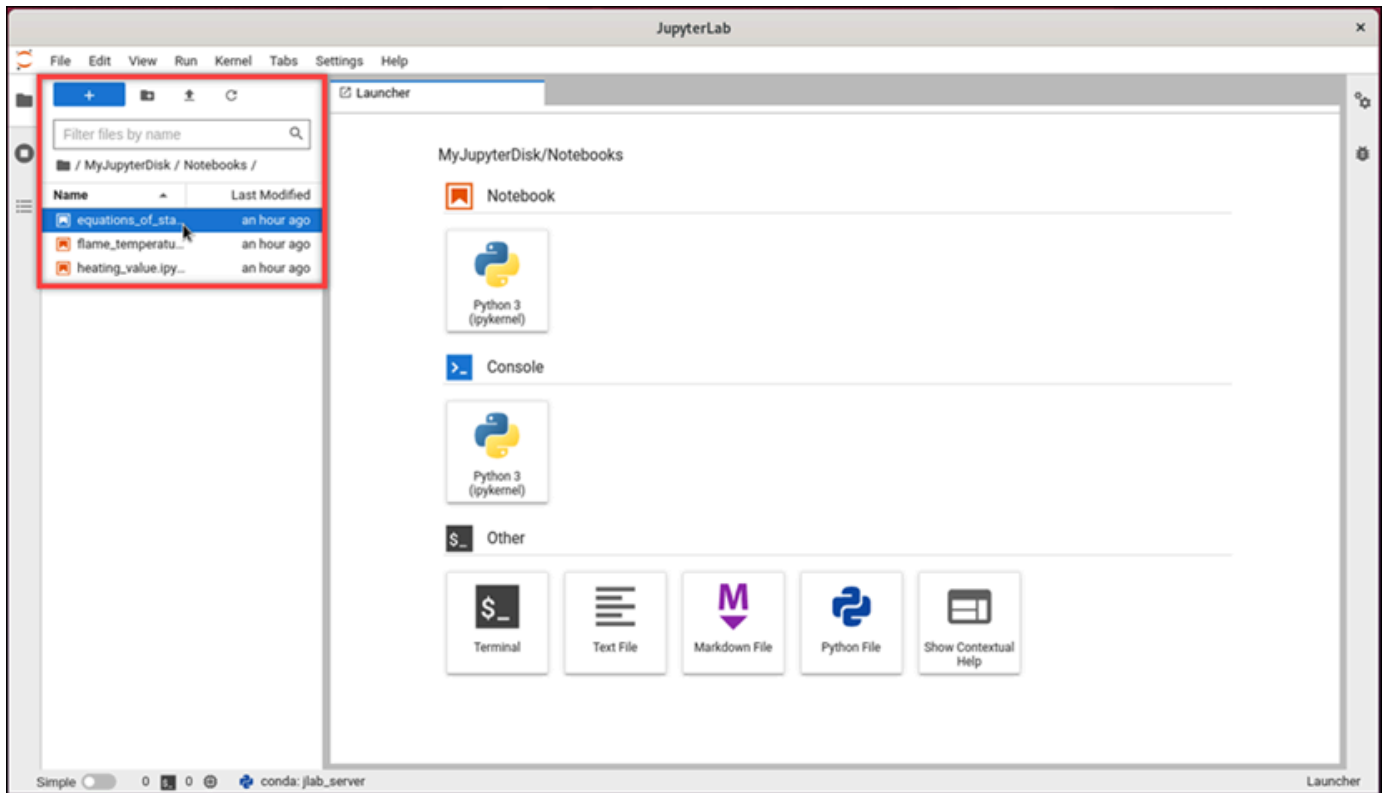
Ubuntu potrebbe anche richiedere una configurazione iniziale. Segui le istruzioni fino al completamento della configurazione e potrai utilizzare il sistema operativo.

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

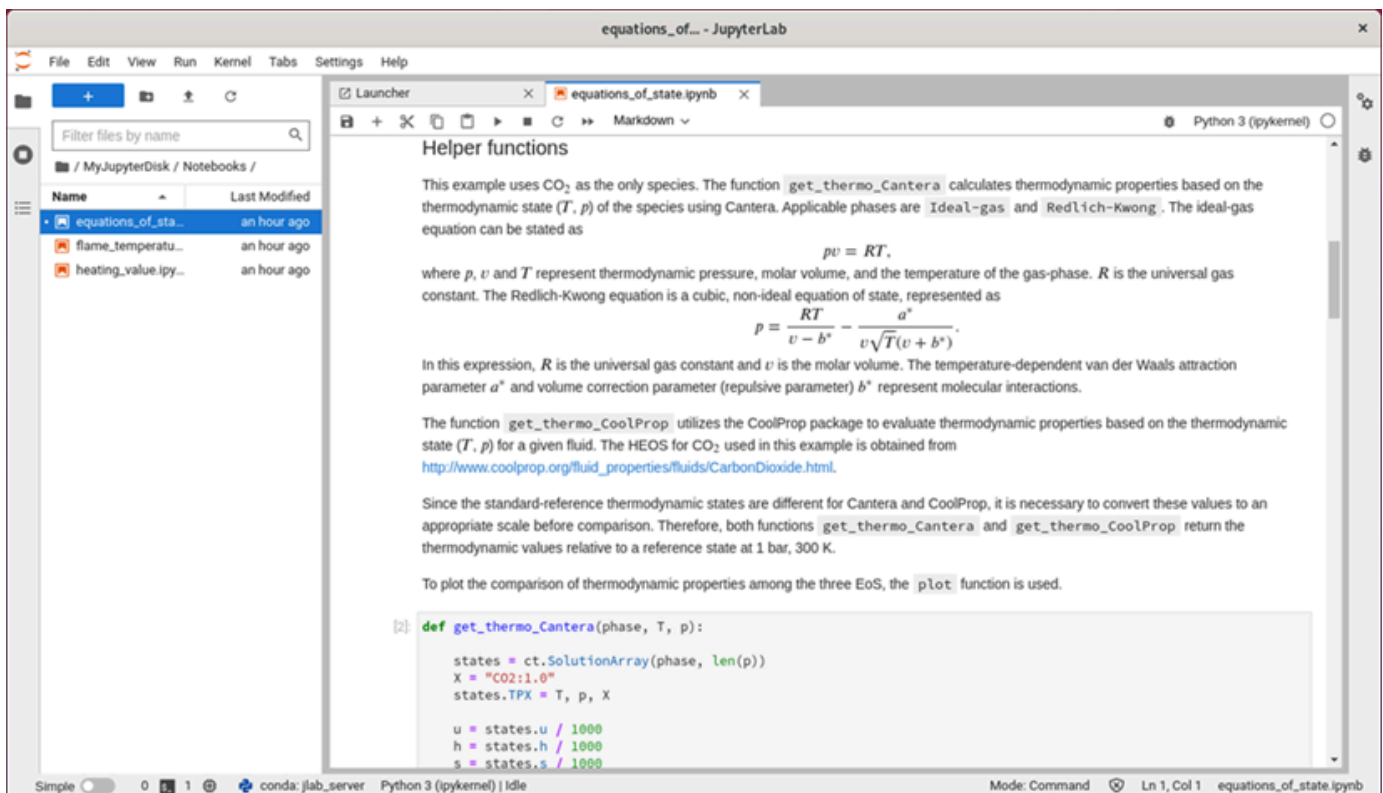


- Per aprire un file JupyterLab, nel riquadro File Browser, scegliete la directory o la cartella in cui sono archiviati i file del progetto. Quindi scegli il file da aprire.

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

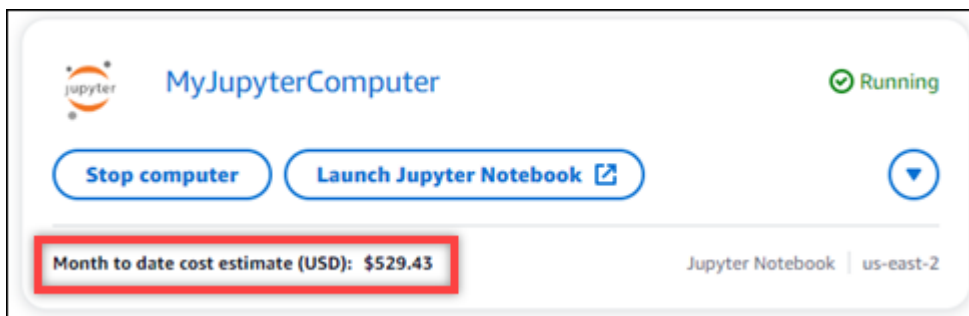
Se non li conosci JupyterLab, ti consigliamo di leggere la loro documentazione ufficiale. Sono disponibili le seguenti risorse JupyterLab online:

- [JupyterLab Documentazione](#)
- [Forum di discussione di Jupyter](#)
- [JupyterLab su StackOverflow](#)
- [JupyterLab su GitHub](#)

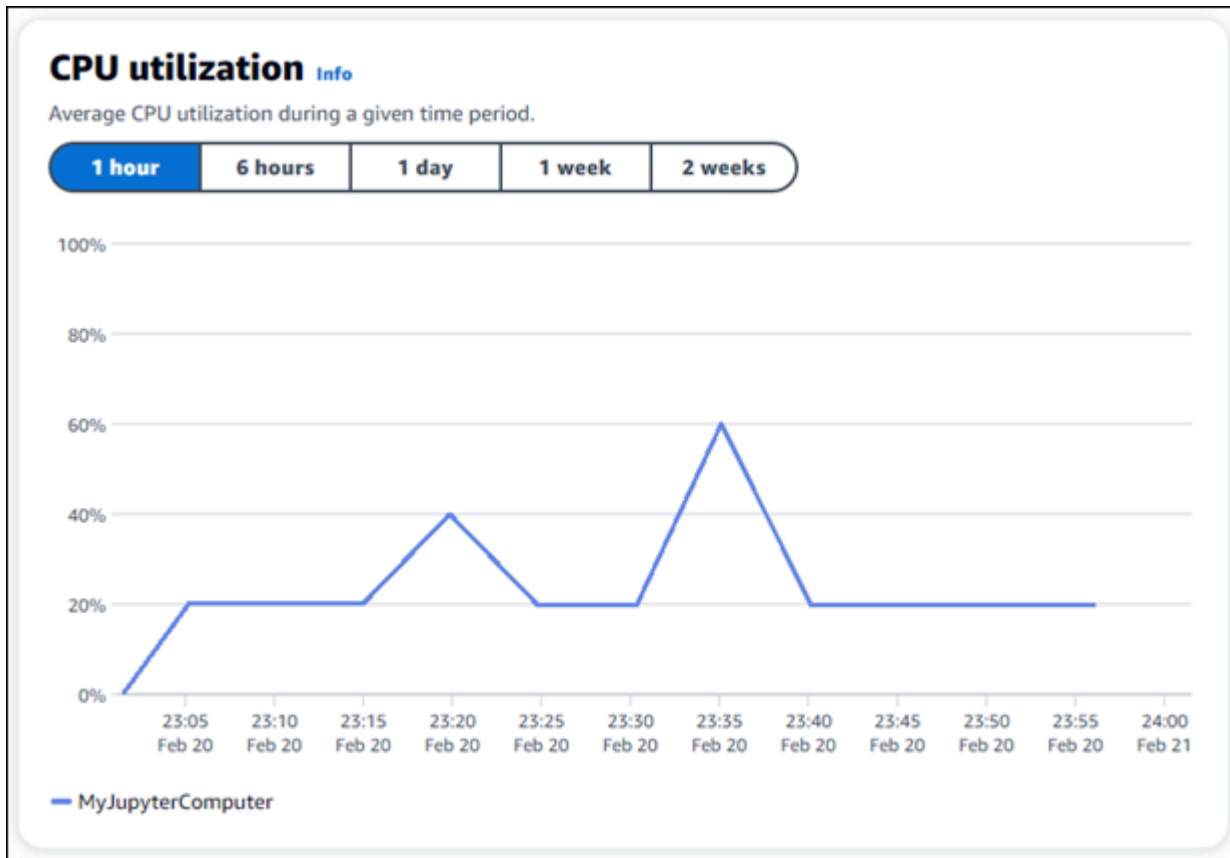
Fase 6: (facoltativa) monitoraggio dell'utilizzo e dei costi

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'CPU utilizzo di un computer virtuale, scegli il nome del computer virtuale, quindi scegli la scheda Dashboard.



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.

Q Filter by name < 1 > ⚙

Name	Region	Month to date cost estimate (USD)	Usage estimate (hours)
MyJupyterComputer	us-east-2	\$529.43	346.02
MyJupyterComputer2	us-east-2	\$241.21	157.65
MyRStudioComputer	us-east-2	\$530.58	346.78

Disks

Q Filter by name < 1 > ⚙

Name	Region	Month to date cost estimate (USD)	Usage estimate (GB)
MyDisk	us-east-2	\$0.45	0.15
MyFirstDisk	us-west-2	\$0.61	0.81
MyRStudioDisk	us-west-2	\$0.58	0.77

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 Stop virtual computer on idle che arresta un computer in esecuzione quando raggiunge una determinata percentuale di CPU utilizzo durante un determinato periodo. Ad esempio, una regola può arrestare automaticamente un computer specifico quando il suo CPU utilizzo 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 fermare il computer virtuale in stato di inattività, ti consigliamo di monitorarne l'utilizzo per alcuni giorni. CPU Prendi nota dell'CPUUtilizzo 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 si crea una regola con una soglia di CPU utilizzo superiore al carico di lavoro, la regola può interrompere 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 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).

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'istananea 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](#)
- [Fase 2: \(facoltativa\) aggiunta di spazio di archiviazione](#)
- [Fase 3: caricamento e download di file](#)
- [Fase 4: Avvia l'applicazione RStudio](#)
- [Fase 5: Leggi la RStudio 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'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, consulta [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 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 key pair, è possibile utilizzarla per stabilire una connessione utilizzando l'utilità Secure Copy (SCP). SCP 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 key pair per connetterti al tuo computer virtuale con SSH. Per ulteriori informazioni, consulta [Connect a un computer virtuale Lightsail for Research tramite Secure Shell](#).

Note

È inoltre possibile accedere all'interfaccia a riga di comando del computer virtuale e trasferire file utilizzando il client basato su browser NICEDEV. NICEDEV è disponibile nella console Lightsail for Research. Per ulteriori informazioni, consulta [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

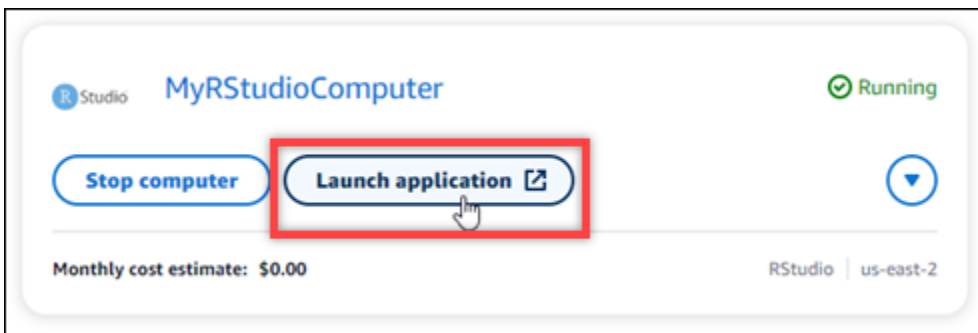
Completa la seguente procedura per avviare l'RStudio applicazione sul tuo nuovo computer virtuale.

Important

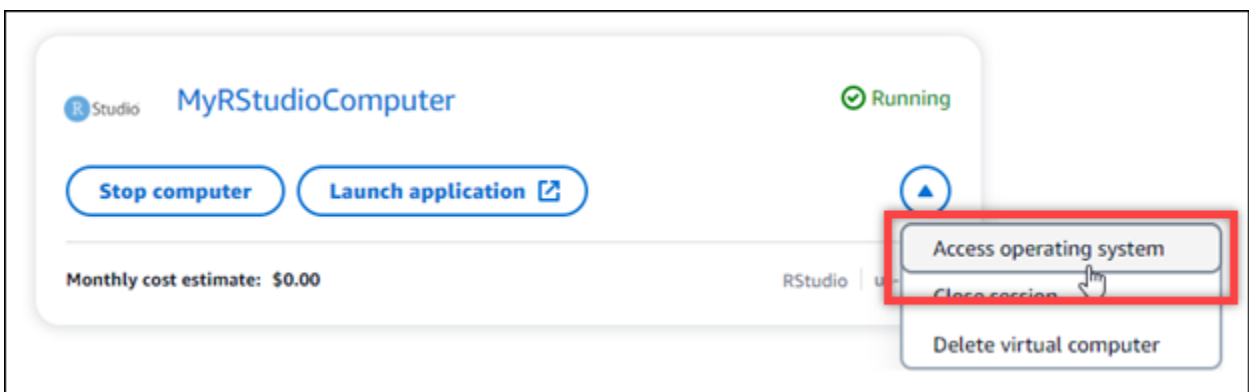
Non aggiornate il sistema operativo o l'RStudio applicazione anche se vi viene richiesto di farlo. Scegli invece l'opzione per chiudere o ignorare queste istruzioni. Inoltre, non

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 applicazione 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

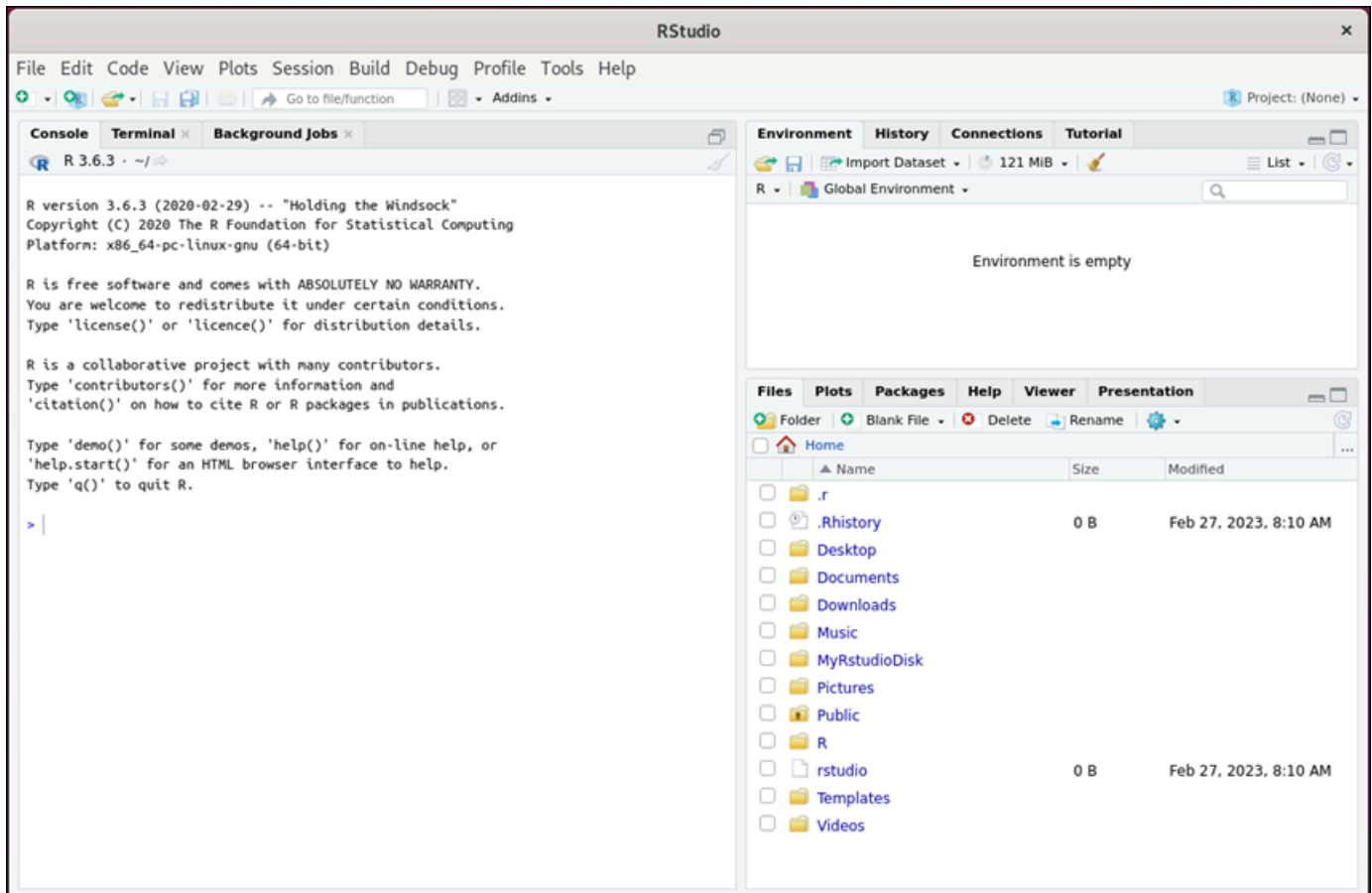
Avvia applicazione, passate al passaggio successivo di questa procedura per aprire un file nell'applicazione. RStudio Se hai scelto l'opzione Accedi al sistema operativo, puoi aprire altre applicazioni tramite il desktop di Ubuntu.

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.

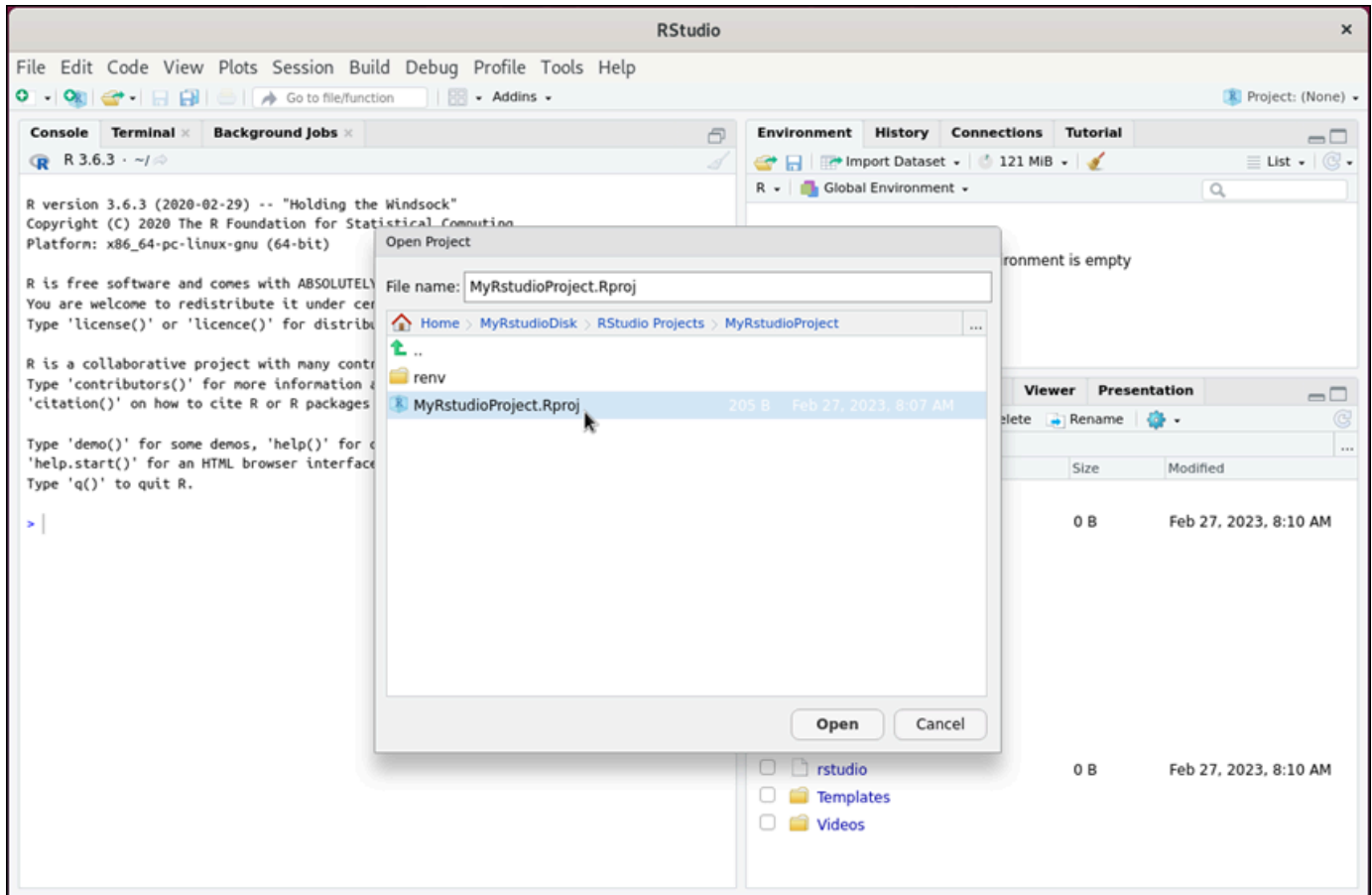
4. L'RStudio applicazione si apre.



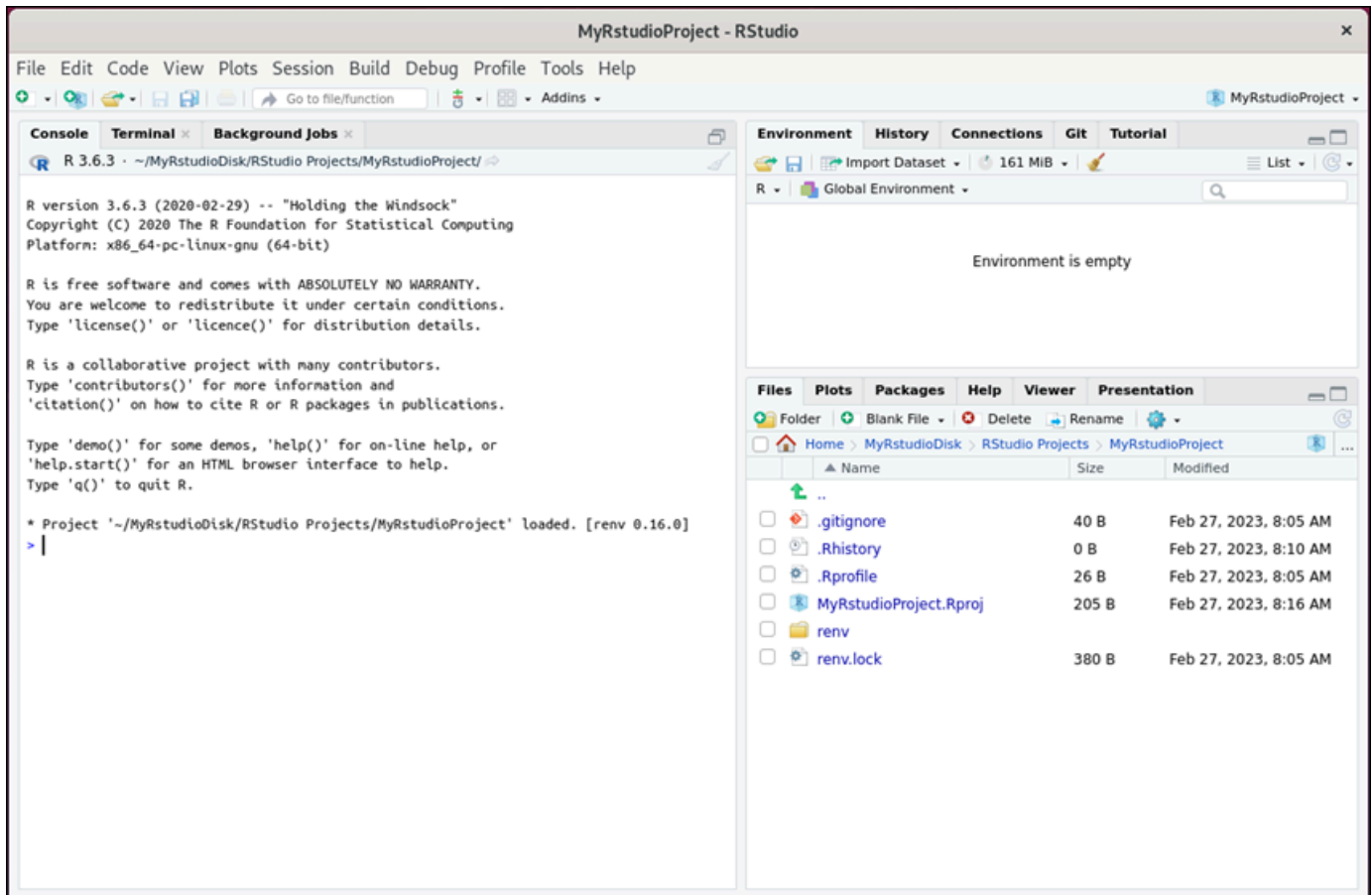
5. Per aprire un progetto in RStudio, scegliete il menu File, quindi scegliete Apri progetto. Seleziona la directory o la cartella in cui sono archiviati i file del progetto. Quindi scegli il file da aprire.

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.



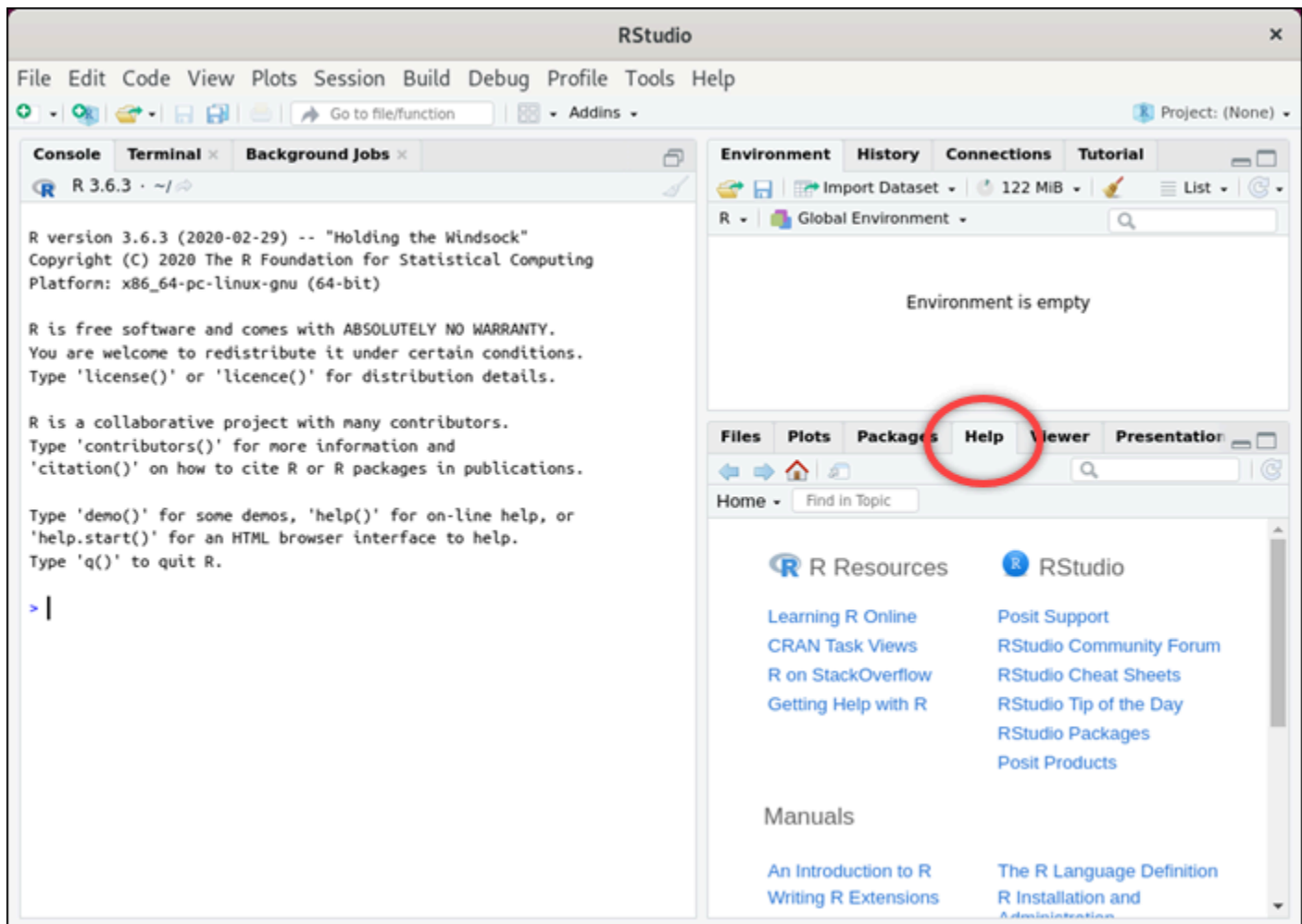
Nell'esempio seguente, abbiamo aperto il file di progetto MyRstudioProject.Rproj.



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.



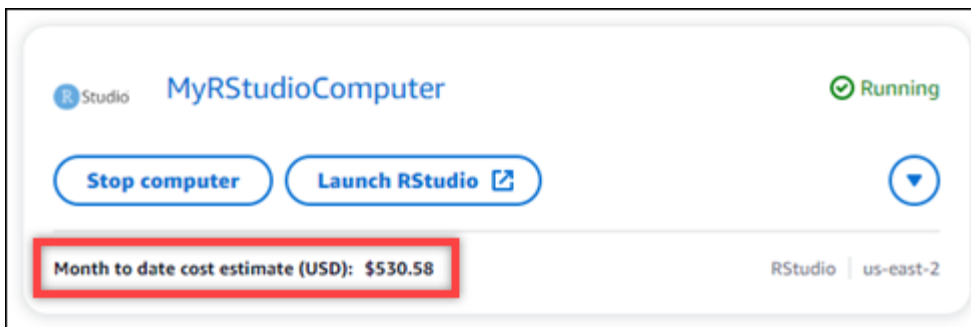
Sono disponibili anche le seguenti risorse RStudio online:

- [Imparare R online](#)
- [R su StackOverflow](#)
- [Utilizzo della Guida con R](#)
- [Supporto Posit](#)
- [RStudioForum della comunità](#)
- [RStudioCheat sheet](#)
- [RStudioSuggerimento del giorno \(Twitter\)](#)
- [RStudioPacchetti](#)

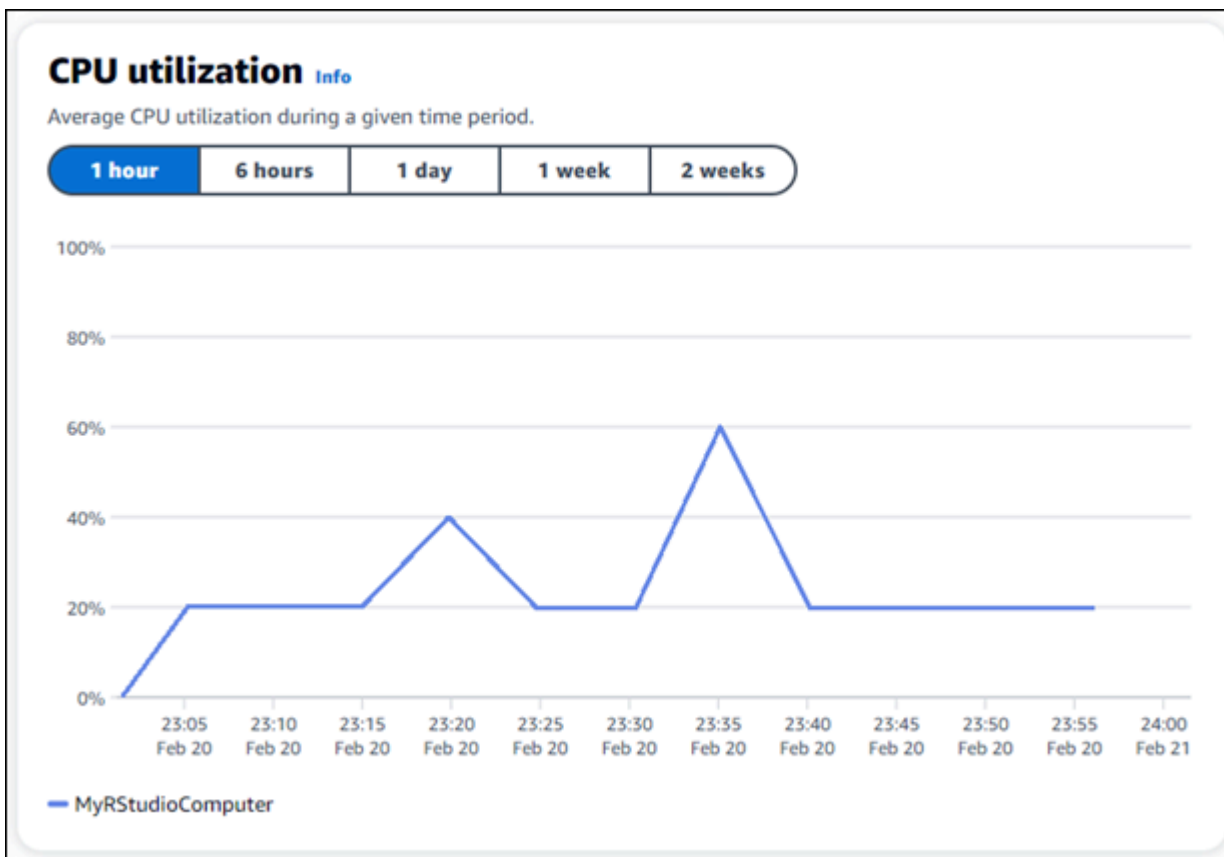
Fase 6: (facoltativa) monitoraggio dell'utilizzo e dei costi

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'CPU Utilizzo di un computer virtuale, scegli il nome del computer virtuale, quindi scegli la scheda Dashboard.



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.

Q Filter by name < 1 > ⚙

Name	Region	Month to date cost estimate (USD)	Usage estimate (hours)
MyJupyterComputer	us-east-2	\$529.43	346.02
MyJupyterComputer2	us-east-2	\$241.21	157.65
MyRStudioComputer	us-east-2	\$530.58	346.78

Disks

Q Filter by name < 1 > ⚙

Name	Region	Month to date cost estimate (USD)	Usage estimate (GB)
MyDisk	us-east-2	\$0.45	0.15
MyFirstDisk	us-west-2	\$0.61	0.81
MyRStudioDisk	us-west-2	\$0.58	0.77

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 Stop virtual computer on idle che arresta un computer in esecuzione quando raggiunge una determinata percentuale di CPU utilizzo durante un determinato periodo. Ad esempio, una regola può arrestare automaticamente un computer specifico quando il suo CPU utilizzo 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 fermare il computer virtuale in stato di inattività, ti consigliamo di monitorarne l'utilizzo per alcuni giorni. CPU Prendi nota dell'CPUUtilizzo 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 si crea una regola con una soglia di CPU utilizzo superiore al carico di lavoro, la regola può interrompere 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 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).

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'istananea 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](#)
- [Crea un computer virtuale Lightsail for Research](#)
- [Visualizza i dettagli del computer virtuale di Lightsail for Research](#)
- [Accedi a un'applicazione per computer virtuale Lightsail for Research](#)
- [Accedi al sistema operativo del tuo computer virtuale Lightsail for Research](#)
- [Gestione delle porte firewall per i computer virtuali Lightsail for Research](#)
- [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](#)
- [Eliminare un computer virtuale Lightsail for Research](#)

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, la memoria e le CPU, lo spazio di archiviazione e l'indennità mensile di 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](#)
- [Piani](#)

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 basato sul web (IDE) 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 open source (IDE) 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, vedere. [RStudioIDE](#)
- VSCodium— VSCodium è una distribuzione binaria gestita dalla comunità dell'editor VS Code di Microsoft. Per ulteriori informazioni, vedere. [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 (), spazio di archiviazione (disco) SSD basato sul volume di archiviazione (disco) 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**— GPU i piani forniscono una piattaforma economica e ad alte prestazioni per l'informatica generica. 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	vCPUs	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
--------------	----	-------	-------	--------

GPU piani

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

Nome del piano	vCPUs	Memoria	Spazio di archiviazione	Indennità mensile per il trasferimento dei dati
GPUXL	4	16 GB	50 GB	1 TB
GPU2XL	8	32 GB	50 GB	1 TB
GPU4XL	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. Seleziona una 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 computer virtuale Lightsail for Research è pronto e puoi connetterti ad esso tramite una sessione di interfaccia utente grafica (). 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 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 (inUSD) per il computer virtuale, per questo ciclo di fatturazione.
- Pannello di controllo: dalla scheda Dashboard, è possibile avviare una sessione per accedere all'applicazione del computer virtuale. È inoltre possibile visualizzare l'CPUutilizzo. CPUl'utilizzo identifica la potenza di elaborazione utilizzata dalle applicazioni del computer virtuale. Ogni punto dati mostrato nel grafico rappresenta l'CPUutilizzo medio 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.

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

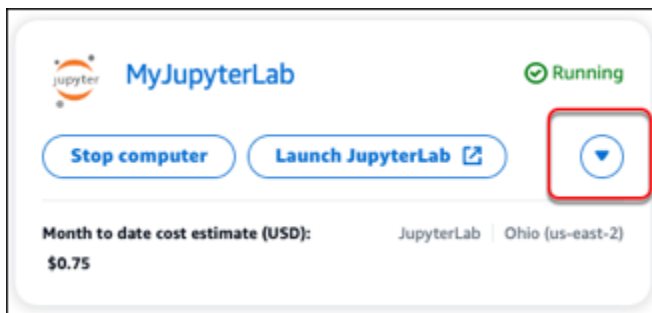
Important

Se nel tuo browser web è installato un blocco pop-up, potresti dover consentire i pop-up 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.

- Accedi alla console [Lightsail for Research](#).
- Nel riquadro di navigazione, scegli **Computer virtuali**.
- 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.

- Scegli **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:

- Transmission Control Protocol (TCP) 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.
- User Datagram Protocol (UDP) viene utilizzato principalmente per stabilire connessioni a bassa latenza e tolleranti le 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 stanno raggiungendo la destinazione prevista 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 - Utilizzato per Secure Shell (SSH).
 - 80 - Utilizzato per Hypertext Transfer Protocol (HTTP).
 - 443 - Utilizzato per Hypertext Transfer Protocol Secure (HTTPS).
 - 8443 - Utilizzato 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 SSH client di connettersi al computer virtuale, si configura una regola firewall che consente TCP l'utilizzo della 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 SSH connessione 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 SSH client 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](#)
- [Ottieni gli stati delle porte per un computer virtuale](#)
- [Aprire le porte per un computer virtuale](#)
- [Chiudere le porte di un computer virtuale](#)
- [Passa alle fasi successive](#)

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 la sezione AWS CLI Command [get-instance-port-states](#) Reference.

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 CIDR intervalli di IP a cui è consentito connettersi al computer virtuale.

```
% 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 `open-instance-public-ports` AWS CLI comando. 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, vedere [open-instance-public-ports](#) nel AWS CLI Command Reference.

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 CIDR intervalli IP appena aggiunti a cui è consentito connettersi al computer virtuale.


```
% 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, vedere [close-instance-public-ports](#) nel AWS CLI Command Reference.

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 CIDR intervalli IP che sono stati chiusi e che non possono più connettersi al computer virtuale.

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

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 key pair, puoi stabilire una connessione utilizzando numerosi SSH client, come Open SShTTY, Pu e Windows Subsystem per Linux. Per ulteriori informazioni, consulta [Richiedi una key pair per un computer virtuale Lightsail for Research](#).
- Connect al computer virtuale utilizzando SSH la riga di comando per gestirlo. Per ulteriori informazioni, consulta [Trasferisci file sui computer virtuali di Lightsail for Research utilizzando Secure Copy](#).

- Connect al computer virtuale utilizzando 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. DKP è specifico per ogni AWS regione in cui crei un'istanza o un computer virtuale. Ad esempio, il DKP 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 che sono stati configurati per utilizzare il al momento della creazione. DKP Lightsail for Research archivia automaticamente la chiave pubblica di sui computer virtuali DKP che crei. Puoi scaricare la chiave privata di DKP in qualsiasi momento effettuando una API chiamata al servizio Lightsail.

In questo documento, ti mostriamo come ottenerla DKP per un computer virtuale. Dopo aver installato ilDKP, è possibile stabilire una connessione utilizzando numerosi SSH client, come Open SSHTTY, Pu e Windows Subsystem per Linux. È inoltre possibile utilizzare Secure Copy (SCP) per trasferire in modo sicuro i file dal computer locale al computer virtuale.

Note

È inoltre possibile stabilire una connessione con il protocollo di visualizzazione remota al computer virtuale utilizzando il client basato su browser NICECDV. NICECDV è disponibile nella console Lightsail for Research. Quel RDP client non richiede che tu ottenga una key pair per il tuo computer. Per ulteriori informazioni, consulta [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](#)
- [Procurati una coppia di chiavi per un computer virtuale](#)
- [Passa alle fasi successive](#)

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 JSON processore a riga di comando leggero e flessibile utilizzato nelle seguenti procedure per estrarre i dettagli delle key pair dagli JSON output 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 Lightsail per un computer virtuale in DKP 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 Lightsail per una regione. AWS Per ulteriori informazioni, consulta la sezione [AWS CLI Command `download-default-key-pair` Reference](#).

1. Apri una finestra del prompt dei comandi.
2. Immettete il seguente comando per ottenere il DKP 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
```

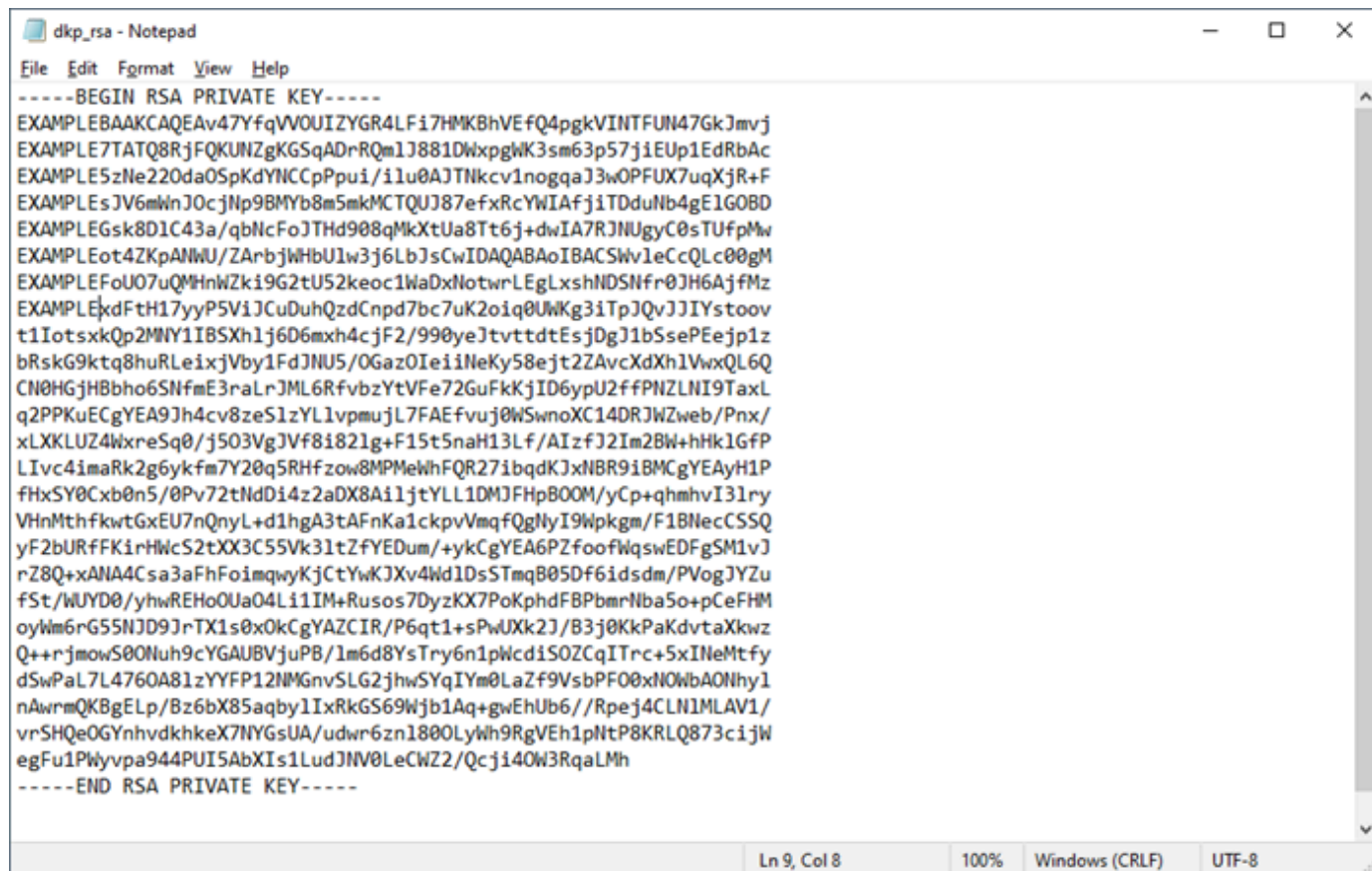
Non c'è risposta al comando. Puoi confermare se il comando ha avuto successo aprendo il `dkp-details.json` file e verificando se le informazioni di DKP Lightsail sono state salvate. Il contenuto del file `dkp-details.json` deve corrispondere all'esempio che segue. Il comando non è riuscito se il file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

```
{
  "publicKeyBase64": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC/jth+pVU5QhlgZHgsWLSwcoGFUR9DImCRUG1MVQ3jsaQma
+McSV0W/7tMBNDxGMVApQ1mAoZkAoTFCaUnzzUNbGmBYreybrennuOIRSnUR1FsBzNF2PqBrnM17bY51o5Kkp1g0IKk+m6L
+KW7QA1M2Ry/WciCponfA48VRfu6peNH4U/w0RKVyw1XqZack5yM2n0ExhvybmaQwJNBQnzt5/FFxhYgB
+OJMN241viASUY4EMgMiCsfwayTwOULjdr+ps1wWglMd33TyoyRe1Rrx03qP53AgDtEk1SDILSxNR+kzDe8N8x
+Si3hkqkA1ZT9kCtuNYdtSXDePotsmwL",
  "privateKeyBase64": "-----BEGIN RSA PRIVATE KEY-----
\EXAMPLEBAAKCAQEAv47YfqWVOUIZYGR4LF17HMKbVhVfQ4pgkVINTFUN47GkJmvj
\nEXAMPLE7TATQ8RjFQKUNZgKGSqADrRQm1J881DwXpgWK3sm63p57jiEUp1EdRbAc
\nEXAMPLE5zNe220da0SpKdYnCCpPui/i1u0AJTnkcv1nogqaJ3wOPFUX7uqXjR+F
\nEXAMPLEsJV6mWnJ0cJNp9BMYb8m5mkMCQUJ87efxRcYwIAfjiTDduNb4gE1GOBD\nEXAMPLEGsk8D1C43a/qbNcFoJTHd908qMkXtUa8Tt6j
+dwIA7RJNUgyC0sTUfPmW\nEXAMPLEEot4ZKpANWU/ZArbjWHbU1w3j6LbJsCwIDAQABoIBACSWV1eCcQLc00gM
\nEXAMPLEFoU07uQMhNwZki9G2tU52keoc1WaDxNotwrLEgLxshNDSNfr0JH6AjfMz
\nEXAMPLExdFth17yyP5VijCuDuhQzdCnpd7bc7uK2oiq0UWKg3iTpJQvJJiYstoov
\nnt1IotsxkQp2MNY1IBSXh1j6D6mxh4cjF2/990yeJtvttdtEsjDgJ1bSsePEejp1z
\nbRskG9ktq8huRLeixjVby1FdJNU5/OGaz0IeiiNeKy58ejt2ZAvCxh1VwxQL6Q
\nCN0HGjHbho6SNfme3raLrJML6RfVbzytVFe72GuFkKjID6ypU2ffPNZLNI9TaxL
\nq2PPKUECgYEA9Jh4cv8zeSlzYLLvpmujL7FAefvuj0WswnoXC14DRJwZweb/Pnx/\nxLXKLUZ4WxreSq0/j503VgJVf8i821g
+F15t5naH13Lf/AIzfJ2Im2Bw+hHk1GFp\nLIVc4imaRk2g6ykfm7Y20q5RHfzow8MPMeWhFQR27ibqdKJxNBR9iBMCgYEAyH1P
\nfHxSY0Cxb0n5/0Pv72tNdDi4z2aDX8Ai1jtYLL10MJFhpB00M/yCp+qhmhvI31ry\nvHnMthfkwGxEU7nQnyL
+d1hgA3tAFnKa1ckpvVmqFqgNyI9Wpkm/F1BNecCSSQ\nyF2bURFFKirHwCS2tXX3C55Vk31tZfYEDum/+ykCgYEA6PZfoofWqswEDFgSM1vJ
\nrZ8Q+xANA4Csa3aFhFoimqwyKjCtYwKJXv4Wd1Ds5TmqB05Df6idsdm/PVogJYZu\nfSt/WUYD0/yhwREHo0Ua04Li1IM
+Rusos7DyzKX7PoKphdFBPbmrNba5o+pCeFHM\nnoyWm6rG55NDJ9JrTX1s0xOkCgYAZCIR/P6qt1+sPwJXk2J/B3j0KkPaKdvtaXkzw\nQ+
+rjmwos00Nuh9cYGAUBVjuPB/lm6d8YsTry6n1pWcd1S0ZCqITrc+5xIneMtfy
\nndSwPal7L4760A81zYFFP12NMGnvSLG2jhWsyqIYm0LaZf9VsbPF00xN0wBAONhy1\nnAwrMqKBgELp/Bz6bX85aqby1IxRkGS69WjB1Aq
+gWUhUb6//Rpej4CLN1MLAV1\nnvrSHQeOGYnhvdkhkeX7NYGSUA/udwr6zn1800LyWh9RgVEh1pNtP8KRLQ873cijW
\negFu1Pwyvpa944PUI5AbXIs1LudJNV0LeCW22/Qcji40W3RqaLMh\n-----END RSA PRIVATE KEY-----\n",
  "createdAt": "2022-02-02T16:17:09.600000-08:00"
}
```


- 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.



```
-----BEGIN RSA PRIVATE KEY-----
EXAMPLEBAAKCAQEAv47YfqVVOUIZYGR4LF17HMKBhVEfQ4pgkVINTFUN47GkJmvj
EXAMPLE7TATQ8RjFQKUNZgKGSqADrRQm1J881DwxpgwK3sm63p57j1EUp1EdRbAc
EXAMPLE5zNe220da0SpKdYnCCpPpui/i1u0AJTNkcv1nogqaJ3wOPFUX7uqXjR+F
EXAMPLEsJV6mWnJ0cjnP9BMYb8m5mkMCTQUJ87efxRcYwIAfjiTDduNb4gE1GOBD
EXAMPLEGsk8D1C43a/qbNcFoJTHd908qMkXtUa8Tt6j+dwIA7R3NUgyC0sTUfpMw
EXAMPLEEot4ZKpANWU/ZArbjWHbU1w3j6LbJsCwIDAQAABaoIBACSw1eCcQLc00gM
EXAMPLEFoU07uQMhNwZki9G2tU52keoc1WaDxNotwrLEgLxshNDSNfr0JH6AjfMz
EXAMPLEkFdH17yyP5V1JCuDuhQzdCnpd7bc7uK2oiq0UwKg3iTpJQvJJYIstoov
t1IotsxkQp2MNY1IBSXh1j6D6mxh4cjF2/990yeJtvttdtEsjDgJ1bSsePEejp1z
bRskG9ktq8huRLeixjVby1FdJNU5/OGaz0IeiiNeKy58ejt2ZAvCXdxh1VwxQL6Q
CN0HGjHbBho6SNfmE3raLrJML6RfVbzYtVFe72GuFkKjID6ypU2ffPNZLNI9TaxL
q2PPKuECgYEA9Jh4cv8zeS1zYL1vpmujL7FAEfvuj0WSwnoXC14DRJWzweb/Pnx/
xLXLUZ4WxreS0q/j503VgJVf81821g+F15t5naH13Lf/AIzfJ2Im2BW+hHk1GfP
LIvc4imaRk2g6ykfm7Y20q5RHfzow8MPMewhFQR27ibqdKJxNBR9iBMCgYEAyH1P
fHxSY0Cxb0n5/0Pv72tNdDi4z2aDX8A11jtYLL1DMJFHpBOOM/yCp+qhmhvI31ry
VHnMthfkwGxEU7nQnyL+d1hgA3tAFnKa1ckpvVmQfQgNyI9WpKgm/F1BNecSSQ
yF2bURfFKirHwC52tXX3C55Vk31tZfYEDum/+ykCgYEA6PZfoofWqswEDFgSM1vJ
rZ8Q+xAANA4Csa3aFhFoimqwyKjCtYwKJXv4Wd1DsSTmqB05Df6idsdm/PVogJYZu
fSt/WUYD0/yhwREHOuOa04L1iIM+Rusos7DyzKX7PoKphdFBPbmrNba5o+pCeFHM
oyWm6rG55NJD9JrTX1s0xOkCgYAZCIR/P6qt1+sPwJXk2J/B3j0KkPaKdvtaXkwz
Q++rjmowS00Nuh9cYGAUBVjuPB/lm6d8YsTry6n1pWcdiSOZCqITrc+5xINeMtfy
dSwPaL7L4760A81zYFFP12NMGnvSLG2jhwSYqIYm0LaZf9VsbPF00xNOWbAONhy1
nAwrnQK8gELp/Bz6bX85aqby1IxRkGS69Wjb1Aq+gwEhUb6//Rpej4CLN1MLAV1/
vrSHQeOGYnhvdkhkeX7NYGsUA/udwr6zn1800LyWh9RgVEh1pNtP8KRLQ873ciJw
egFu1PWyvpa944PUI5AbXIIs1LudJNV0LeCWZ2/Qcji40W3RqaLMh
-----END RSA PRIVATE KEY-----
```

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

Otteni 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

Lightsail per una regione. AWS Per ulteriori informazioni, consulta la sezione [AWS CLI Command download-default-key-pair](#) Reference.

1. Apri una finestra del terminale.
2. Immettete il seguente comando per ottenere il DKP 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 di DKP 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.

```

{
  "publicKeyBase64": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQC/
jth+pVU5QhlgZHgsWLSwcoGFUR9DimCRUg1MVQ3jsaQma+McSV0W/
7tMBNDxGMVApQ1mAoZKoA0tFCaUnzzUNbGmBYreybrennu0IRSnUR1FsBzNF2PqBrnM17bY51o5KkpIlg0IKk+m6L+KW7QA1M2Ry/
MeiCponfa48VRfu6peNH4U/w0RKVywLXqZack5yM2n0ExhvybmaQwJNBQnzt5/
FFxhYgB+0JMN241viASUY4EMgMiCsfwayTw0ULjdr+pslwWgLMd33TyoyRelRrx03qP53AgDtEk1SDILSxNR+kzDe8N8x+Si3hkqkA1ZT9KctuNYdtSX
"privateKeyBase64": "-----BEGIN RSA PRIVATE KEY-----
\nEXAMPLEBAAKCAQEAv47YfqVV0UIZYGR4LFi7HMKbHVEfQ4pgkVINTFUN47GkJmvj\nEXAMPLE7TAT08RjFQKUNZgKGSqADrRQmLJ881DwXpgWK3sm6
i1lu0AJTNkcVInogqaJ3w0PFUX7uqXjR+F\nEXAMPLEsJV6mWnJ0cjNp9BMYb8m5mkMCTQUJ87efxRcYwIAfjiTDduNb4gELG0BD\nEXAMPLEGsk8D1LC4
qbNcFoJTHd908qMkXtUa8Tt6j+dwIA7RJNUGyC0sTUfPmW\n3vDfMfkot4ZKpANWU/
ZARbjWHbUlW3j6LbJscIWAQABAoIBACSWvleCccQLc00gM\nKMAfuq3FoU07uQMHNWZki9G2tU52keoc1WaDxNotwrLEgLxshNDSnfr0JH6AjfMz\nnVC
0Gaz0IeiiNeKy58ejt2ZAvCXdXhLVwxQL6Q\nCN0HGjHBbho6SNfmE3raLrJML6RfVbzYtVFe72GuFkKjID6ypU2fFPNZLNI9TaxL\nnq2PPKuECgYEA9
Pnx/\nLXLKLUZ4WxreSq0/j503VgJVf8i82lg+F15t5naH13Lf/
AIzJ2Im2BW+hHkLGFp\nlIvc4imaRk2g6yKfm7Y20q5RHfzow8MPMewhFQR27ibqDKJxNBR9iBMcGyEAYH1P\nfHxSY0Cxb0n5/0Pv72tNdDi4z2aDX
yCp+qhmhvI3lry\nVHnMthfkwTgxEU7nQnyL+d1hgA3tAFnKa1ckpvVmQfQgNyI9WpKgm/
F1BNecSSQ\nnyF2bURfFKiRHwC52tXX3C55Vk3ltZfYEDum/
+ykCgYEA6PZfoofWqswEDFgSM1vJ\nrZ8Q+xANA4Csa3aFhFoimqwyKjCtYwKJXv4Wd1DsSTmQ805Df6idsdm/PVogJYZu\nnfSt/WUYD0/
yhwREHo0Ua04Li1IM+Rusos7DyzKX7PoKphdFBPbmrNba5o+pCeFHM\nnoyWm6rG55NJ09JrTX1s0x0kCgYAZCIR/P6qt1+sPwUXk2J/
B3j0KkPaKdvtaXkwz\nq++rjmowS00Nuh9cYGAUBVjuPB/
lm6d8YsTry6n1pWcdiS0ZCqITrc+5xINeMtfy\nndSwPaL7L4760A8lzYYFP12NMGvNSLg2jhwSYqIYm0LaZf9VsbPF00xN0WbA0Nhy1\nnAwrmQKBgEL
Bz6bX85aqbylIxRkGS69WjblAq+gWEHUb6//Rpej4CLN1MLAV1/\nvrSHQeOGYnhvdkhkeX7NYGsUA/
udwr6znl800LYwh9RgVEHlpNtP8KRLQ873cijW\negFu1Pwyypa944PUI5AbXIs1LudJNV0LeCWZ2/Qcji40W3RqaLMh\n-----END RSA PRIVATE
KEY-----\n"
}

```

- 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.


```

-----BEGIN RSA PRIVATE KEY-----
EXAMPLEBAAKCAQEAv47YfqVV0UIZYGR4LFi7HMKBhVEfQ4pgkVINTFUN47GkJmvj
EXAMPLE7TATQ8RjFQKUNZgKGSqADrRQmLJ881DwXpgWK3sm63p57jiEUp1EdRbAc
EXAMPLE5zNe220da0SpKdYNCpPpui/ilu0AJTNkcv1nogqaJ3w0PFUX7uqXjR+F
EXAMPLEsJV6mWnJ0cjNp9BMYb8m5mkMCTQUJ87efxRcYWIafjiTDduNb4qElG0BD
EXAMPLEGsk8DlC43a/qbNcFoJTHd908qMkXtUa8Tt6j+dwIA7RJNUgyC0sTufpMw
3vDFmfkot4ZKpANWU/ZArbjWHbUlw3j6LbJscwIDAQABAoIBACSwleCcQLc00gM
KMAfuq3FoU07uQMhWZki9G2tU52keoc1WaDxNotwrLEgLxshNDSNfr0JH6AjfmZ
VCMzP0UxdFtH17yyP5ViJCuDuhQzdCnpd7bc7uK2oiq0UWKg3iTpJQvJJiYstoov
t1IotsxkQp2MNY1IBSxhlj6D6mxh4cjF2/990yeJtvtttdtEsjDgJ1bSsePEejPlz
bRskG9ktq8huRLeixjvby1FdJNU5/OGaz0IeiNeKy58ejt2ZAvCdXhLvwQL6Q
CN0HGjHBbho6SNfmE3raLrJML6RfVbzYtVFe72GuFkKjID6ypU2ffPNZLNI9TaxL
q2PPKuECgYEA9Jh4cv8zeSlzYLlvpmujL7FAEfvuj0WSwnoXC14DRJWZweb/Pnx/
xLXLKLUZ4WxreSq0/j503VgJVf8i82lg+F15t5naH13Lf/AIzFJ2Im2Bw+hhkLGFp
LIvc4imaRk2g6ykm7Y20q5RHfzow8MPMeWhFQR27ibqdKJxNBR9iBMCgYEAyH1P
fHxSY0Cxb0n5/0Pv72tNdD14z2aDX8AiljtYLL1DMJFHpB00M/yCp+qhmhvI3lry
VHnMthfkwGxEU7nQnyL+d1hgA3tAFnKa1ckpvVmQfQgNyI9Wpkgm/F1BNecCSSQ
yF2BURfFKirHwC52tXX3C55V3ltZfYEDum/+ykCgYEA6P2foofWqswEDFgSM1vJ
rZ8Q+ANA4Csa3aFhFoimqwyKjCtYwKJXv4wldS5TmqB05Df6idsdm/PVogJYZu
fSt/WUYD0/yhwREH00Ua04Li1IM+Rusos7DyzKX7PoKphdFBPbmrNba5o+pCeFHM
oyWm6rG55NJD9JrTX1s0x0kCgYAZCIR/P6qt1+sPwUXk2J/B3j0KkPaKdvtaXkwz
Q++rjmowS00Nuh9cYGAUBVjuPB/lm6d8YsTry6n1pwcDiS0ZCqITrc+5xINeMtfy
dSwPaL7L4760A8lzYFFP12NMGnvSLG2jhwSYqIYm0LaZf9VsbPF00xNOWbAONhyl
nAwrMQKBgElp/Bz6bX85aqbylIxRkGS69WjblAq+gwEhUb6//Rpej4CLNlMLAV1/
vr5HQe0GYnhvdkhkeX7NYGsUA/udwr6zn1800LyWh9RgVEH1pNtP8KRLQ873cijw
egFu1PWyvpa944PUI5AbXiS1LudJNV0LeCWZ2/Qcji40W3RqaLMh
-----END RSA PRIVATE KEY-----

```

- 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 SCP connessione SSH o una connessione 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:

- Connect al computer virtuale utilizzando SSH la riga di comando per gestirlo. Per ulteriori informazioni, consulta [Connect a un computer virtuale Lightsail for Research tramite Secure Shell](#).
- Connect al computer virtuale utilizzando 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 Secure Shell (SSH). Puoi utilizzarlo SSH per gestire il tuo computer virtuale da remoto in modo da poter accedere al tuo computer tramite Internet ed eseguire comandi.

Note

È inoltre possibile stabilire una connessione con il protocollo di visualizzazione remota al computer virtuale utilizzando il client basato su browser NICEVCV. NICEVCV 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](#)
- [Connect a un computer virtuale tramite SSH](#)
- [Passa alle fasi successive](#)

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 riapirla 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 AWS CloudShell per connetterti al tuo computer virtuale, consulta la [Connect a un computer virtuale tramite AWS CloudShell](#) sezione successiva. Per ulteriori informazioni, consulta [Cos'è 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 JSON processore a riga di comando leggero e flessibile utilizzato nelle seguenti procedure per estrarre i dettagli delle key pair. Per ulteriori informazioni sul download e l'installazione di jq, consulta [Scarica jq](#) sul sito Web di jq.

Connect a un computer virtuale tramite SSH

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

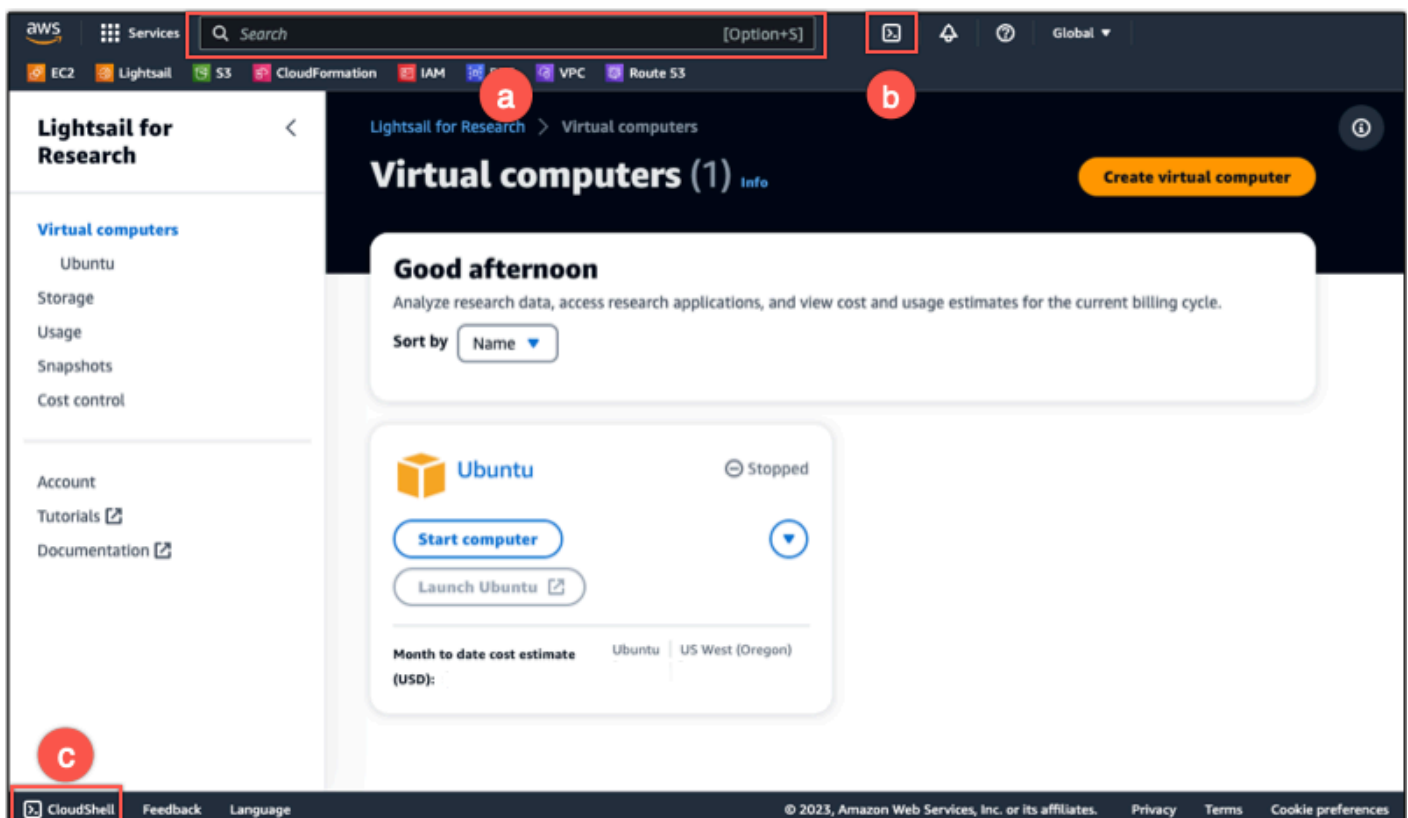
Connect a un computer virtuale tramite AWS CloudShell

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. AWS Management Console È 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 .

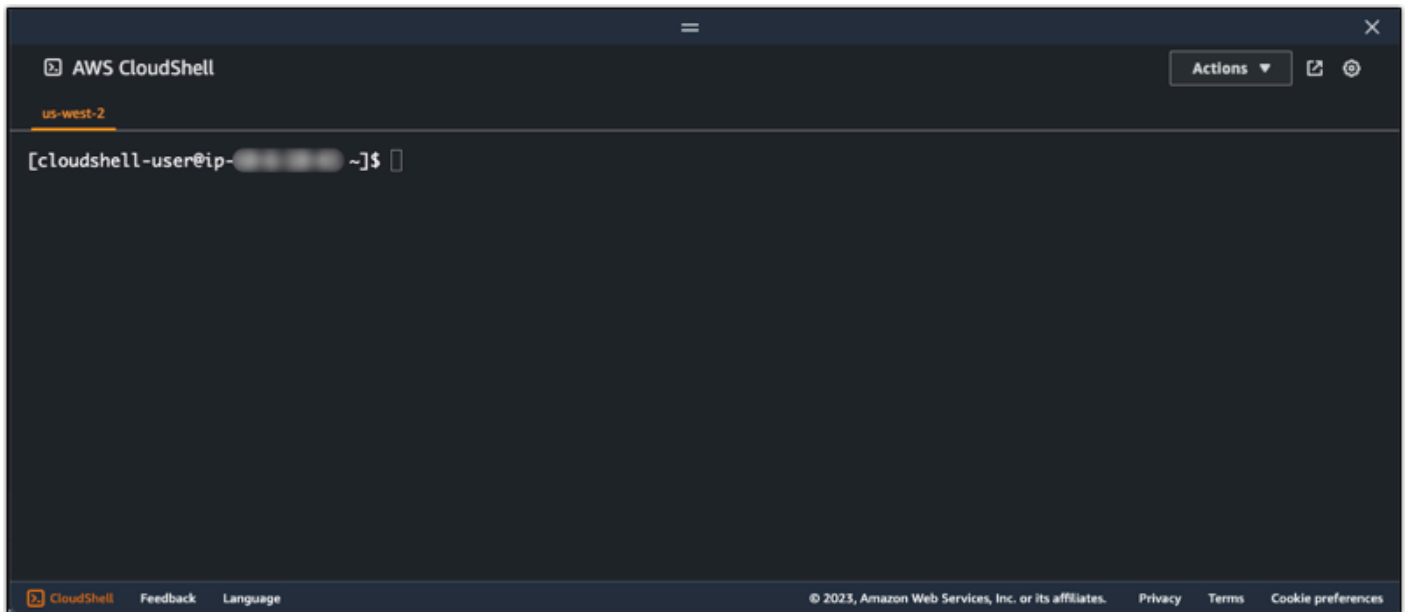
⚠ Important

Prima di iniziare, assicurati di avere la coppia di chiavi predefinita di Lightsail 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, scegli l'CloudShell icona.
 - c. Fai CloudShell clic sulla 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. Bash è la shell predefinita che viene eseguita all'avvio AWS CloudShell.

Bash

```
bash
```

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

3. Per connettersi a un computer virtuale dalla finestra del CloudShell terminale, vedere [Connect a un computer virtuale utilizzando SSH un computer locale Linux, Unix o macOS](#).

Per informazioni sul software preinstallato nell' CloudShell ambiente, consulta l'ambiente di [AWS CloudShell calcolo nella Guida](#) per l'AWS CloudShell utente.

Connect a un computer virtuale utilizzando SSH 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 predefinita di Lightsail 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 di DKP 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.

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



3. Immetti il seguente comando per stabilire una SSH connessione 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 SSH connessione stabilita con un computer virtuale Ubuntu in Lightsail for Research.

```
System information as of Thu Feb  9 19:48:23 UTC 2023
System load:          0.0
Usage of /:           0.3% of 620.36GB
Memory usage:        1%
Swap usage:          0%
Processes:           163
Users logged in:     0
IPv4 address for eth0: 192.0.2.0
IPv6 address for eth0: fe80::20c:29ff:fe00:0000

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

https://ubuntu.com/aws/pro

135 updates can be installed immediately.
9 of these updates are security updates.
To see these additional updates run: apt list --upgradable

3 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Wed Feb  8 06:50:04 2023 from 192.0.2.1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-192-0-2-0:~$
```

Ora che hai stabilito con successo una SSH connessione al tuo computer virtuale, vai alla [sezione successiva](#) per ulteriori passaggi successivi.

Connect a un computer virtuale utilizzando SSH 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 predefinita di Lightsail 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 di DKP 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.

```
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 '.in  
stance.publicIpAddress'  
[1] 31203 31204  
ubuntu  
18.118.120.226
```

3. Immetti il seguente comando per stabilire una SSH connessione 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 SSH connessione stabilita con un computer virtuale Ubuntu in Lightsail for Research.

```
* Support:      https://ubuntu.com/advantage

System information as of Thu Feb  9 23:43:27 UTC 2023

System load:          0.0
Usage of /:           0.3% of 620.36GB
Memory usage:         1%
Swap usage:           0%
Processes:            161
Users logged in:      0
IPv4 address for eth0: 192.0.2.0
IPv6 address for eth0: fe80::20c:29ff:fe00:0000

* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.

https://ubuntu.com/aws/pro

135 updates can be installed immediately.
9 of these updates are security updates.
To see these additional updates run: apt list --upgradable

New release '22.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

3 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Thu Feb  9 19:59:52 2023 from [redacted]
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-192-0-2-0:~$
```

Ora che hai stabilito con successo una SSH connessione al tuo computer virtuale, vai alla [sezione successiva](#) per ulteriori passaggi successivi.

Passa alle fasi successive

Puoi completare i seguenti passaggi aggiuntivi dopo aver stabilito correttamente una SSH connessione al tuo computer virtuale:

- Connect al computer virtuale utilizzando 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 NICE DCV client basato su browser disponibile nella console Lightsail for Research. Con il NICE DCV client, puoi trasferire rapidamente singoli file. Per ulteriori informazioni, consulta [Accedi al sistema operativo del tuo computer virtuale Lightsail for Research](#).

Argomenti

- [Completa i prerequisiti](#)
- [Connect a un computer virtuale tramite SCP](#)

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 JSON processore a riga di comando leggero e flessibile utilizzato nelle seguenti procedure per estrarre i dettagli delle key pair. 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 riapirla 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](#).

Connect a un computer virtuale tramite SCP

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

Connect a un computer virtuale utilizzando SCP 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 predefinita di Lightsail 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 di DKP Lightsail in `dkp_rsa` a 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.

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



3. Immettere il seguente comando per stabilire una SCP connessione con il computer virtuale e trasferire i file su di esso.

```
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.

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

Connect a un computer virtuale utilizzando SCP 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 predefinita di Lightsail 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 di DKP 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

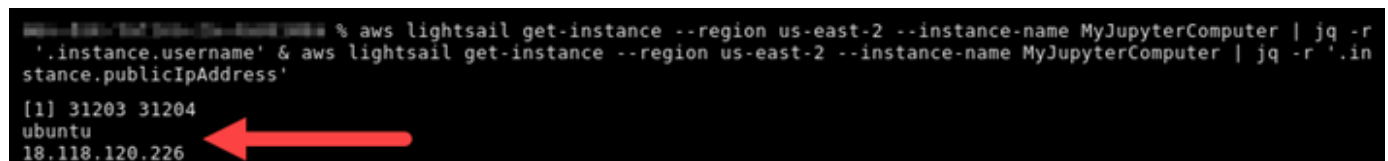
cui è stato creato il computer virtuale, ad esempio. `us-east-2` Sostituisci *computer-name* con il nome del computer virtuale a cui desideri connetterti.

```
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.



```
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 '.in
stance.publicIpAddress'
[1] 31203 31204
ubuntu
18.118.120.226
```

3. Immettere il seguente comando per stabilire una SCP connessione con il computer virtuale e trasferire i file su di esso.

```
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.

```
([root@ip-192-0-2-0 ~]#) <0> [~/Documents/Keys]
[root@ip-192-0-2-0 ~]# scp -i dkp_rsa -r 'Files' ubuntu@192.0.2.0:/home/lightsail-user/Uploads/
myfile2.txt          100% 10    0.2KB/s  00:00
myfile6.txt          100% 10    0.2KB/s  00:00
myfile7.txt          100%  8    0.1KB/s  00:00
myfile10.txt         100%  7    0.1KB/s  00:00
myfile1.txt          100%  9    0.2KB/s  00:00
myfile3.txt          100% 10    0.2KB/s  00:00
myfile12.txt         100% 13    0.2KB/s  00:00
myfile.txt           100% 11    0.2KB/s  00:00
myfile9.txt          100%  9    0.2KB/s  00:00
myfile11.txt         100%  4    0.1KB/s  00:00
myfile5.txt          100% 10    0.2KB/s  00:00
myfile4.txt          100%  9    0.2KB/s  00:00
myfile8.txt          100%  9    0.2KB/s  00:00
```

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](#)
- [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](#)

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. Sceglie 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 lo 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](#)
- [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'istananea nella console Lightsail for Research](#)

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

Completa i seguenti passaggi per creare un'istananea 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'istananea 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 AWS gestione 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 AWS Management Console e apri la AWS Billing console all'indirizzo <https://console.aws.amazon.com/billing/>.

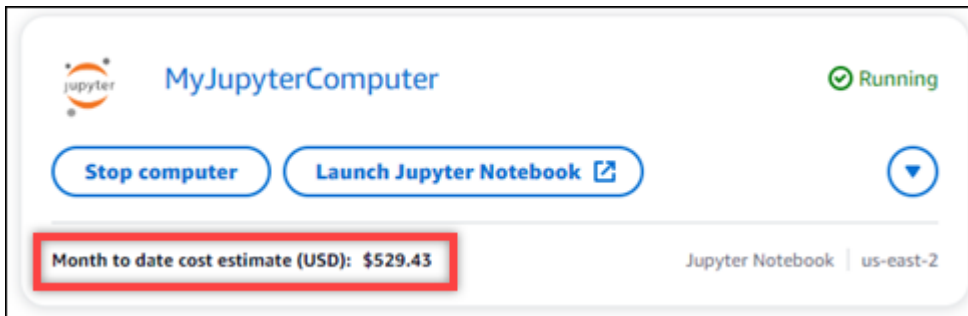
Argomenti

- [Visualizza le stime dei costi e dell'utilizzo delle tue risorse in Lightsail for Research](#)

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.



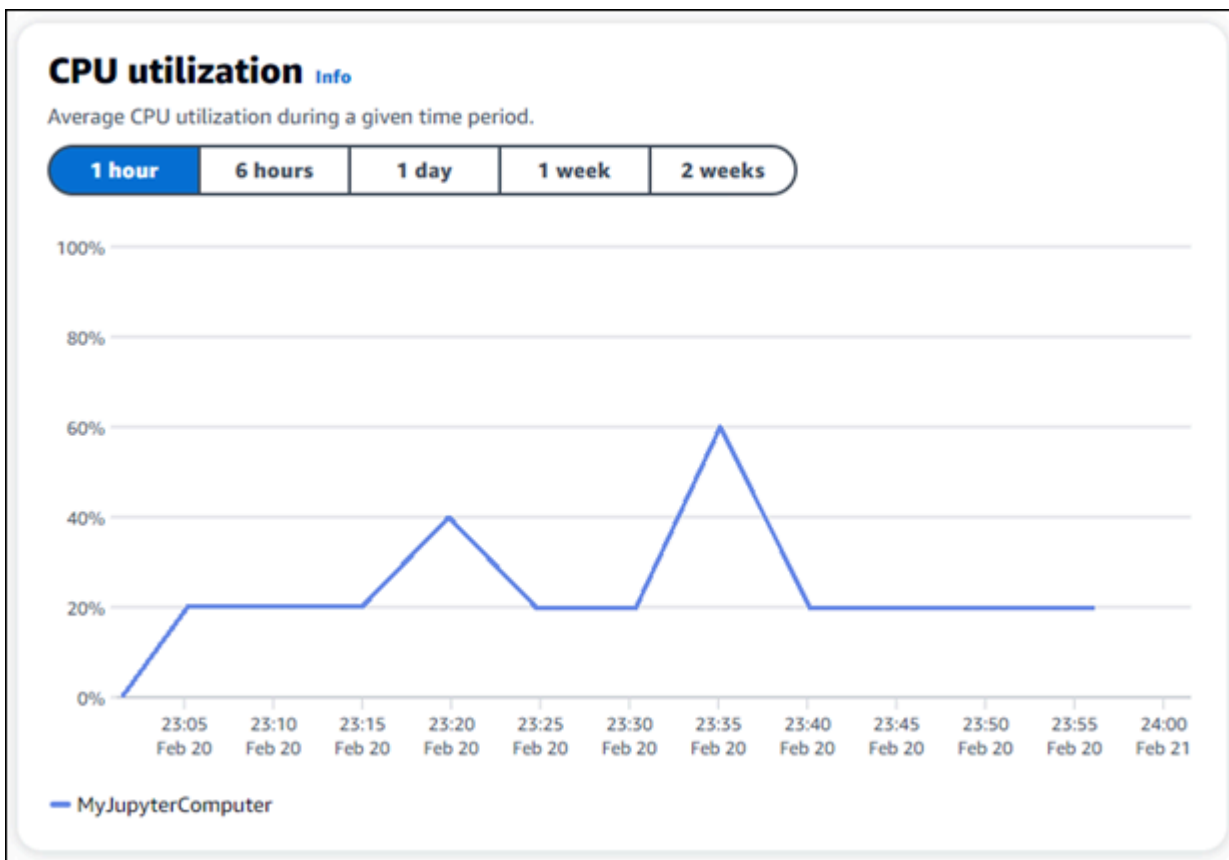
MyJupyterComputer Running

Stop computer Launch Jupyter Notebook

Month to date cost estimate (USD): **\$529.43**

Jupyter Notebook | us-east-2

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



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.

< 1 > ⚙

Name	Region	Month to date cost estimate (USD)	Usage estimate (hours)
MyJupyterComputer	us-east-2	\$529.43	346.02
MyJupyterComputer2	us-east-2	\$241.21	157.65
MyRStudioComputer	us-east-2	\$530.58	346.78

Disks

< 1 > ⚙

Name	Region	Month to date cost estimate (USD)	Usage estimate (GB)
MyDisk	us-east-2	\$0.45	0.15
MyFirstDisk	us-west-2	\$0.61	0.81
MyRStudioDisk	us-west-2	\$0.58	0.77

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 Stop virtual computer on idle che arresta un computer in esecuzione quando raggiunge una determinata percentuale di CPU utilizzo durante un determinato periodo. Ad esempio, una regola può arrestare automaticamente un computer specifico quando il suo CPU utilizzo 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](#)
- [Eliminare le regole di controllo dei costi per i computer virtuali Lightsail for Research](#)

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. CPU'utilizzo 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. Specificate la percentuale di CPU utilizzo 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 il CPU suo utilizzo 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 della chiave è di 128 caratteri Unicode in UTF-8.
- La lunghezza massima del valore è di 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. Tale prefisso è riservato all'uso AWS .

Argomenti

- [Tagga Lightsail for Research: risorse](#)
- [Rimuovi i tag dalle risorse di Lightsail for Research](#)

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. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua 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](#)
- [Identity and Access Management per Amazon Lightsail for Research](#)
- [Convalida della conformità per Amazon Lightsail for Research](#)
- [Resilienza in Amazon Lightsail for Research](#)
- [Sicurezza dell'infrastruttura in Amazon Lightsail for Research](#)
- [Analisi della configurazione e delle vulnerabilità in Amazon Lightsail for Research](#)
- [Best practice di sicurezza per Amazon Lightsail for Research](#)

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 ulteriori informazioni sulla privacy dei dati, consulta la sezione [Privacy dei dati FAQ](#). Per informazioni sulla protezione dei dati in Europa, consulta il [Modello di responsabilitàAWS condivisa e GDPR](#) il post sul blog sulla AWS sicurezza.

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

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- UsaSSL/TLSper comunicare con AWS le risorse. Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Configurazione API e registrazione delle attività degli utenti con AWS CloudTrail.
- 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 FIPS 140-3 moduli crittografici convalidati per accedere AWS tramite un'interfaccia a riga di comando o unAPI, usa un endpoint. FIPS Per ulteriori informazioni sugli FIPS endpoint disponibili, vedere [Federal Information Processing Standard \(\) 140-3. FIPS](#)

Ti consigliamo vivamente 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 altri utenti che utilizzano la consoleAPI,, 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. Se fornisci un messaggio URL a un server esterno, ti consigliamo vivamente di non includere le informazioni sulle credenziali URL per convalidare la tua richiesta a quel server.

Identity and Access Management per Amazon Lightsail for Research

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

Note

Amazon Lightsail e Lightsail for Research condividono gli stessi parametri di 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](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come funziona Amazon Lightsail for Research con IAM](#)
- [Esempi di policy basate sull'identità per Amazon Lightsail for Research](#)
- [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Lightsail for Research](#)

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Lightsail for Research.

Utente del servizio: se utilizzi il servizio Lightsail for Research per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Lightsail for Research per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni

aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Lightsail for Research, consulta [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Lightsail for Research](#)

Amministratore del servizio: se sei responsabile delle risorse di Lightsail for Research presso la tua azienda, probabilmente hai pieno accesso a Lightsail for Research. Il tuo compito è determinare a quali funzionalità e risorse di Lightsail for Research devono accedere gli utenti del servizio. È quindi necessario inviare richieste all'IAM amministratore per modificare le autorizzazioni degli utenti del servizio. Consulta le informazioni contenute in questa pagina per comprendere i concetti di base di IAM. Per saperne di più su come la tua azienda può utilizzare IAM Lightsail for Research, consulta [Come funziona Amazon Lightsail for Research con IAM](#)

IAM amministratore: se sei un IAM amministratore, potresti voler saperne di più su come scrivere politiche per gestire l'accesso a Lightsail for Research. Per visualizzare esempi di policy basate sull'identità di Lightsail for Research che puoi utilizzare, consulta IAM [Esempi di policy basate sull'identità per Amazon Lightsail for Research](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi utilizzando le tue credenziali di identità. AWS È necessario autenticarsi (accedere a AWS) come Utente root dell'account AWS, come IAM utente o assumendo un ruolo. IAM

È possibile accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Quando accedi come identità federata, l'amministratore aveva precedentemente configurato la federazione delle identità utilizzando i ruoli. IAM Quando si accede AWS utilizzando la federazione, si assume indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando () per firmare crittograficamente le tue richieste utilizzando le tue credenziali. CLI Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [Firmare AWS API le richieste](#) nella Guida per l'IAM utente.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'AWS IAM Identity Center utente e [Utilizzo dell'autenticazione a più fattori \(MFA\) AWS nella Guida per l'IAMutente](#).

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per l'elenco completo delle attività che richiedono l'accesso come utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'IAMutente.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per informazioni su IAM Identity Center, vedi [Cos'è IAM Identity Center?](#) nella Guida AWS IAM Identity Center per l'utente.

IAM users and groups

Un [IAMutente](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Laddove possibile, consigliamo di fare affidamento su credenziali temporanee anziché creare IAM utenti con credenziali a lungo termine come password e chiavi di accesso. Tuttavia, se hai casi d'uso specifici che richiedono credenziali a lungo termine con IAM gli utenti, ti consigliamo di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta

[Ruotare regolarmente le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente. IAM

Un [IAMgruppo](#) è un'identità che specifica un insieme di utenti. IAM Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per IAM amministrare le risorse.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Quando creare un IAM utente \(anziché un ruolo\)](#) nella Guida per l'IAMutente.

IAMruoli

Un [IAMruolo](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un IAM utente, ma non è associato a una persona specifica. È possibile assumere temporaneamente un IAM ruolo in AWS Management Console [cambiando ruolo](#). È possibile assumere un ruolo chiamando un' AWS APIoperazione AWS CLI or o utilizzando un'operazione personalizzataURL. Per ulteriori informazioni sui metodi di utilizzo dei ruoli, vedere [Utilizzo IAM dei ruoli](#) nella Guida per l'IAMutente.

IAMI ruoli con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per informazioni sui ruoli per la federazione, vedere [Creazione di un ruolo per un provider di identità di terze parti](#) nella Guida per l'IAMutente. Se utilizzi IAM Identity Center, configuri un set di autorizzazioni. Per controllare a cosa possono accedere le identità dopo l'autenticazione, IAM Identity Center correla il set di autorizzazioni a un ruolo in. IAM Per informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .
- **Autorizzazioni IAM utente temporanee:** un IAM utente o un ruolo può assumere il IAM ruolo di assumere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso su più account:** puoi utilizzare un IAM ruolo per consentire a qualcuno (un responsabile fidato) di un altro account di accedere alle risorse del tuo account. I ruoli sono lo strumento

principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la [sezione Accesso alle risorse su più account IAM nella Guida per l'utente](#). IAM

- **Accesso tra servizi:** alcuni Servizi AWS utilizzano funzionalità in altri. Servizi AWS Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
- **Sessioni di accesso inoltrato (FAS):** quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. FAS le richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).
- **Ruolo di servizio:** un ruolo di servizio è un [IAM ruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere [Creazione di un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAM utente](#).
- **Ruolo collegato al servizio:** 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'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.
- **Applicazioni in esecuzione su Amazon EC2:** puoi utilizzare un IAM ruolo per gestire le credenziali temporanee per le applicazioni in esecuzione su un'EC2 istanza e che effettuano AWS CLI o effettuano AWS API richieste. Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell'EC2 istanza. Per assegnare un AWS ruolo a un'EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull'EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta [Usare un IAM ruolo per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella Guida per l'IAM utente](#).

Per sapere se utilizzare IAM ruoli o IAM utenti, consulta [Quando creare un IAM ruolo \(anziché un utente\)](#) nella Guida per l'IAMutente.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come JSON documenti. Per ulteriori informazioni sulla struttura e il contenuto dei documenti relativi alle JSON politiche, vedere [Panoramica delle JSON politiche](#) nella Guida per l'IAMutente.

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

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM politiche. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

IAMle politiche definiscono le autorizzazioni per un'azione indipendentemente dal metodo utilizzato per eseguire l'operazione. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale criterio può ottenere informazioni sul ruolo da AWS Management Console, da o da. AWS CLI AWS API

Policy basate su identità

I criteri basati sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un IAM utente, un gruppo di utenti o un ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. [Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM](#)

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli all'interno del tuo. Account AWS Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una politica gestita o una politica in linea, consulta [Scelta tra politiche gestite e politiche in linea nella Guida](#) per l'IAMutente.

Policy basate su risorse

Le politiche basate sulle risorse sono documenti di JSON policy allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

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

Elenchi di controllo degli accessi () ACLs

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

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la [panoramica di Access control list \(ACL\)](#) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- **Limiti delle autorizzazioni:** un limite di autorizzazioni è una funzionalità avanzata in cui si impostano le autorizzazioni massime che una politica basata sull'identità può concedere a un'entità (utente o ruolo). IAM IAM È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. [Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità nella Guida per l'utente. IAM IAM](#)
- **Politiche di controllo del servizio (SCPs):** SCPs sono JSON politiche che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations

AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna Utente root dell'account AWS. Per ulteriori informazioni su Organizations and SCPs, consulta [le politiche di controllo dei servizi](#) nella Guida AWS Organizations per l'utente.

- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [le politiche di sessione](#) nella Guida IAM per l'utente.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determinare se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle politiche](#) nella Guida per l'IAMutente.

Come funziona Amazon Lightsail for Research con IAM

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

IAM funzionalità che puoi usare con Amazon Lightsail for Research

IAM caratteristica	Supporto Lightsail for Research
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì

IAMcaratteristica	Supporto Lightsail for Research
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC(tag nelle politiche)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	No
Ruoli di servizio	No
Ruoli collegati al servizio	No

Per avere una panoramica generale di come Lightsail for Research e AWS gli altri servizi funzionano con la IAM maggior parte delle funzionalità, [AWS consulta i servizi con cui funziona IAM](#) nella Guida per l'utente. IAM

Politiche basate sull'identità per Lightsail for Research

Supporta le policy basate su identità: sì

Le politiche basate sull'identità sono documenti relativi alle politiche di JSON autorizzazione che è possibile allegare a un'identità, ad esempio un utente, un gruppo di utenti o un IAM ruolo. Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. [Per informazioni su come creare una politica basata sull'identità, consulta Creazione di politiche nella Guida per l'utente. IAM IAM](#)

Con le politiche IAM basate sull'identità, puoi specificare azioni e risorse consentite o negate, nonché le condizioni in base alle quali le azioni sono consentite o negate. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per ulteriori informazioni su tutti gli elementi che è possibile utilizzare in una JSON politica, vedere il [riferimento agli elementi IAM JSON della politica](#) nella Guida per l'IAMutente.

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 politiche basate sulle risorse sono documenti JSON politici allegati a una risorsa. Esempi di politiche basate sulle risorse sono le policy di trust dei IAM ruoli 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. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per abilitare l'accesso tra più account, puoi specificare un intero account o IAM entità in un altro account come principale in una politica basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un IAM amministratore dell'account fidato deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta la sezione [Cross Account Resource Access IAM nella Guida IAM per l'utente](#).

Azioni politiche per Lightsail for Research

Supporta le operazioni di policy: si

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

L'Actionelemento di una JSON policy descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell' AWS APIoperazione associata. Esistono alcune eccezioni, come le azioni basate solo sulle autorizzazioni che non hanno un'operazione corrispondente. API Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi 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 di policy: sì

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

L'elemento Resource JSON policy specifica l'oggetto o gli oggetti a cui si applica l'azione. Le istruzioni devono includere un elemento Resource o un elemento NotResource. Come best practice, specifica una risorsa utilizzando il relativo [Amazon Resource Name \(ARN\)](#). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, 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 le caratteristiche 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 AWS JSON le policy per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento Condition(o blocco Condition) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento Condition è facoltativo. Puoi 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.

Se specifichi più elementi Condition in un'istruzione o più chiavi in un singolo elemento Condition, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica OR. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile concedere a un IAM utente l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome IAM utente. Per ulteriori informazioni, consulta [gli elementi IAM della politica: variabili e tag](#) nella Guida IAM per l'utente.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'IAM utente.

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](#)

ACLsin 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

ABACcon Lightsail per la ricerca

Supporti ABAC (tag nelle politiche): Parziale

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. È possibile allegare tag a IAM entità (utenti o ruoli) e a molte AWS risorse. L'etichettatura di entità e risorse è il primo passo di ABAC. Quindi si progettano ABAC politiche per consentire le operazioni quando il tag del principale corrisponde al tag sulla risorsa a cui sta tentando di accedere.

ABAC è utile in ambienti in rapida crescita e aiuta in situazioni in cui la gestione delle politiche diventa complicata.

Per controllare l'accesso basato su tag, fornisci 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 Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, vedere [Cos'è? ABAC](#) nella Guida IAM per l'utente. Per visualizzare un tutorial con i passaggi per la configurazione ABAC, consulta [Utilizzare il controllo di accesso basato sugli attributi \(ABAC\)](#) nella Guida per l'IAM utente.

Utilizzo di credenziali temporanee con Lightsail for Research

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione [Servizi AWS relativa alla funzionalità IAM nella Guida](#) per l'IAM utente.

Si utilizzano credenziali temporanee se si accede AWS Management Console utilizzando qualsiasi metodo tranne il nome utente e la password. Ad esempio, quando accedete AWS utilizzando il link Single Sign-on (SSO) della vostra azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sul cambio di ruolo, consulta [Passare a un ruolo \(console\)](#) nella Guida per l'IAMutente.

È possibile creare manualmente credenziali temporanee utilizzando AWS CLI o AWS API. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, vedere [Credenziali di sicurezza temporanee](#) in IAM.

Autorizzazioni principali multiservizio per Lightsail for Research

Supporta sessioni di accesso diretto (): No FAS

Quando utilizzi un IAM utente o un ruolo per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. FAS le richieste vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli FAS delle politiche relative alle richieste, consulta [Forward access sessions](#).

Ruoli di servizio per Lightsail for Research

Supporta i ruoli di servizio: No

Un ruolo di servizio è un [IAMruolo](#) che un servizio assume per eseguire azioni per conto dell'utente. Un IAM amministratore può creare, modificare ed eliminare un ruolo di servizio dall'interno IAM. Per ulteriori informazioni, vedere [Creazione di un ruolo per delegare le autorizzazioni a un utente Servizio AWS nella Guida per l'IAMutente](#).

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'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un IAM amministratore può visualizzare, ma non modificare le autorizzazioni per i ruoli collegati al servizio.

[Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta AWS Servizi compatibili con. 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. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o. AWS API Per concedere agli utenti il permesso di eseguire azioni sulle risorse di cui hanno bisogno, un IAM amministratore può creare IAM policy. L'amministratore può quindi aggiungere le IAM politiche ai ruoli e gli utenti possono assumerli.

Per informazioni su come creare una politica IAM basata sull'identità utilizzando questi documenti di esempioJSON, consulta [Creazione di IAM politiche](#) nella Guida per l'IAMutente.

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](#)
- [Utilizzo della console Lightsail for Research](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)

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 crei o modifichi policy basate su identità, segui 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 ulteriori informazioni, consulta [le politiche AWS gestite o le politiche AWS gestite per le funzioni lavorative](#) nella Guida per l'IAM utente.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le IAM politiche, concedi solo le autorizzazioni necessarie per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo per applicare le autorizzazioni, consulta [Politiche](#) e autorizzazioni nella Guida IAM per l'utente. IAM IAM
- Utilizza le condizioni nelle IAM politiche per limitare ulteriormente l'accesso: puoi aggiungere una condizione alle tue politiche per limitare l'accesso ad azioni e risorse. Ad esempio, puoi scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. È inoltre possibile utilizzare condizioni per concedere l'accesso alle azioni di servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta [Elementi IAM JSON della politica: Condizione](#) nella Guida IAM per l'utente.
- Usa IAM Access Analyzer per convalidare IAM le tue policy e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio delle IAM policy () e alle best practice. JSON IAM IAM Access Analyzer fornisce più di 100 controlli delle politiche e consigli pratici per aiutarti a creare policy sicure e funzionali. Per ulteriori informazioni, vedere [Convalida delle policy di IAM Access Analyzer nella Guida per l'utente. IAM](#)
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede l'utilizzo di IAM utenti o di un utente root Account AWS, attiva questa opzione MFA per una maggiore sicurezza. Per richiedere MFA quando vengono richiamate API le operazioni, aggiungi MFA delle condizioni alle tue politiche. Per ulteriori informazioni, vedere [Configurazione dell'API accesso MFA protetto nella Guida](#) per l'IAM utente.

Per ulteriori informazioni sulle procedure consigliate in IAM, consulta la sezione [Procedure consigliate in materia di sicurezza IAM nella](#) Guida per l'IAM utente.

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 il CLI AWS API. Consenti invece l'accesso solo alle azioni che corrispondono all'API/operazione 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 ulteriori informazioni, consulta [Aggiungere autorizzazioni a un utente nella Guida per l'utente](#). IAM

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra come è possibile creare una politica che consenta IAM agli utenti di visualizzare le politiche in linea e gestite allegate alla loro identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando o a livello di codice. AWS CLI
AWS API

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



```
    "Action": [  
      "iam:GetGroupPolicy",  
      "iam:GetPolicyVersion",  
      "iam:GetPolicy",  
      "iam:ListAttachedGroupPolicies",  
      "iam:ListGroupPolicies",  
      "iam:ListPolicyVersions",  
      "iam:ListPolicies",  
      "iam:ListUsers"  
    ],  
    "Resource": "*"    
  }  
]  
}
```

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](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse Lightsail for Research](#)

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

Se ricevi un errore che indica che non disponi dell'autorizzazione per eseguire un'operazione, le tue policy devono essere aggiornate in modo che ti sei consentito eseguire tale operazione.

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

```
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 assistenza, contatta l'amministratore. AWS 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 ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Lightsail for Research supporta queste funzionalità, consulta [Come funziona Amazon Lightsail for Research con IAM](#)
- Per sapere come fornire l'accesso alle risorse di tua proprietà, consulta [Fornire l'accesso a un IAM utente di un altro Account AWS utente di tua proprietà nella Guida](#) per l'IAMutente. Account AWS
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a persone Account AWS di proprietà di terzi](#) nella Guida per l'IAMutente.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso agli utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'IAMutente.
- Per conoscere la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta la sezione Accesso alle [risorse tra account nella Guida per l'utente](#). IAM 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. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Guide introduttive su sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- [Architettura per la HIPAA sicurezza e la conformità su Amazon Web Services](#): questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee. HIPAA

Note

Non tutte sono idonee. Servizi AWS HIPAA Per ulteriori informazioni, consulta la [Guida ai servizi HIPAA idonei](#).

- [AWS Risorse per AWS](#) per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe riguardare il tuo settore e la tua località.
- [AWS Guide alla conformità dei clienti](#): comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization ()). ISO
- [Evaluating Resources with Rules](#) nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub](#)— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina [Documentazione di riferimento sui controlli della Centrale di sicurezza](#).
- [Amazon GuardDuty](#): Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, ad esempio PCI DSS soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- [AWS Audit Manager](#)— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

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, puoi 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, consulta [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 API le chiamate AWS pubblicate per accedere a Lightsail for Research attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). Richiediamo TLS 1.2 e consigliamo TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS) come (Ephemeral Diffie-Hellman) o DHE (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 O puoi 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, gestiscile 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. AWS Management Console. 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 i rilasci della documentazione per Lightsail for Research.

Modifica	Descrizione	Data
Versione iniziale	Versione iniziale della Guida per l'utente di Lightsail.	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.