aws

Benutzerhandbuch

Amazon Lightsail für die Forschung

Amazon Lightsail für die Forschung: Benutzerhandbuch

Table of Contents

Was ist Amazon Lightsail for Research?

Mit Amazon Lightsail for Research können Wissenschaftler und Forscher leistungsstarke virtuelle Computer in der Amazon Web Services ()AWS Cloud erstellen. Diese virtuellen Computer verfügen über vorinstallierte Forschungsanwendungen wie Scilab. RStudio

Mit Lightsail for Research können Sie Daten direkt aus einem Webbrowser hochladen, um mit Ihrer Arbeit zu beginnen. Sie können Ihre virtuellen Computer jederzeit erstellen und löschen, sodass Sie bei Bedarf auf leistungsstarke Rechenressourcen zugreifen können.

Sie zahlen nur so lange, wie Sie den virtuellen Computer benötigen. Lightsail for Research bietet Budgetierungssteuerungen, mit denen Ihr Computer automatisch angehalten werden kann, wenn er ein vorkonfiguriertes Kostenlimit erreicht, sodass Sie sich keine Gedanken über Mehrkosten machen müssen.

Alles, was Sie in der Lightsail for Research-Konsole tun, wird durch eine öffentlich verfügbare Version unterstützt. API Erfahren Sie, wie Sie das und APIfür Amazon Lightsail installieren AWS CLIund verwenden.

Preisgestaltung

Mit Lightsail for Research zahlen Sie nur für die Ressourcen, die Sie erstellen und verwenden. Weitere Informationen finden Sie unter Preise für Lightsail for Research.

Verfügbarkeit

Lightsail for Research ist in den gleichen AWS Regionen wie Amazon Lightsail verfügbar, mit Ausnahme der Region USA Ost (Nord-Virginia). Lightsail for Research verwendet auch dieselben Endpunkte wie Lightsail. Informationen zu den derzeit unterstützten AWS Regionen und Endpunkten für Lightsail finden Sie unter Lightsail-Endpunkte und Kontingente in der allgemeinen Referenz.AWS

Amazon Lightsail for Research einrichten

Wenn Sie ein neuer AWS Kunde sind, müssen Sie die auf dieser Seite aufgeführten Einrichtungsvoraussetzungen erfüllen, bevor Sie Amazon Lightsail for Research verwenden.

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für Ihren Root-Benutzer.

   Anweisungen finden Sie im Benutzerhandbuch unter Aktivieren eines virtuellen MFA Geräts für Ihren AWS-Konto IAM Root-Benutzer (Konsole).

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM Identity Center-Benutzer anzumelden, verwenden Sie die Anmeldung, URL die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM Identity Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Tutorial: Erste Schritte mit virtuellen Computern von Lightsail for Research

Verwenden Sie dieses Tutorial, um mit virtuellen Computern von Amazon Lightsail for Research zu beginnen. Sie erfahren, wie Sie einen virtuellen Computer erstellen, eine Verbindung zu ihm herstellen und ihn verwenden. In Lightsail for Research ist ein virtueller Computer eine Forschungs-Workstation, die Sie in der erstellen und verwalten. AWS Cloud Virtuelle Computer basieren auf Lightsail-Linux-Instanzen mit dem Ubuntu-Betriebssystem. Auf Ihrem virtuellen Computer können Sie eine Forschungsanwendung wie JupyterLab,RStudio, Scilab und mehr vorkonfigurieren.

Für den virtuellen Computer, den Sie in diesem Tutorial erstellen, fallen ab dem Zeitpunkt, an dem Sie ihn erstellen, bis zu dem Zeitpunkt, an dem Sie ihn löschen, Nutzungsgebühren an. Das Löschen ist der letzte Schritt in diesem Tutorial. Weitere Informationen zur Preisgestaltung finden Sie unter Preise für Lightsail for Research.

Themen

Schritt 1: Erfüllen der Voraussetzungen

Wenn Sie ein neuer AWS Kunde sind, müssen Sie die Einrichtungsvoraussetzungen erfüllen, bevor Sie Amazon Lightsail for Research verwenden. Weitere Informationen finden Sie unter Amazon Lightsail for Research einrichten.

Schritt 2: Erstellen eines virtuellen Computers

Sie können einen virtuellen Computer mithilfe der Lightsail for Research-Konsole erstellen, wie im folgenden Verfahren beschrieben. Diese Anleitung soll Ihnen helfen, Ihren ersten virtuellen

Computer schnell zu starten. Wir empfehlen außerdem, sich mit den verfügbaren Anwendungen und Hardwareplänen vertraut zu machen. Weitere Informationen erhalten Sie unter Wählen Sie Anwendungsbilder und Hardwarepläne für Lightsail for Research und Erstellen Sie einen virtuellen Lightsail for Research-Computer.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie auf der Startseite die Option Virtuellen Computer erstellen aus.
3. Wählen Sie eine AWS-Region für Ihren virtuellen Computer aus.

   Wählen Sie eine AWS-Region , die Ihrem physischen Standort am nächsten liegt, um die Latenz zu reduzieren.
4. Wählen Sie in API Lightsail eine Anwendung aus, die auch als Blueprint bezeichnet wird.

   Die von Ihnen gewählte Anwendung wird bei der Erstellung auf Ihrem virtuellen Computer installiert und konfiguriert.
5. Wählen Sie einen Hardwareplan, der im API Lightsail auch als Bundle bezeichnet wird.

   Hardwarepläne bieten unterschiedliche Mengen an Rechenleistung, einschließlich CPU V-Cores, Arbeitsspeicher, Speicher und monatlicher Datenübertragung. Lightsail for Research bietet Standardpläne und GPU Pläne für virtuelle Computer. Wählen Sie einen Standardplan, wenn der Rechenaufwand für Ihre Arbeit gering ist. Wählen Sie einen GPU Plan, wenn diese Anforderungen hoch sind, z. B. bei der Ausführung von Modellen für maschinelles Lernen oder anderen rechenintensiven Aufgaben.
6. Geben Sie einen Namen für den virtuellen Computer an.
7. Wählen Sie im Bereich Übersicht die Option Virtuellen Computer erstellen aus.

Sobald Ihr neuer virtueller Computer betriebsbereit ist, fahren Sie mit dem Abschnitt über das Starten seiner Anwendung in diesem Tutorial fort.

Schritt 3: Starten Sie die Anwendung eines virtuellen Computers

Nachdem Sie einen virtuellen Computer erstellt haben und er sich im Status Wird ausgeführt befindet, können Sie eine virtuelle Sitzung in Ihrem Webbrowser starten. Mit der Sitzung können Sie mit der Anwendung, die auf Ihrem virtuellen Computer installiert ist, interagieren und sie verwalten.

1. Wählen Sie im Navigationsbereich der Lightsail for Research-Konsole die Option Virtuelle Computer aus.

2. Suchen Sie den Namen des virtuellen Computers, den Sie in Schritt 1 erstellt haben, und wählen Sie Anwendung starten aus. Zum Beispiel Launch. JupyterLab Eine Anwendungssitzung wird in einem neuen Webbrowser-Fenster geöffnet.

   > **Important**
   >
   > Wenn in Ihrem Webbrowser ein Popup-Blocker installiert ist, müssen Sie möglicherweise Popups von der Domain aws.amazon.com zulassen, bevor Sie Ihre Sitzung öffnen können.

Fahren Sie mit dem nächsten Schritt dieses Tutorials fort, um zu erfahren, wie Sie eine Verbindung zu Ihrem virtuellen Computer herstellen.

Schritt 4: Verbinden mit dem virtuellen Computer

Sie können eine Verbindung mit Ihrem virtuellen Computer mithilfe der folgenden Methoden herstellen:

- Verwenden Sie den browserbasierten NICE DCV Client, der in der Lightsail for Research-Konsole verfügbar ist. Mit können Sie eine grafische Benutzeroberfläche (GUI) verwenden NICEDCV, um mit Ihrer Forschungsanwendung und dem Betriebssystem Ihres virtuellen Computers zu interagieren.

  Mit dem browserbasierten NICE DCV Client können Sie auch auf die Befehlszeilenschnittstelle Ihres virtuellen Computers zugreifen und Dateien übertragen.
- Verwenden Sie einen Secure Shell (SSH) -Client wie Open SSHTTY, Pu oder Windows Subsystem for Linux, um auf die Befehlszeilenschnittstelle Ihres virtuellen Computers zuzugreifen. Mit einem SSH Client können Sie Skripts und Konfigurationsdateien bearbeiten.
- Verwenden Sie Secure Copy (SCP), um Dateien sicher zwischen Ihrem lokalen Computer und Ihrem virtuellen Computer zu übertragen. Mit SCP können Sie Ihre Arbeit lokal beginnen und auf Ihrem virtuellen Computer fortsetzen. Sie können auch Dateien von Ihrem virtuellen Computer herunterladen, um die Arbeit auf Ihren lokalen Computer zu kopieren.

Sie müssen das key pair Ihres virtuellen Computers angeben, um eine Verbindung zu ihm herzustellen SSH oder Dateien zu übertragenSCP. Ein key pair ist ein Satz von Sicherheitsanmeldedaten, mit denen Sie Ihre Identität nachweisen, wenn Sie eine Verbindung zu

einem virtuellen Lightsail for Research-Computer herstellen. Ein Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel.

Weitere Informationen zur Verbindung mit Ihrem virtuellen Computer finden Sie in der folgenden Dokumentation:

- Herstellen einer Verbindung zum Remote Display Protocol:
  - Greifen Sie auf eine virtuelle Computeranwendung von Lightsail for Research zu
  - Greifen Sie auf das Betriebssystem Ihres virtuellen Lightsail for Research-Computers zu
- Stellen Sie eine SSH Verbindung her oder übertragen Sie Dateien mit: SCP
  - Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer
  - Stellen Sie mithilfe von Secure Shell eine Connect zu einem virtuellen Lightsail for Research-Computer her
  - Dateien mithilfe von Secure Copy auf virtuelle Lightsail for Research-Computer übertragen

Fahren Sie mit dem nächsten Schritt dieses Tutorials fort, um mehr über den Speicher Ihres virtuellen Computers zu erfahren.

Schritt 5: Hinzufügen von Speicherplatz zum virtuellen Computer

Lightsail for Research stellt Speichervolumes (Festplatten) auf Blockebene bereit, die Sie an einen virtuellen Computer anschließen können. Obwohl Ihr virtueller Computer mit einem System-Datenträger geliefert wird, können Sie zusätzliche Datenträger hinzufügen, wenn sich Ihre Anforderungen ändern. Sie können einen Datenträger auch von einem virtuellen Computer trennen und an einen anderen virtuellen Computer anschließen.

Wenn Sie über die Konsole eine Festplatte an Ihren virtuellen Computer anschließen, formatiert Lightsail for Research die Festplatte automatisch und mountet sie in Ihrem Betriebssystem. Dieser Vorgang dauert einige Minuten. Sie sollten sich daher vergewissern, dass die Festplatte im Status Mounted ist, bevor Sie sie verwenden.

Weitere Informationen zum Erstellen, Anhängen und Verwalten einer Festplatte finden Sie in der Dokumentation.

- Erstellen Sie eine Speicherfestplatte in der Lightsail for Research-Konsole
- Details zur Speicherfestplatte in der Lightsail for Research-Konsole anzeigen
- Hinzufügen von Speicherplatz zu einem virtuellen Computer in Lightsail for Research

- Trennen Sie in Lightsail for Research eine Festplatte von einem virtuellen Computer
- Löschen Sie ungenutzte Speicherplatten in Lightsail for Research

Fahren Sie mit dem nächsten Schritt dieses Tutorials fort, um mehr über die Sicherung Ihres virtuellen Computers zu erfahren.

Schritt 6: Erstellen eines Snapshots

Schnappschüsse sind eine point-in-time Kopie Ihrer Daten. Sie können Snapshots Ihrer virtuellen Computer erstellen und diese als Baselines für die Erstellung neuer virtueller Computer oder für Datensicherungen verwenden. Ein Snapshot enthält alle Daten, die erforderlich sind, um Ihre virtuellen Computer wiederherzustellen (von dem Zeitpunkt, an dem der Snapshot erstellt wurde).

Weitere Informationen zum Erstellen und Verwalten von Snapshots finden Sie in der folgenden Dokumentation:

- Erstellen Sie Schnappschüsse von virtuellen Computern oder Festplatten mit Lightsail for Research
- Virtuelle Computer- und Festplatten-Snapshots in Lightsail for Research anzeigen und verwalten
- Einen virtuellen Computer oder einen virtuellen Datenträger aus einem Snapshot erstellen
- Löschen Sie einen Snapshot in der Lightsail for Research-Konsole

Um zu erfahren, wie Sie Ihre virtuellen Computer-Ressourcen bereinigen, fahren Sie mit dem nächsten Schritt dieses Tutorials fort.

Schritt 7: Bereinigen

Wenn Sie den für dieses Tutorial erstellten virtuellen Computer nicht mehr benötigen, können Sie ihn löschen. Dadurch fallen keine Gebühren für den virtuellen Computer an.

Durch das Löschen eines virtuellen Computers werden die zugehörigen Snapshots oder angeschlossenen Festplatten nicht gelöscht. Wenn Sie Snapshots und Festplatten erstellt haben, sollten Sie diese manuell löschen, damit keine Gebühren für sie anfallen.

Um Ihren virtuellen Computer für später zu speichern, ohne dass Gebühren zu normalen Stundenpreisen anfallen, können Sie den virtuellen Computer anhalten, anstatt ihn zu löschen. Dann können Sie ihn später erneut starten. Weitere Informationen finden Sie unter Details zum virtuellen

Computer von Lightsail for Research anzeigen. Weitere Informationen zur Preisgestaltung finden Sie unter Preise für Lightsail for Research.

> **Important**
>
> Das Löschen einer Lightsail for Research-Ressource ist eine permanente Aktion. Die gelöschten Daten können nicht wiederhergestellt werden. Wenn Sie die Daten später benötigen, erstellen Sie einen Snapshot Ihres virtuellen Computers, bevor Sie ihn löschen. Weitere Informationen finden Sie unter Erstellen eines Snapshots.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im linken Navigationsbereich Virtuelle Computer aus.
3. Wählen Sie den zu löschenden virtuellen Computer aus.
4. Wählen Sie Aktionen und anschließend Virtuellen Computer löschen.
5. Geben Sie confirm in den Textblock ein. Wählen Sie dann Virtuellen Computer löschen.

Erste Schritte mit datenwissenschaftlichen Anwendungen auf Lightsail for Research

Die folgenden Tutorials bieten zusätzliche Informationen zu den ersten Schritten mit bestimmten Anwendungen, die in Lightsail for Research verfügbar sind.

Themen

> **Note**
>
> Ein ausführliches Tutorial für die ersten Schritte mit Lightsail for Research, das im AWS Public Sector Blog veröffentlicht wurde. RStudio Weitere Informationen finden Sie unter Erste Schritte mit Amazon Lightsail for Research: Ein Tutorial zur Verwendung von. RStudio

JupyterLab Auf Lightsail for Research starten und verwenden

In diesem Tutorial zeigen wir Ihnen, wie Sie mit der Verwaltung und Nutzung Ihres JupyterLab virtuellen Computers in Amazon Lightsail for Research beginnen können.

Themen

Schritt 1: Erfüllen der Voraussetzungen

Erstellen Sie mithilfe der JupyterLab Anwendung einen virtuellen Computer, falls Sie dies noch nicht getan haben. Weitere Informationen finden Sie unter Erstellen Sie einen virtuellen Lightsail for Research-Computer.

Wenn Ihr neuer virtueller Computer betriebsbereit ist, fahren Sie mit dem Abschnitt „ JupyterLab Anwendung starten“ dieses Tutorials fort.

Schritt 2: (Optional) Hinzufügen von Speicherplatz

Ihr virtueller Computer wird mit einer Systemfestplatte geliefert. Wenn sich Ihre Speicheranforderungen ändern, können Sie Ihrem virtuellen Computer jedoch zusätzliche Festplatten hinzufügen, um dessen Speicherplatz zu vergrößern.

Sie können Ihre Arbeitsdateien auch auf einer angeschlossenen Festplatte speichern. Anschließend können Sie die Festplatte trennen und an einen anderen virtuellen Computer anschließen, um Ihre Dateien schnell von einem Computer auf einen anderen zu übertragen.

Alternativ können Sie einen Snapshot eines angeschlossenen Datenträgers erstellen, der Ihre Arbeitsdateien enthält, und dann ein Festplatten-Duplikat aus dem Snapshot erstellen. Anschließend können Sie die neue doppelte Festplatte an einen anderen Computer anschließen, um Ihre Arbeit auf verschiedenen virtuellen Computern zu duplizieren. Weitere Informationen erhalten Sie unter Erstellen Sie eine Speicherfestplatte in der Lightsail for Research-Konsole und Hinzufügen von Speicherplatz zu einem virtuellen Computer in Lightsail for Research.

> **Note**
>
> Wenn Sie über die Konsole eine Festplatte an Ihren virtuellen Computer anschließen, formatiert und mountet Lightsail for Research die Festplatte automatisch. Dieser Vorgang dauert einige Minuten. Sie sollten sich daher vergewissern, dass die Festplatte den Bereitstellungsstatus Mounted erreicht hat, bevor Sie sie verwenden. Standardmäßig mountet Lightsail for Research Festplatten in das Verzeichnis. `/home/lightsail-user/<disk-name>` `<disk-name>`ist der Name, den Sie Ihrer Festplatte gegeben haben.

Schritt 3: Hochladen und Herunterladen von Dateien

Sie können Dateien auf Ihren JupyterLab virtuellen Computer hochladen und Dateien von diesem herunterladen. Führen Sie dazu die folgenden Schritte aus:

1. Besorgen Sie sich ein key pair von Amazon Lightsail. Weitere Informationen finden Sie unter Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer.
2. Sobald Sie das key pair haben, können Sie es verwenden, um mit dem Secure Copy (SCP) - Hilfsprogramm eine Verbindung herzustellen. SCPermöglicht das Hoch- und Herunterladen von Dateien über die Befehlszeile oder das Terminal. Weitere Informationen finden Sie unter Dateien mithilfe von Secure Copy auf virtuelle Lightsail for Research-Computer übertragen.
3. (Optional) Sie können das key pair auch verwenden, um eine Verbindung zu Ihrem virtuellen Computer herzustellenSSH. Weitere Informationen finden Sie unter Stellen Sie mithilfe von Secure Shell eine Connect zu einem virtuellen Lightsail for Research-Computer her.

> **Note**
>
> Sie können auch mit dem browserbasierten NICE DCV Client auf die Befehlszeilenschnittstelle Ihres virtuellen Computers zugreifen und Dateien übertragen. NICEDCVist in der Lightsail for Research-Konsole verfügbar. Weitere Informationen erhalten Sie unter Greifen Sie auf eine virtuelle Computeranwendung von Lightsail for Research zu und Greifen Sie auf das Betriebssystem Ihres virtuellen Lightsail for Research-Computers zu.

Um Ihre Projektdateien auf einem angeschlossenen Laufwerk zu verwalten, stellen Sie sicher, dass Sie sie in das richtige Mount-Verzeichnis für das angeschlossene Laufwerk hochladen. Wenn Sie über die Konsole eine Festplatte an Ihren virtuellen Computer anschließen, formatiert Lightsail for Research die Festplatte automatisch und mountet sie im Verzeichnis. `/home/lightsail-user/<disk-name>` `<disk-name>`ist der Name, den Sie Ihrer Festplatte gegeben haben.

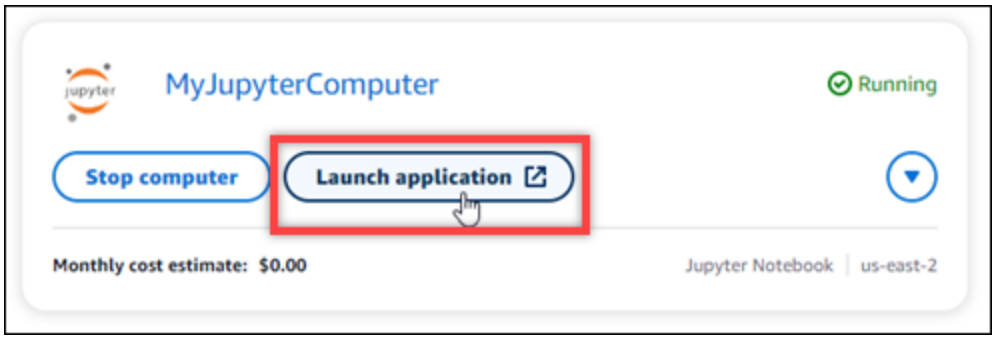
Schritt 4: Starten Sie die JupyterLab Anwendung

Gehen Sie wie folgt vor, um die JupyterLab Anwendung auf Ihrem neuen virtuellen Computer zu starten.

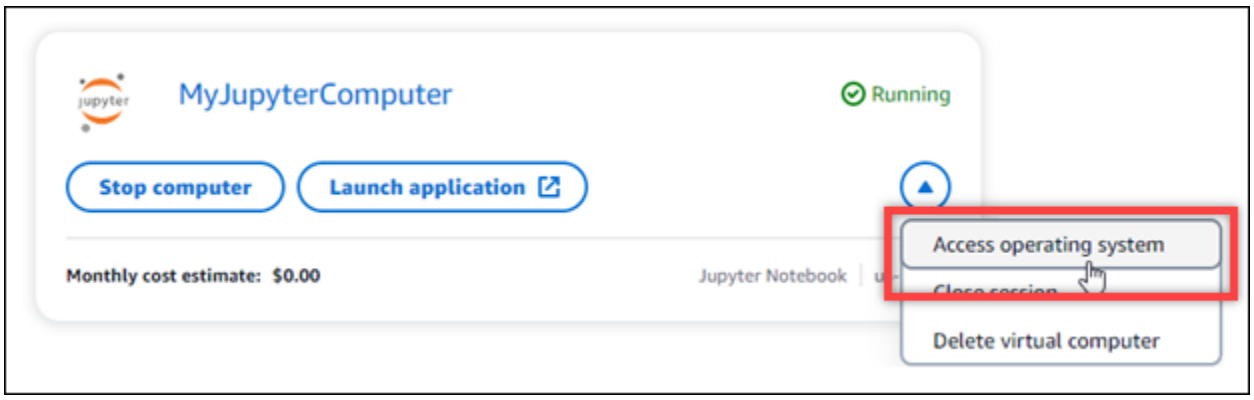
> **Important**
>
> Aktualisieren Sie das Betriebssystem oder die JupyterLab Anwendung nicht, auch wenn Sie dazu aufgefordert werden. Schließen oder ignorieren Sie stattdessen diese Eingabeaufforderungen. Ändern Sie außerdem keine der Dateien, die sich im Verzeichnis /home/lightsail-admin/ befinden. Derartige Schritte könnten den virtuellen Computer unbrauchbar machen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich Virtuelle Computer aus, um die in Ihrem Konto verfügbaren virtuellen Computer anzuzeigen.
3. Suchen Sie auf der Seite Virtuelle Computer nach Ihrem virtuellen Computer und wählen Sie eine der folgenden Optionen, um eine Verbindung zu ihm herzustellen:

   a. (Empfohlen) Wählen Sie Anwendung starten, um die JupyterLab Anwendung im fokussierten Modus zu starten. Wenn Sie in letzter Zeit keine Verbindung zu Ihrem virtuellen Computer hergestellt haben, müssen Sie möglicherweise einige Minuten warten, bis Lightsail for Research Ihre Sitzung vorbereitet.



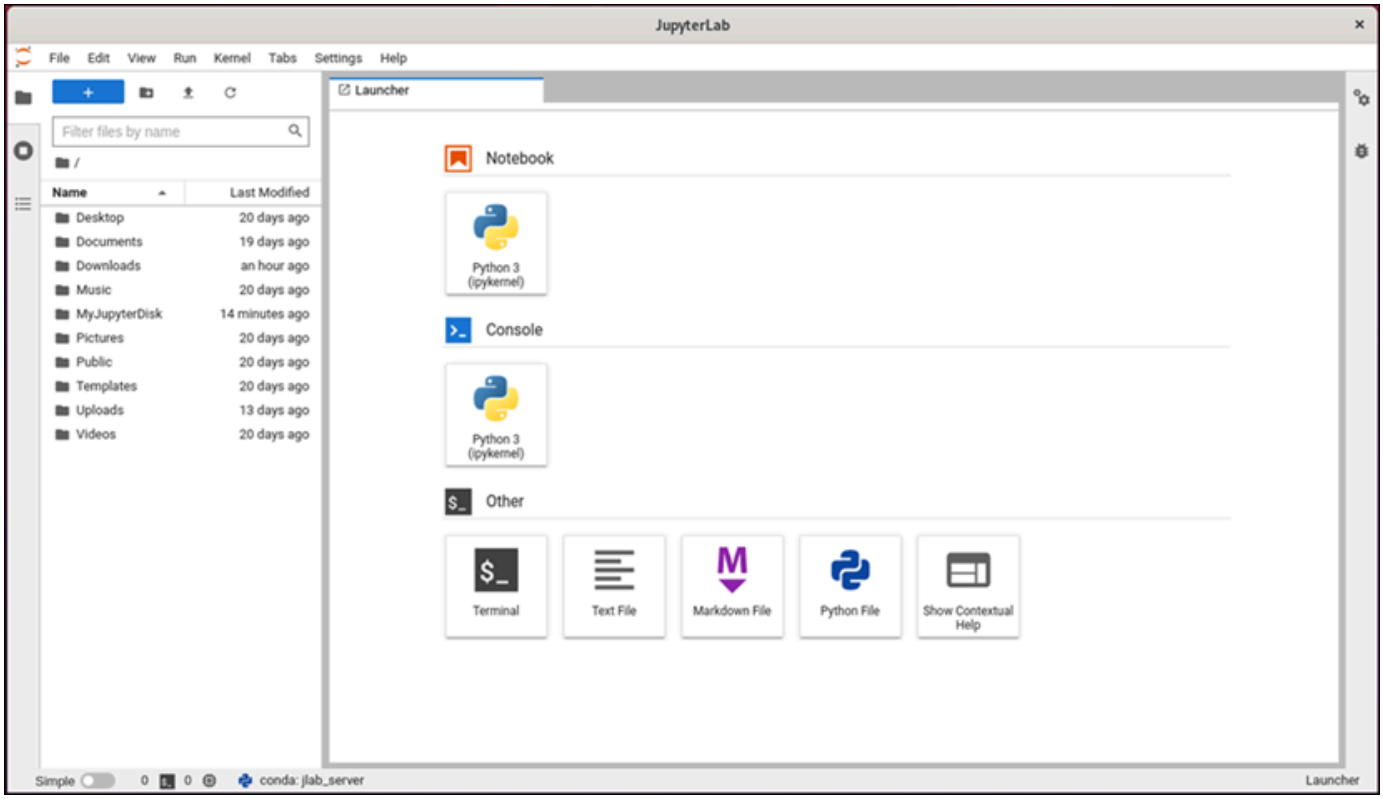
   b. Wählen Sie das Dropdownmenü für den Computer und wählen Sie dann Zugriff auf das Betriebssystem aus, um auf den Desktop Ihres virtuellen Computers zuzugreifen.



Lightsail for Research führt einige Befehle aus, um die Verbindung zum Remote-Display-Protokoll herzustellen. Nach einigen Augenblicken wird eine neue Browser-Registerkarte geöffnet, in der eine virtuelle Desktop-Verbindung zu Ihrem virtuellen Computer hergestellt wird. Wenn Sie die Option Anwendung starten ausgewählt haben, fahren Sie mit dem nächsten Schritt dieses Verfahrens fort, um eine Datei in der JupyterLab Anwendung zu öffnen. Wenn Sie Zugriff auf das Betriebssystem ausgewählt haben, können Sie andere Anwendungen über den Ubuntu-Desktop öffnen.

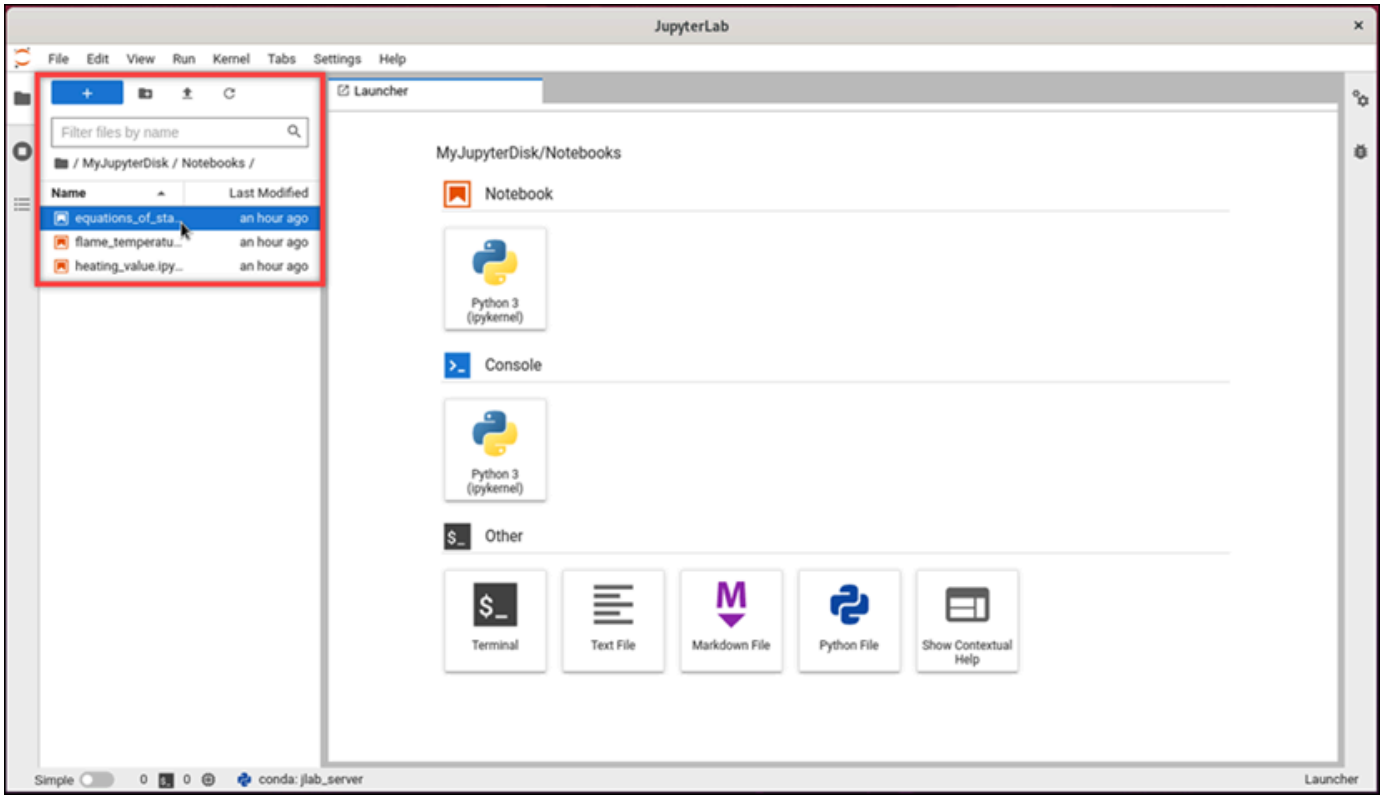
> **Note**
>
> Ihr Browser fordert Sie eventuell auf, Ihre Zwischenablage freizugeben. Wenn Sie dies zulassen, können Sie zwischen Ihrem lokalen Computer und Ihrem virtuellen Computer hin und her kopieren und einfügen.
> Ubuntu fordert Sie möglicherweise auch zu einer Ersteinrichtung auf. Folgen Sie den Anweisungen, bis Sie die Einrichtung abgeschlossen haben und das Betriebssystem verwenden können.

4. Die JupyterLab Anwendung wird geöffnet. Im Launcher-Menü können Sie ein neues Notebook erstellen, die Konsole starten, das Terminal starten und verschiedene Dateien erstellen.

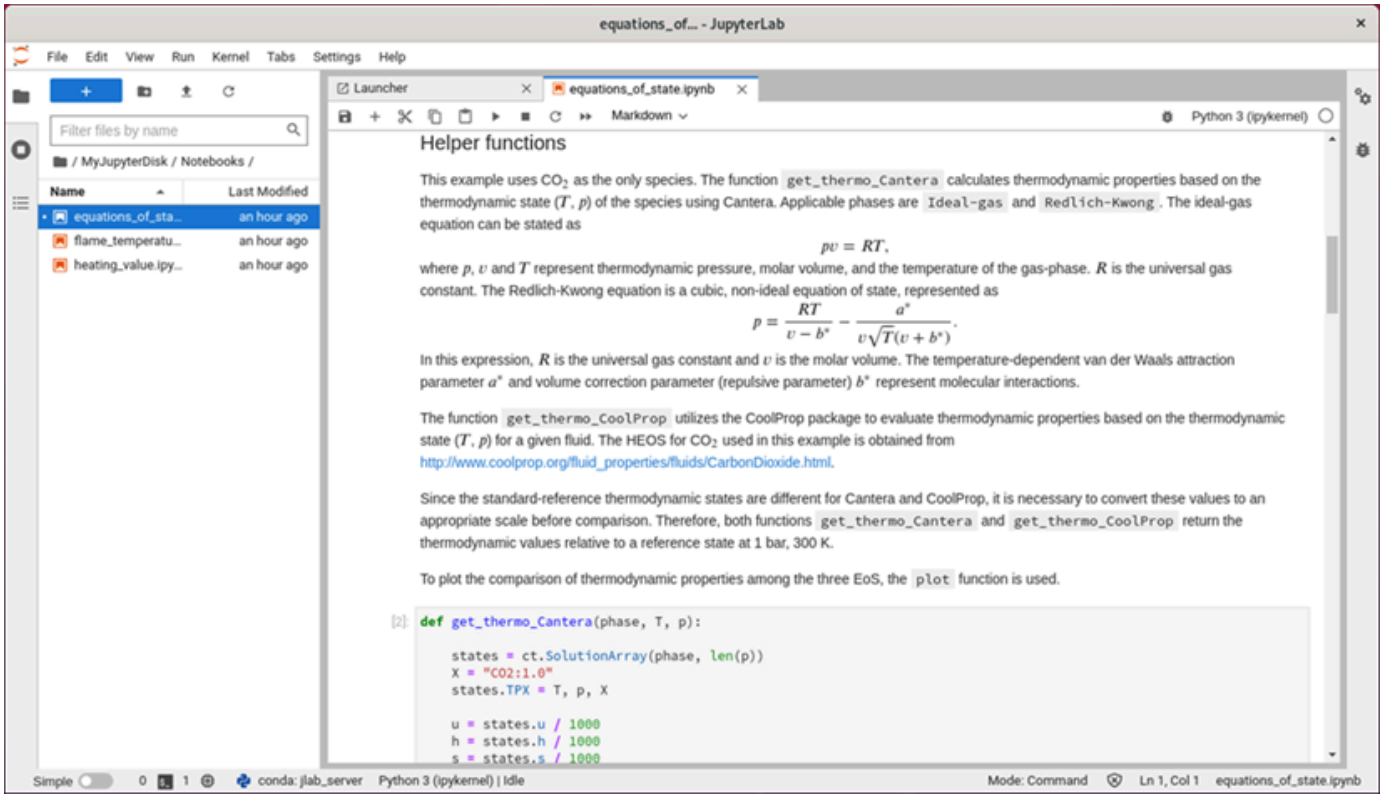


5. Um eine Datei zu öffnen JupyterLab, wählen Sie im Bereich Dateibrowser das Verzeichnis oder den Ordner aus, in dem Ihre Projektdateien gespeichert sind. Wählen Sie dann die zu öffnende Datei.

   Wenn Sie Ihre Projektdateien auf eine angeschlossene Festplatte hochgeladen haben, suchen Sie nach dem Verzeichnis, in dem die Festplatte gemountet ist. Standardmäßig mountet Lightsail for Research Festplatten in das Verzeichnis. `/home/lightsail-user/<disk-name>` *<disk-name>*ist der Name, den Sie Ihrer Festplatte gegeben haben. Im folgenden Beispiel steht das Verzeichnis `MyJupyterDisk` für die bereitgestellte Festplatte, und das Unterverzeichnis `Notebooks` enthält unsere Jupyter-Notebook-Dateien.



Im folgenden Beispiel haben wir die Jupyter-Notebook-Datei `equations_of_state.ipynb` geöffnet.



Weitere Informationen zu den ersten Schritten finden Sie im Abschnitt Schritt 5: Lesen Sie die JupyterLab Dokumentation dieses Tutorials.

Schritt 5: Lesen Sie die JupyterLab Dokumentation

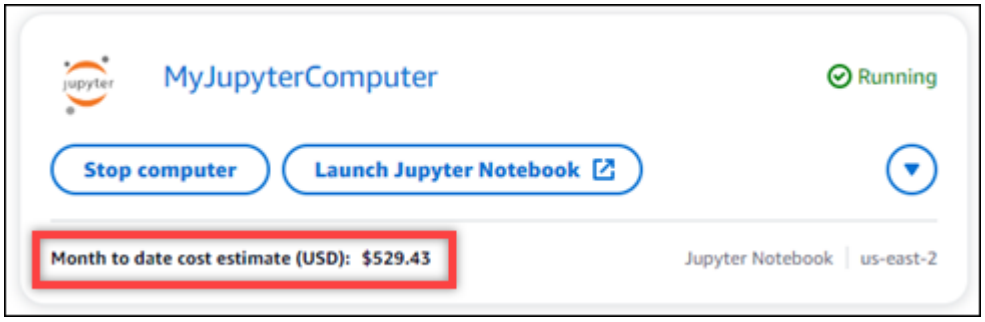
Wenn Sie damit nicht vertraut sind JupyterLab, empfehlen wir Ihnen, die offizielle Dokumentation zu lesen. Die folgenden JupyterLab Online-Ressourcen sind verfügbar:

- JupyterLabDokumentation
- Jupyter-Diskursforum
- JupyterLab auf StackOverflow
- JupyterLab auf GitHub

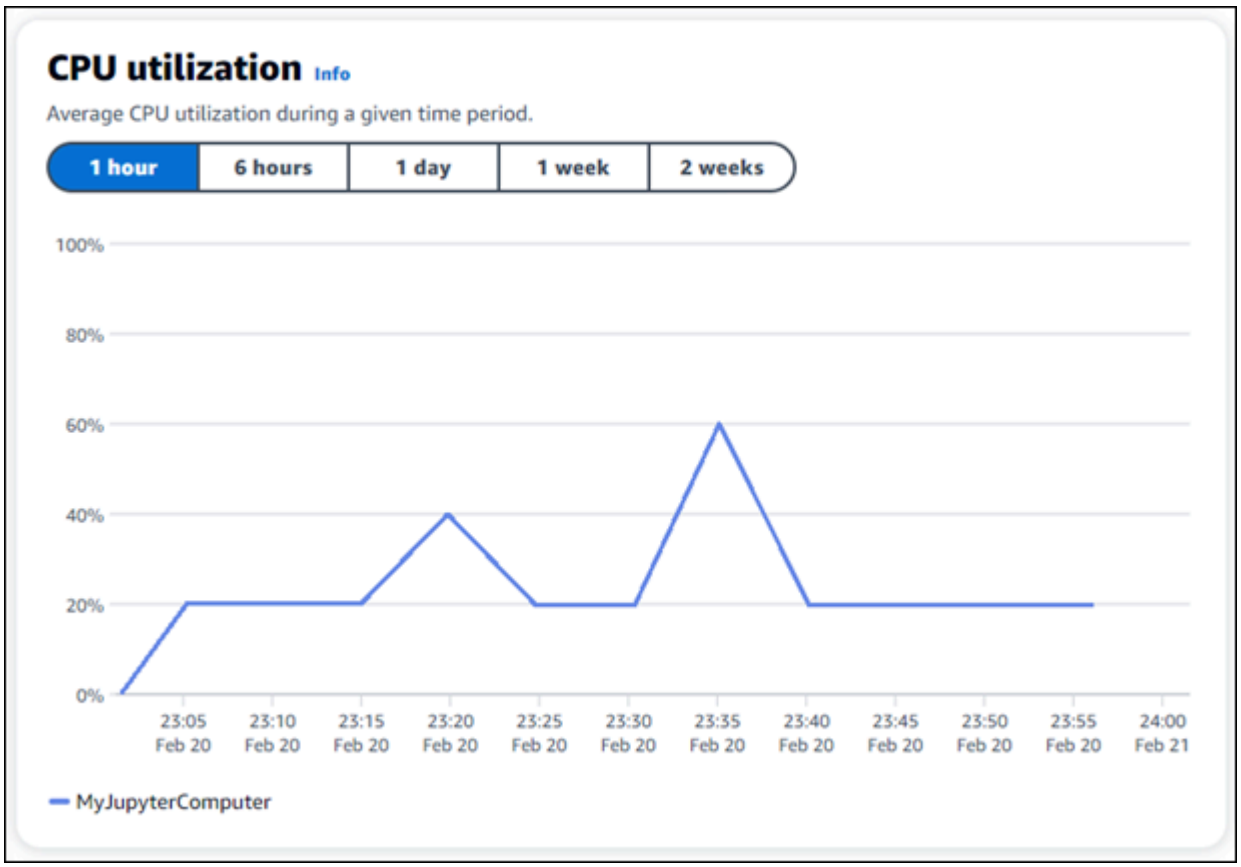
Schritt 6: (Optional) Überwachen von Nutzung und Kosten

Die Kosten- und Nutzungsschätzungen für Ihre Lightsail for Research-Ressourcen seit Monatsbeginn werden in den folgenden Bereichen der Lightsail for Research-Konsole angezeigt.

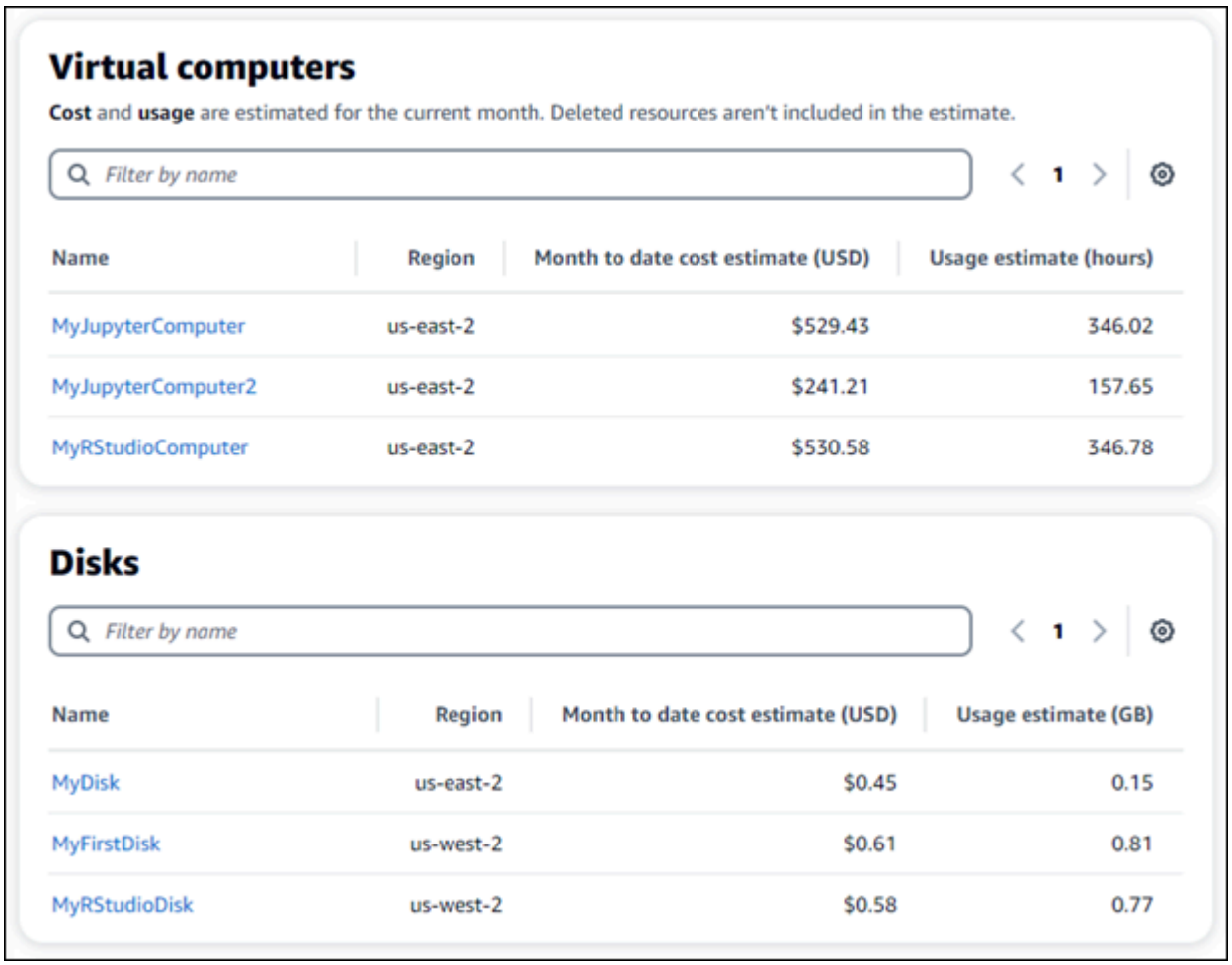
1. Wählen Sie im Navigationsbereich der Lightsail for Research-Konsole die Option Virtuelle Computer aus. Der Kostenvoranschlag für Ihre virtuellen Computer seit Monatsbeginn ist unter jedem laufenden virtuellen Computer aufgeführt.



2. Um die CPU Auslastung eines virtuellen Computers anzuzeigen, wählen Sie den Namen des virtuellen Computers und dann die Registerkarte Dashboard aus.



3. Um die Kosten- und Nutzungsschätzungen für alle Ihre Lightsail for Research-Ressourcen seit Monatsbeginn anzuzeigen, wählen Sie im Navigationsbereich Nutzung aus.



Schritt 7: (Optional) Erstellen einer Kostenkontrollregel

Verwalten Sie die Nutzung und die Kosten Ihrer virtuellen Computer, indem Sie Regeln zur Kostenkontrolle erstellen. Sie können die Regel „Virtuellen Computer im Leerlauf beenden“ erstellen, mit der ein laufender Computer gestoppt wird, wenn er in einem bestimmten Zeitraum einen bestimmten Prozentsatz seiner CPU Auslastung erreicht hat. Mit einer Regel kann beispielsweise ein bestimmter Computer automatisch angehalten werden, wenn seine CPU Auslastung innerhalb von 30 Minuten 5% oder weniger beträgt. Dies kann bedeuten, dass der Computer inaktiv ist und Lightsail for Research den Computer stoppt, sodass Ihnen keine Kosten für eine inaktive Ressource entstehen.

> **Important**
>
> Bevor Sie eine Regel zum Stoppen Ihres virtuellen Computers im Leerlauf erstellen, empfehlen wir, die CPU Auslastung einige Tage lang zu überwachen. Notieren Sie sich die CPU Auslastung, wenn Ihr virtueller Computer unterschiedlichen Belastungen ausgesetzt

ist. Zum Beispiel beim Kompilieren von Code, beim Verarbeiten eines Vorgangs und beim Leerlauf. Auf diese Weise können Sie einen genauen Schwellenwert für die Regel ermitteln. Weitere Informationen finden Sie im Abschnitt Schritt 6: (Optional) Überwachen von Nutzung und Kosten in diesem Tutorial.
Wenn Sie eine Regel mit einem CPU Nutzungsschwellenwert erstellen, der höher ist als Ihre Arbeitslast, kann die Regel Ihren virtuellen Computer nacheinander stoppen. Wenn Sie Ihren virtuellen Computer beispielsweise sofort starten, nachdem eine Regel ihn beendet hat, wird die Regel reaktiviert und der Computer wieder angehalten.

Detaillierte Anweisungen zum Erstellen und Verwalten von Regeln zur Kostenkontrolle finden Sie in den folgenden Anleitungen:

- Regeln zur Kostenkontrolle in Lightsail for Research verwalten
- Erstellen Sie Regeln zur Kostenkontrolle für Ihre virtuellen Lightsail for Research-Computer
- Löschen Sie die Regeln zur Kostenkontrolle für Ihre virtuellen Lightsail for Research-Computer

Schritt 8: (Optional) Erstellen eines Snapshots

Snapshots sind eine point-in-time Kopie Ihrer Daten. Sie können Snapshots Ihrer virtuellen Computer erstellen und diese als Baselines für die Erstellung neuer virtueller Computer oder für Datensicherungen verwenden. Ein Snapshot enthält alle Daten, die erforderlich sind, um Ihre virtuellen Computer wiederherzustellen (von dem Zeitpunkt, an dem der Snapshot erstellt wurde).

Detaillierte Anweisungen zum Erstellen und Verwalten von Snapshots finden Sie in den folgenden Anleitungen:

- Erstellen Sie Schnappschüsse von virtuellen Computern oder Festplatten mit Lightsail for Research
- Virtuelle Computer- und Festplatten-Snapshots in Lightsail for Research anzeigen und verwalten
- Einen virtuellen Computer oder einen virtuellen Datenträger aus einem Snapshot erstellen
- Löschen Sie einen Snapshot in der Lightsail for Research-Konsole

Schritt 9: (Optional) Stoppen oder Löschen des virtuellen Computers

Wenn Sie den für dieses Tutorial erstellten virtuellen Computer nicht mehr benötigen, können Sie ihn löschen. Dadurch fallen keine Gebühren für den virtuellen Computer an.

Durch das Löschen eines virtuellen Computers werden die zugehörigen Snapshots oder angeschlossenen Festplatten nicht gelöscht. Wenn Sie Snapshots und Festplatten erstellt haben, sollten Sie diese manuell löschen, damit keine Gebühren für sie anfallen.

Um Ihren virtuellen Computer für später zu speichern, ohne dass Gebühren zu normalen Stundenpreisen anfallen, können Sie den virtuellen Computer anhalten, anstatt ihn zu löschen. Dann können Sie ihn später erneut starten. Weitere Informationen finden Sie unter Details zum virtuellen Computer von Lightsail for Research anzeigen. Weitere Informationen zur Preisgestaltung finden Sie unter Preise für Lightsail for Research.

> **Important**
>
> Das Löschen einer Lightsail for Research-Ressource ist eine permanente Aktion. Die gelöschten Daten können nicht wiederhergestellt werden. Wenn Sie die Daten später benötigen, erstellen Sie einen Snapshot Ihres virtuellen Computers, bevor Sie ihn löschen. Weitere Informationen finden Sie unter Erstellen eines Snapshots.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im linken Navigationsbereich Virtuelle Computer aus.
3. Wählen Sie den zu löschenden virtuellen Computer aus.
4. Wählen Sie Aktionen und anschließend Virtuellen Computer löschen.
5. Geben Sie confirm in den Textblock ein. Wählen Sie dann Virtuellen Computer löschen.

RStudioAuf Lightsail for Research starten und verwenden

In diesem Tutorial zeigen wir Ihnen, wie Sie mit der Verwaltung und Nutzung Ihres RStudio virtuellen Computers in Amazon Lightsail for Research beginnen können.

> **Note**
>
> Ein ausführliches Tutorial für die ersten Schritte mit Lightsail for Research, das im AWS Public Sector Blog veröffentlicht wurde. RStudio Weitere Informationen finden Sie unter Erste Schritte mit Amazon Lightsail for Research: Ein Tutorial zur Verwendung von. RStudio

Themen

Schritt 1: Erfüllen der Voraussetzungen

Erstellen Sie mithilfe der RStudio Anwendung einen virtuellen Computer, falls Sie dies noch nicht getan haben. Weitere Informationen finden Sie unter Erstellen Sie einen virtuellen Lightsail for Research-Computer.

Schritt 2: (Optional) Hinzufügen von Speicherplatz

Ihr virtueller Computer wird mit einer Systemfestplatte geliefert. Wenn sich Ihre Speicheranforderungen ändern, können Sie Ihrem virtuellen Computer jedoch zusätzliche Festplatten hinzufügen, um dessen Speicherplatz zu vergrößern.

Sie können Ihre Arbeitsdateien auch auf einer angeschlossenen Festplatte speichern. Anschließend können Sie die Festplatte trennen und an einen anderen virtuellen Computer anschließen, um Ihre Dateien schnell von einem Computer auf einen anderen zu übertragen.

Alternativ können Sie einen Snapshot eines angeschlossenen Datenträgers erstellen, der Ihre Arbeitsdateien enthält, und dann ein Festplatten-Duplikat aus dem Snapshot erstellen. Anschließend können Sie die neue doppelte Festplatte an einen anderen Computer anschließen, um Ihre Arbeit auf verschiedenen virtuellen Computern zu duplizieren. Weitere Informationen erhalten Sie unter Erstellen Sie eine Speicherfestplatte in der Lightsail for Research-Konsole und Hinzufügen von Speicherplatz zu einem virtuellen Computer in Lightsail for Research.

> **Note**
>
> Wenn Sie über die Konsole eine Festplatte an Ihren virtuellen Computer anschließen, formatiert und mountet Lightsail for Research die Festplatte automatisch. Dieser Vorgang

dauert einige Minuten. Sie sollten sich daher vergewissern, dass die Festplatte den Bereitstellungsstatus Mounted erreicht hat, bevor Sie sie verwenden. Standardmäßig mountet Lightsail for Research Festplatten in dem `/home/lightsail-user/<disk-name>` Verzeichnis, das der Name *<disk-name>* ist, den Sie Ihrer Festplatte gegeben haben.

Schritt 3: Hochladen und Herunterladen von Dateien

Sie können Dateien auf Ihren RStudio virtuellen Computer hochladen und Dateien von diesem herunterladen. Führen Sie dazu die folgenden Schritte aus:

1. Besorgen Sie sich ein key pair von Amazon Lightsail. Weitere Informationen finden Sie unter Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer.
2. Sobald Sie das key pair haben, können Sie es verwenden, um mit dem Secure Copy (SCP) - Hilfsprogramm eine Verbindung herzustellen. SCPermöglicht das Hoch- und Herunterladen von Dateien über die Befehlszeile oder das Terminal. Weitere Informationen finden Sie unter Dateien mithilfe von Secure Copy auf virtuelle Lightsail for Research-Computer übertragen.
3. (Optional) Sie können das key pair auch verwenden, um eine Verbindung zu Ihrem virtuellen Computer herzustellenSSH. Weitere Informationen finden Sie unter Stellen Sie mithilfe von Secure Shell eine Connect zu einem virtuellen Lightsail for Research-Computer her.

> **Note**
>
> Sie können auch mit dem browserbasierten NICE DCV Client auf die Befehlszeilenschnittstelle Ihres virtuellen Computers zugreifen und Dateien übertragen. NICEDCVist in der Lightsail for Research-Konsole verfügbar. Weitere Informationen erhalten Sie unter Greifen Sie auf eine virtuelle Computeranwendung von Lightsail for Research zu und Greifen Sie auf das Betriebssystem Ihres virtuellen Lightsail for Research-Computers zu.

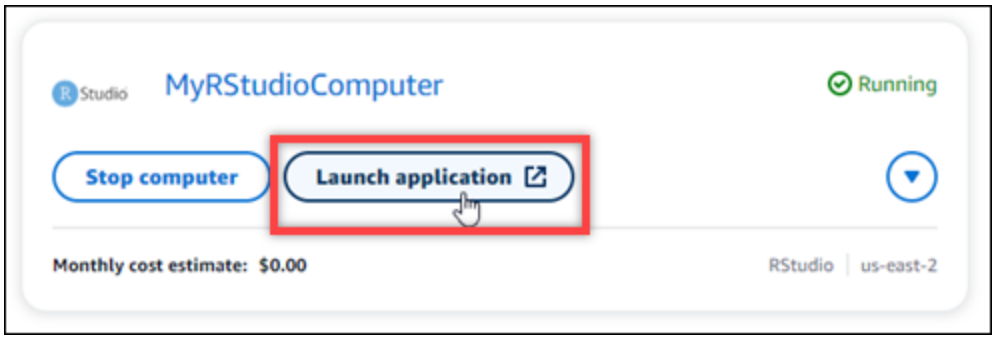
Schritt 4: Starten Sie die Anwendung RStudio

Gehen Sie wie folgt vor, um die RStudio Anwendung auf Ihrem neuen virtuellen Computer zu starten.

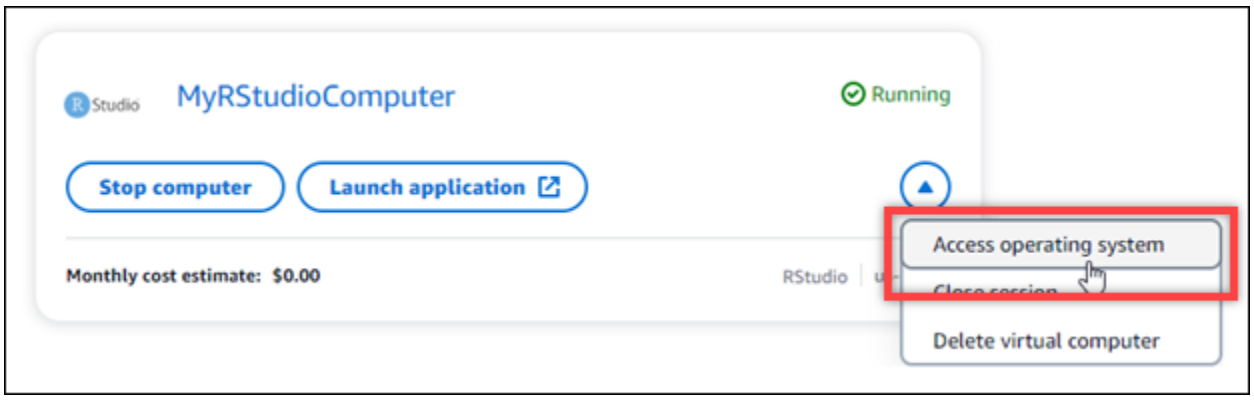
> **Important**
>
> Aktualisieren Sie das Betriebssystem oder die RStudio Anwendung nicht, auch wenn Sie dazu aufgefordert werden. Schließen oder ignorieren Sie stattdessen diese Eingabeaufforderungen. Ändern Sie außerdem keine der Dateien, die sich im Verzeichnis /home/lightsail-admin/ befinden. Derartige Schritte könnten den virtuellen Computer unbrauchbar machen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich Virtuelle Computer aus, um die in Ihrem Konto verfügbaren virtuellen Computer anzuzeigen.
3. Suchen Sie auf der Seite Virtuelle Computer nach Ihrem virtuellen Computer und wählen Sie eine der folgenden Optionen, um eine Verbindung zu ihm herzustellen:

   a. (Empfohlen) Wählen Sie Anwendung starten, um die RStudio Anwendung im fokussierten Modus zu starten. Wenn Sie in letzter Zeit keine Verbindung zu Ihrem virtuellen Computer hergestellt haben, müssen Sie möglicherweise einige Minuten warten, bis Lightsail for Research Ihre Sitzung vorbereitet.

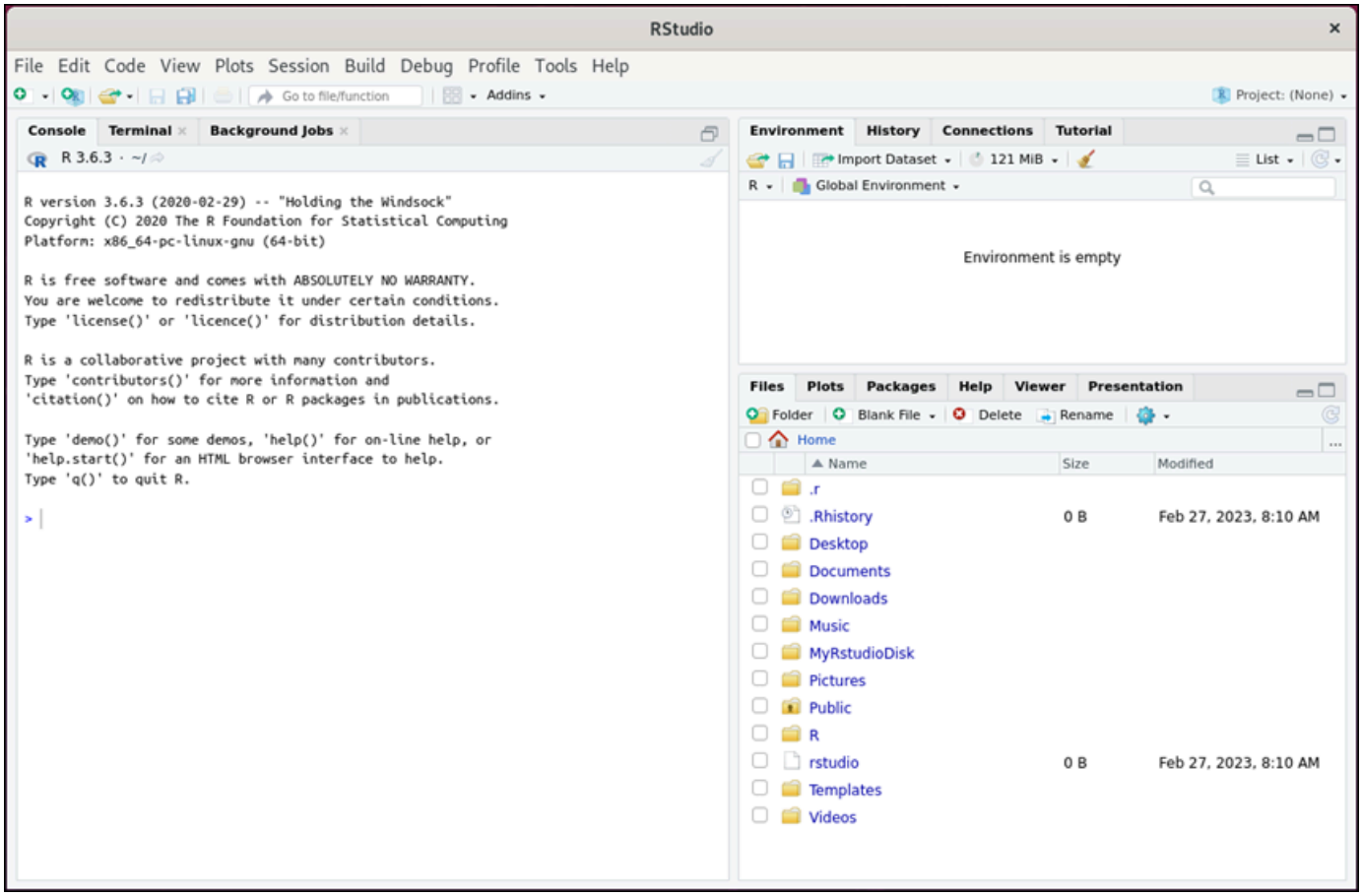
   b. Wählen Sie das Dropdownmenü für den Computer und wählen Sie dann Zugriff auf das Betriebssystem aus, um auf den Desktop Ihres virtuellen Computers zuzugreifen. Tun Sie das, wenn Sie eine andere Anwendung auf dem Betriebssystem installieren möchten.



Lightsail for Research führt einige Befehle aus, um die Verbindung zum Remote-Display-Protokoll herzustellen. Nach einigen Augenblicken wird eine neue Browser-Registerkarte geöffnet, in der eine virtuelle Desktop-Verbindung zu Ihrem virtuellen Computer hergestellt wird. Wenn Sie die Option Anwendung starten ausgewählt haben, fahren Sie mit dem nächsten Schritt dieses Verfahrens fort, um eine Datei in der RStudio Anwendung zu öffnen. Wenn Sie Zugriff auf das Betriebssystem ausgewählt haben, können Sie andere Anwendungen über den Ubuntu-Desktop öffnen.

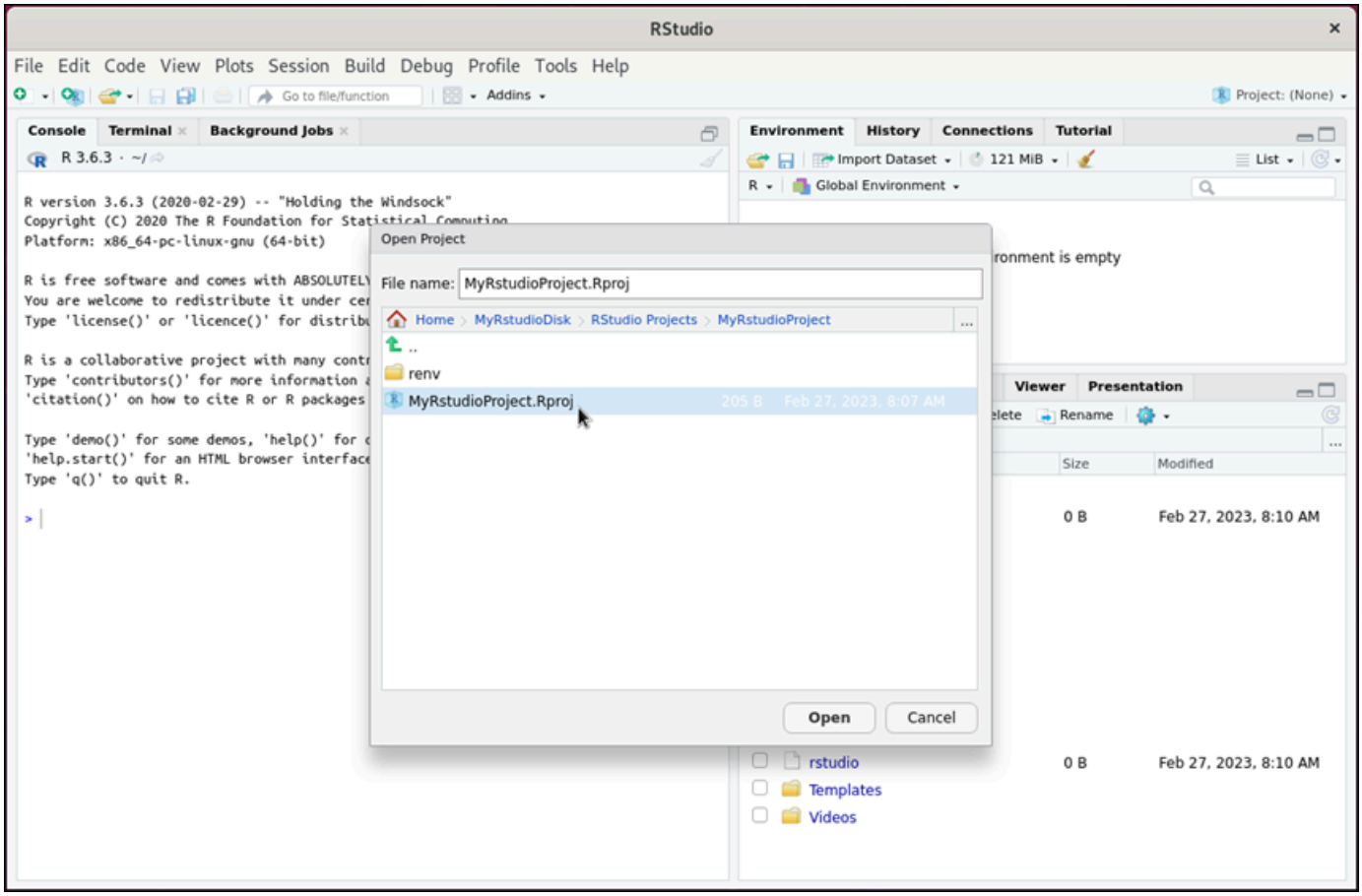
> **Note**
>
> Ihr Browser fordert Sie eventuell auf, Ihre Zwischenablage freizugeben. Wenn Sie dies zulassen, können Sie zwischen Ihrem lokalen Computer und Ihrem virtuellen Computer hin und her kopieren und einfügen.
> Ubuntu fordert Sie möglicherweise auch zu einer Ersteinrichtung auf. Folgen Sie den Anweisungen, bis Sie die Einrichtung abgeschlossen haben und das Betriebssystem verwenden können.

4. Die RStudio Anwendung wird geöffnet.

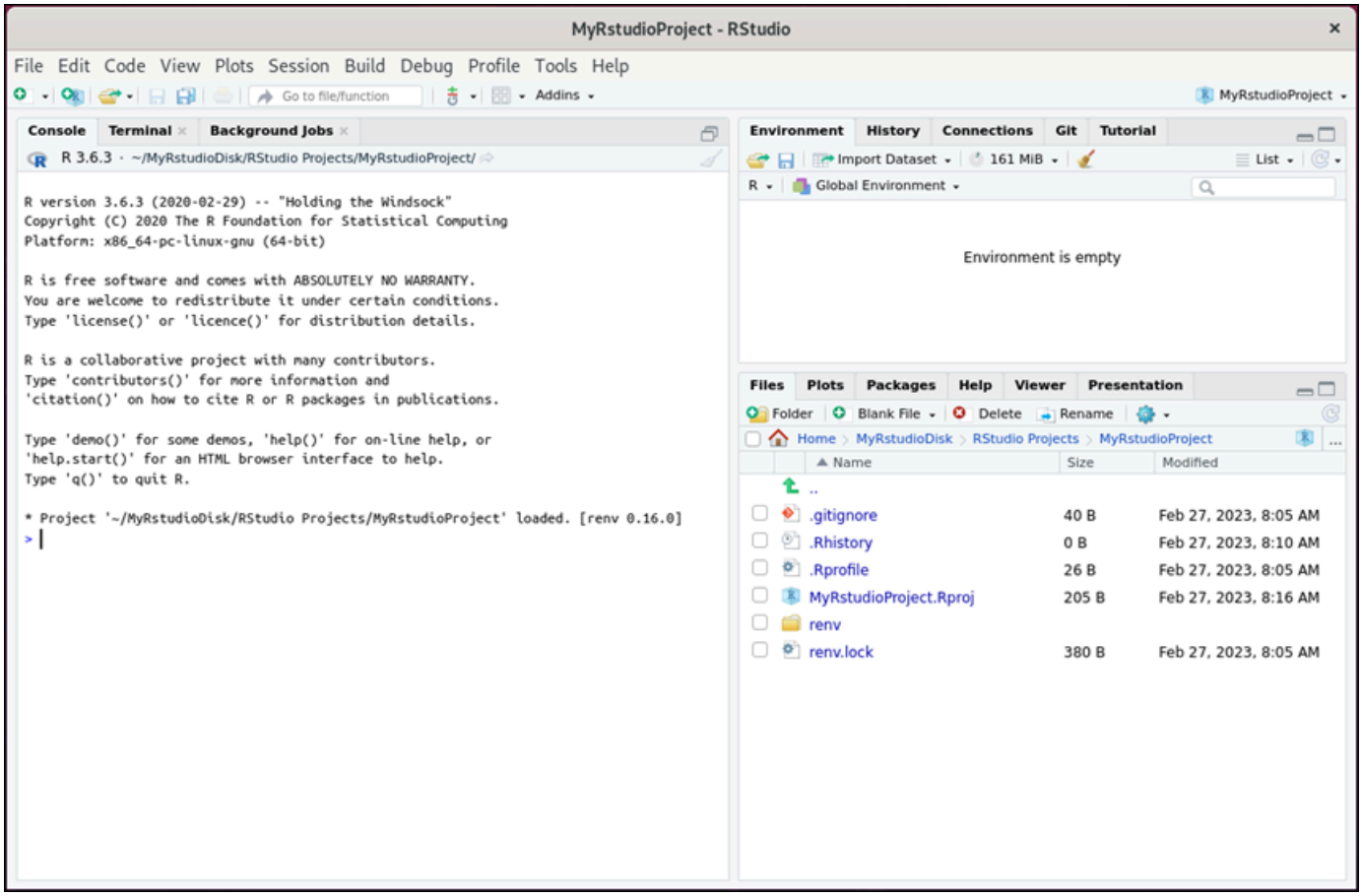


5. Um ein Projekt in zu öffnenRStudio, wählen Sie das Menü Datei und dann Projekt öffnen. Suchen Sie das Verzeichnis oder den Ordner, in dem Ihre Projektdateien gespeichert sind. Wählen Sie dann die zu öffnende Datei.

   Wenn Sie Ihre Projektdateien auf eine angeschlossene Festplatte hochgeladen haben, suchen Sie nach dem Verzeichnis, in dem die Festplatte gemountet ist. Standardmäßig mountet Lightsail for Research Festplatten in das Verzeichnis. `/home/lightsail-user/<disk-name>` `<disk-name>`ist der Name, den Sie Ihrer Festplatte gegeben haben. Im folgenden Beispiel steht das `MyRstudioDisk` Verzeichnis für die bereitgestellte Festplatte, und das `Projects` Unterverzeichnis enthält unsere RStudio Projektdateien.



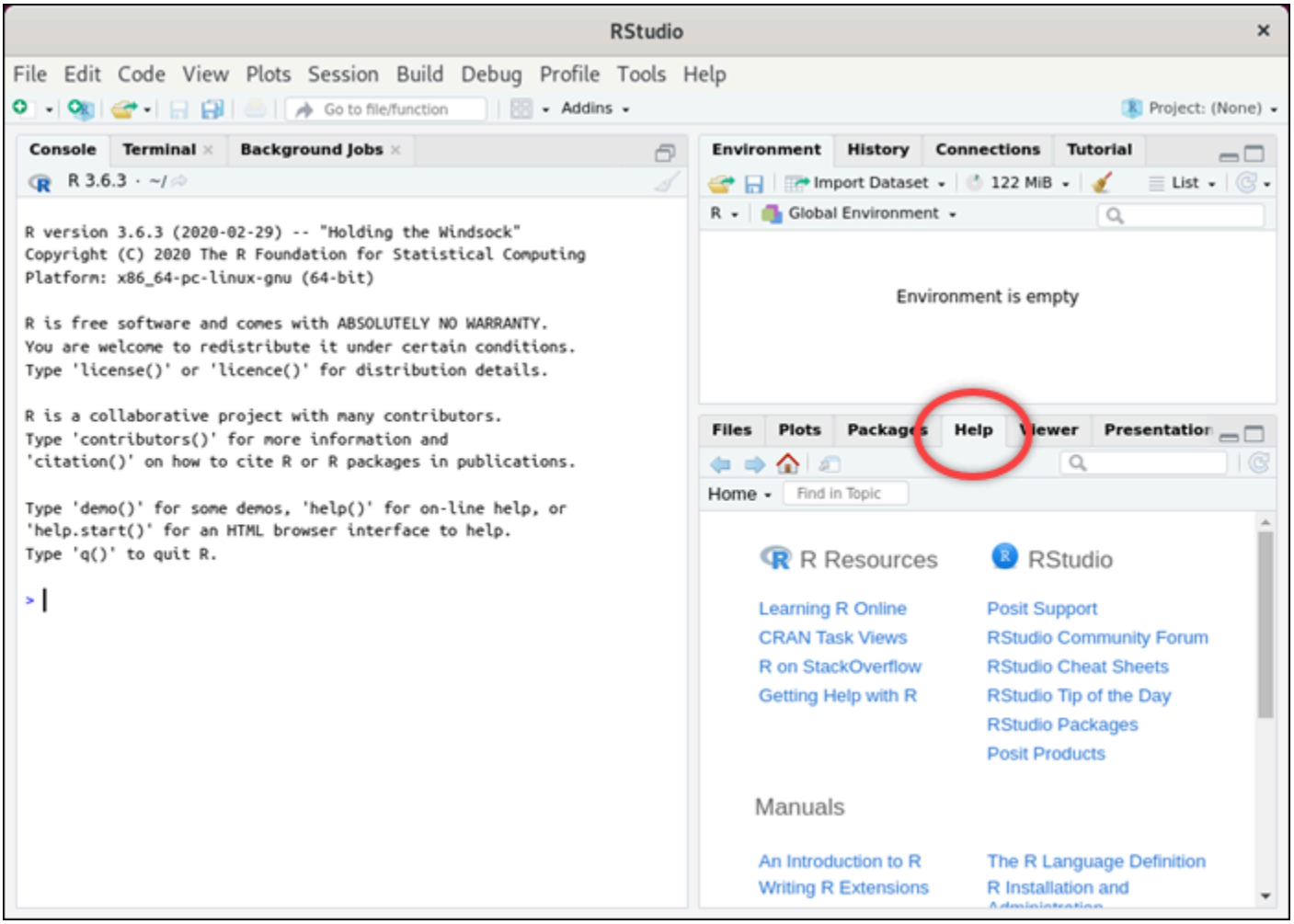
Im folgenden Beispiel haben wir die RStudio-Projektdatei `MyRstudioProject.Rproj` geöffnet.



Informationen zu den ersten Schritten finden Sie im Schritt 5: Lesen Sie die RStudio Dokumentation Abschnitt dieses Tutorials. RStudio

Schritt 5: Lesen Sie die RStudio Dokumentation

Die RStudio Anwendung ist mit einem umfassenden Dokumentationspaket gebündelt. Um mit dem Lernen zu beginnenRStudio, empfehlen wir Ihnen, RStudio wie im folgenden Beispiel gezeigt, auf die Registerkarte Hilfe zuzugreifen.



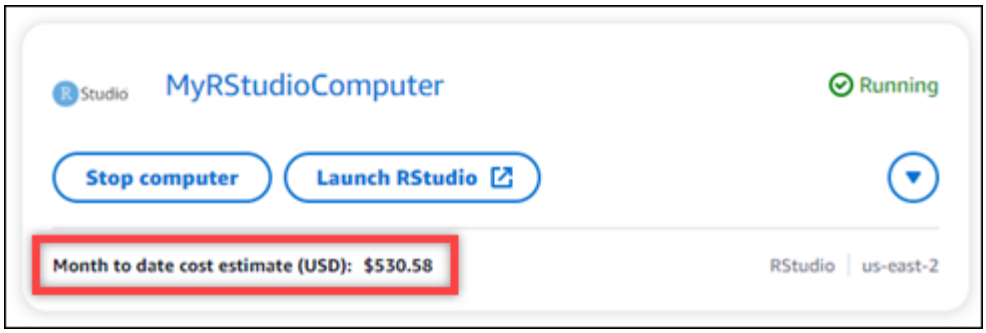
Die folgenden RStudio Online-Ressourcen sind ebenfalls verfügbar:

- R online lernen
- R ein StackOverflow
- Hilfe für R erhalten
- Posit-Unterstützung
- RStudioGemeinschaftsforum
- RStudioSpickzettel
- RStudioTipp des Tages (Twitter)
- RStudioPakete

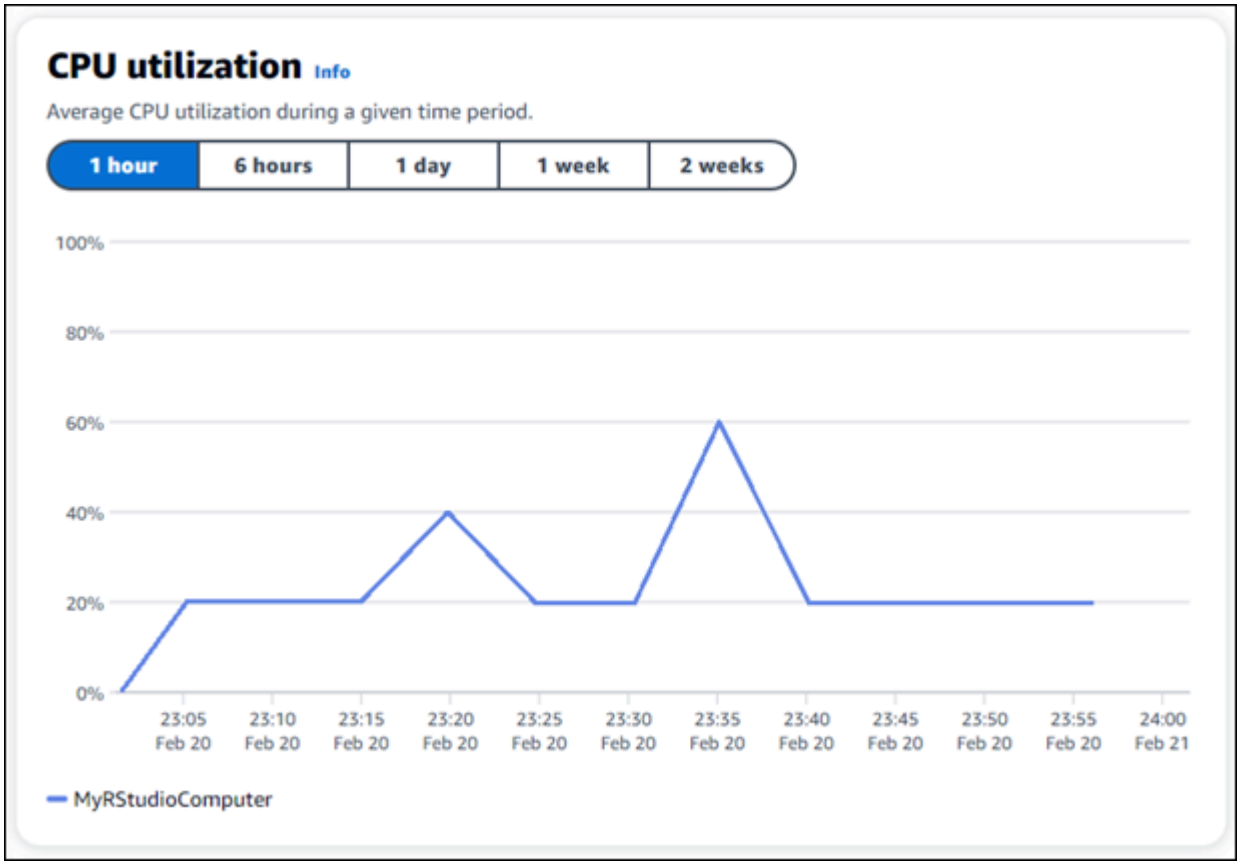
Schritt 6: (Optional) Überwachen von Nutzung und Kosten

Die Kosten- und Nutzungsschätzungen für Ihre Lightsail for Research-Ressourcen seit Monatsbeginn werden in den folgenden Bereichen der Lightsail for Research-Konsole angezeigt.

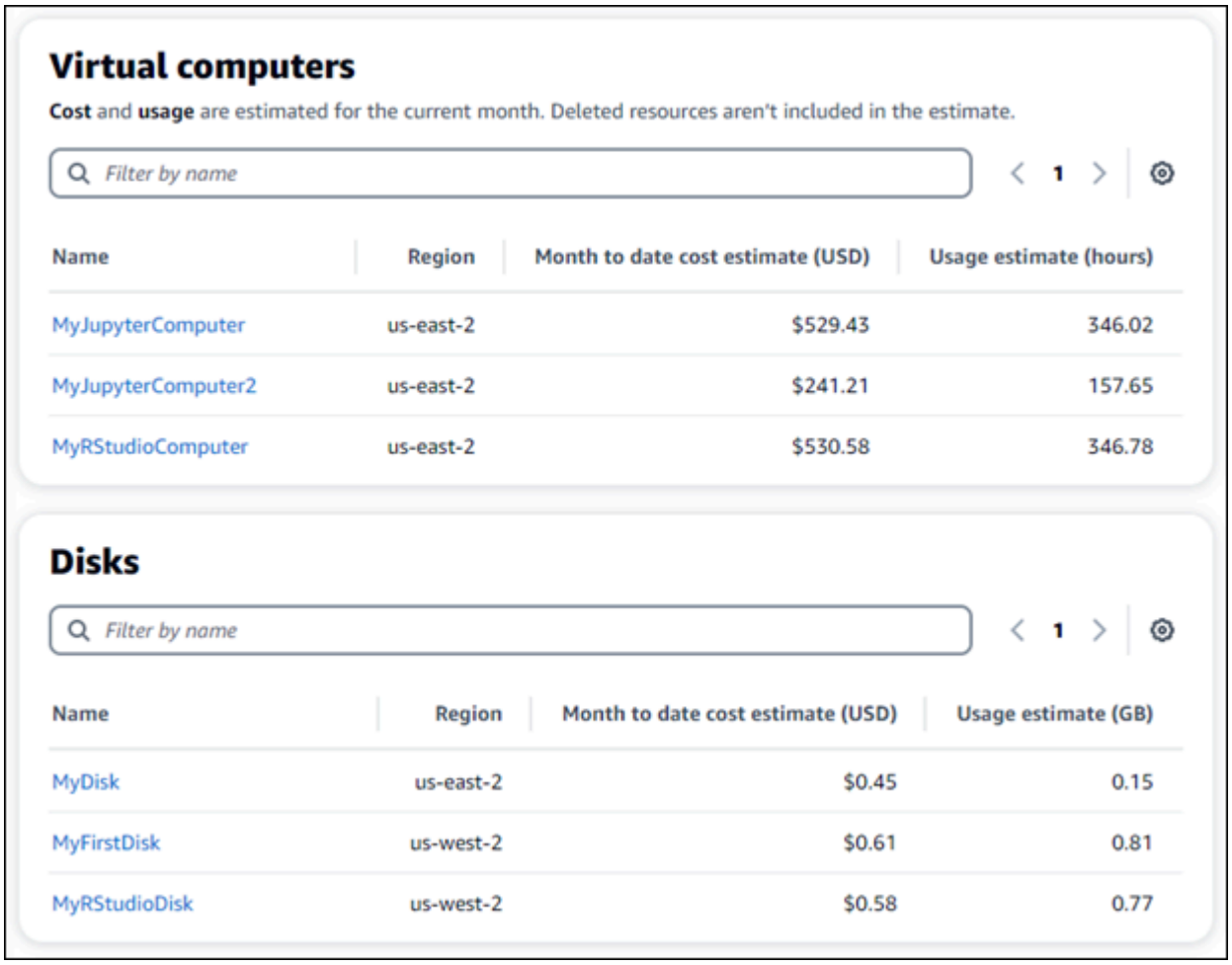
1. Wählen Sie im Navigationsbereich der Lightsail for Research-Konsole die Option Virtuelle Computer aus. Der Kostenvoranschlag für Ihre virtuellen Computer seit Monatsbeginn ist unter jedem laufenden virtuellen Computer aufgeführt.



2. Um die CPU Auslastung eines virtuellen Computers anzuzeigen, wählen Sie den Namen des virtuellen Computers und dann die Registerkarte Dashboard aus.



3. Um die Kosten- und Nutzungsschätzungen für alle Ihre Lightsail for Research-Ressourcen seit Monatsbeginn anzuzeigen, wählen Sie im Navigationsbereich Nutzung aus.



Schritt 7: (Optional) Erstellen einer Kostenkontrollregel

Verwalten Sie die Nutzung und die Kosten Ihrer virtuellen Computer, indem Sie Regeln zur Kostenkontrolle erstellen. Sie können die Regel „Virtuellen Computer im Leerlauf beenden“ erstellen, mit der ein laufender Computer gestoppt wird, wenn er in einem bestimmten Zeitraum einen bestimmten Prozentsatz seiner CPU Auslastung erreicht hat. Mit einer Regel kann beispielsweise ein bestimmter Computer automatisch angehalten werden, wenn seine CPU Auslastung innerhalb von 30 Minuten 5% oder weniger beträgt. Dies kann bedeuten, dass der Computer inaktiv ist und Lightsail for Research den Computer stoppt, sodass Ihnen keine Kosten für eine inaktive Ressource entstehen.

> **Important**
>
> Bevor Sie eine Regel zum Stoppen Ihres virtuellen Computers im Leerlauf erstellen, empfehlen wir, die CPU Auslastung einige Tage lang zu überwachen. Notieren Sie sich die CPU Auslastung, wenn Ihr virtueller Computer unterschiedlichen Belastungen ausgesetzt ist. Zum Beispiel beim Kompilieren von Code, beim Verarbeiten eines Vorgangs und beim Leerlauf. Auf diese Weise können Sie einen genauen Schwellenwert für die Regel ermitteln. Weitere Informationen finden Sie im Abschnitt Schritt 6: (Optional) Überwachen von Nutzung und Kosten in diesem Tutorial.
>
> Wenn Sie eine Regel mit einem CPU Nutzungsschwellenwert erstellen, der höher ist als Ihre Arbeitslast, kann die Regel Ihren virtuellen Computer nacheinander stoppen. Wenn Sie Ihren virtuellen Computer beispielsweise sofort starten, nachdem eine Regel ihn beendet hat, wird die Regel reaktiviert und der Computer wieder angehalten.

Detaillierte Anweisungen zum Erstellen und Verwalten von Regeln zur Kostenkontrolle finden Sie in den folgenden Anleitungen:

- Regeln zur Kostenkontrolle in Lightsail for Research verwalten
- Erstellen Sie Regeln zur Kostenkontrolle für Ihre virtuellen Lightsail for Research-Computer
- Löschen Sie die Regeln zur Kostenkontrolle für Ihre virtuellen Lightsail for Research-Computer

Schritt 8: (Optional) Erstellen eines Snapshots

Snapshots sind eine point-in-time Kopie Ihrer Daten. Sie können Snapshots Ihrer virtuellen Computer erstellen und diese als Baselines für die Erstellung neuer virtueller Computer oder für Datensicherungen verwenden. Ein Snapshot enthält alle Daten, die erforderlich sind, um Ihre virtuellen Computer wiederherzustellen (von dem Zeitpunkt, an dem der Snapshot erstellt wurde).

Detaillierte Anweisungen zum Erstellen und Verwalten von Snapshots finden Sie in den folgenden Anleitungen:

- Erstellen Sie Schnappschüsse von virtuellen Computern oder Festplatten mit Lightsail for Research
- Virtuelle Computer- und Festplatten-Snapshots in Lightsail for Research anzeigen und verwalten
- Einen virtuellen Computer oder einen virtuellen Datenträger aus einem Snapshot erstellen
- Löschen Sie einen Snapshot in der Lightsail for Research-Konsole

Schritt 9: (Optional) Stoppen oder Löschen des virtuellen Computers

Wenn Sie den für dieses Tutorial erstellten virtuellen Computer nicht mehr benötigen, können Sie ihn löschen. Dadurch fallen keine Gebühren für den virtuellen Computer an.

Durch das Löschen eines virtuellen Computers werden die zugehörigen Snapshots oder angeschlossenen Festplatten nicht gelöscht. Wenn Sie Snapshots und Festplatten erstellt haben, sollten Sie diese manuell löschen, damit keine Gebühren für sie anfallen.

Um Ihren virtuellen Computer für später zu speichern, ohne dass Gebühren zu normalen Stundenpreisen anfallen, können Sie den virtuellen Computer anhalten, anstatt ihn zu löschen. Dann können Sie ihn später erneut starten. Weitere Informationen finden Sie unter Details zum virtuellen Computer von Lightsail for Research anzeigen. Weitere Informationen zur Preisgestaltung finden Sie unter Preise für Lightsail for Research.

> **Important**
>
> Das Löschen einer Lightsail for Research-Ressource ist eine permanente Aktion. Die gelöschten Daten können nicht wiederhergestellt werden. Wenn Sie die Daten später benötigen, erstellen Sie einen Snapshot Ihres virtuellen Computers, bevor Sie ihn löschen. Weitere Informationen finden Sie unter Erstellen eines Snapshots.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im linken Navigationsbereich Virtuelle Computer aus.
3. Wählen Sie den zu löschenden virtuellen Computer aus.
4. Wählen Sie Aktionen und anschließend Virtuellen Computer löschen.
5. Geben Sie confirm in den Textblock ein. Wählen Sie dann Virtuellen Computer löschen.

Virtuelle Computer auf Lightsail for Research erstellen und verwalten

Mit Amazon Lightsail for Research können Sie virtuelle Computer in der erstellen. AWS Cloud

Wenn Sie einen virtuellen Computer erstellen, wählen Sie eine Anwendung und einen Hardwareplan aus, den Sie verwenden möchten. Sie können ein Ausgabenlimit für Ihren virtuellen Computer festlegen und bestimmen, was passiert, wenn der virtuelle Computer dieses Limit erreicht. Sie können beispielsweise festlegen, dass der virtuelle Computer automatisch gestoppt wird, sodass Ihnen höchstens das konfigurierte Budget in Rechnung gestellt wird.

> **Important**
>
> Ab dem 22. März 2024 werden virtuelle Computer von Lightsail for Research standardmäßig IMDSv2 durchgesetzt.

Themen

Wählen Sie Anwendungsbilder und Hardwarepläne für Lightsail for Research

Wenn Sie einen virtuellen Computer mit Amazon Lightsail for Research erstellen, wählen Sie eine Anwendung und einen Hardwareplan (Plan) dafür aus.

Eine Anwendung stellt eine Softwarekonfiguration bereit (z. B. eine Anwendung und ein Betriebssystem). Ein Plan stellt die Hardware des virtuellen Computers bereit, z. B. die AnzahlvCPUs, den Arbeitsspeicher, den Speicherplatz und die monatliche Datenübertragungsmenge. Die Anwendung und der Plan bilden zusammen die Konfiguration des virtuellen Computers.

> **Note**
>
> Sie können die Anwendung oder den Plan Ihres virtuellen Computers nach der Erstellung nicht mehr ändern. Sie können jedoch einen Snapshot des virtuellen Computers erstellen und dann einen neuen Plan wählen, wenn Sie anhand des Snapshots einen neuen virtuellen Computer erstellen. Weitere Informationen zu -Snapshots finden Sie unter Backup virtuelle Computer und Festplatten mit Lightsail for Research-Snapshots.

Themen

Anwendungen

Amazon Lightsail for Research stellt Maschinenimages bereit und verwaltet sie, die die Anwendung und das Betriebssystem enthalten, die zum Starten eines virtuellen Computers erforderlich sind. Sie wählen aus einer Liste von Anwendungen, wenn Sie einen virtuellen Computer in Lightsail for Research erstellen. Alle Lightsail for Research-Anwendungsimages verwenden das Betriebssystem Ubuntu (Linux).

Die folgenden Anwendungen sind in Lightsail for Research verfügbar:

- JupyterLab— JupyterLab ist eine webbasierte integrierte Entwicklungsumgebung (IDE) für Notebooks, Code und Daten. Mit der flexiblen Oberfläche können Sie Workflows in den Bereichen Datenwissenschaft, wissenschaftlicher Datenverarbeitung, rechnergestützter Journalismus und

Machine Learning konfigurieren und anordnen. Weitere Informationen finden Sie in der Jupyter-Projektdokumentation.

- RStudio— RStudio ist eine integrierte Open-Source-Entwicklungsumgebung (IDE) für R, eine Programmiersprache für statistische Berechnungen und Grafiken, und Python. Sie kombiniert einen Quellcode-Editor, Tools zur Build-Automatisierung und einen Debugger sowie Tools zum Plotten und zur Workspace-Verwaltung. Weitere Informationen finden Sie in der RStudioIDE.
- VSCodium— VSCodium ist eine von der Community betriebene, binäre Distribution von Microsofts Editor VS Code. Weitere Informationen finden Sie unter. VSCodium
- Scilab – Scilab ist ein Open-Source-Paket für numerische Berechnungen und eine numerisch orientierte High-Level-Programmiersprache. Weitere Informationen finden Sie unter Scilab.
- Ubuntu 20.04 LTS — Ubuntu ist eine Open-Source-Linux-Distribution, die auf Debian basiert. Ubuntu Server ist schlank, schnell und leistungsstark und bietet Dienste zuverlässig, vorhersehbar und wirtschaftlich. Es ist eine hervorragende Grundlage, auf der Sie Ihre virtuellen Computer aufbauen können. Weitere Informationen finden Sie unter Ubuntu-Versionen.

Pläne

Ein Plan enthält die Hardwarespezifikationen und legt die Preise für Ihren virtuellen Lightsail for Research-Computer fest. Ein Plan beinhaltet eine feste Menge an Arbeitsspeicher (RAM), Rechenleistung (vCPUs) und Speicherplatz SSD auf dem Speichervolumen (Festplatte) sowie eine monatliche Datenübertragungsgebühr. Die Pläne werden stündlich und on demand abgerechnet, sodass Sie nur für die Zeit zahlen, in der Ihr virtueller Computer läuft.

Die Wahl des Plans hängt unter Umständen von den Ressourcen ab, die Ihre Workload benötigt. Lightsail for Research bietet die folgenden Tarife an:

- Standard – Standard-Pläne sind für die Datenverarbeitung optimiert und ideal für rechenintensive Anwendungen, die von Hochleistungsprozessoren profitieren.
- GPU— GPU Pläne bieten eine kostengünstige Hochleistungsplattform für allgemeine GPU Computeranwendungen. Mit diesen Plänen können Sie wissenschaftliche, technische und Rendering-Anwendungen sowie -Workloads beschleunigen.

Standardpläne

Im Folgenden finden Sie die Hardwarespezifikationen der in Lightsail for Research verfügbaren Standardpläne.

Name des Plans	vCPUs	Arbeitsspeicher	Speicherplatz	Monatliche Kapazität für die Datenübertragung
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

GPUPläne

Im Folgenden finden Sie die Hardwarespezifikationen der in Lightsail for Research verfügbaren GPU Pläne.

Name des Plans	vCPUs	Arbeitsspeicher	Speicherplatz	Monatliche Kapazität für die Datenübertragung
GPUXL	4	16 GB	50 GB	1 TB
GPU2XL	8	32 GB	50 GB	1 TB
GPU4XL	16	64 GB	50 GB	1 TB

Erstellen Sie einen virtuellen Lightsail for Research-Computer

Gehen Sie wie folgt vor, um einen virtuellen Lightsail for Research-Computer zu erstellen, auf dem eine Anwendung ausgeführt wird.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie auf der Startseite die Option Virtuellen Computer erstellen aus.
3. Wählen Sie einen AWS-Region für Ihren virtuellen Computer aus, der sich in der Nähe Ihres physischen Standorts befindet.

4. Wählen Sie einen Anwendungs- und Hardwareplan aus. Weitere Informationen finden Sie unter Wählen Sie Anwendungsbilder und Hardwarepläne für Lightsail for Research.
5. Geben Sie einen Namen für den virtuellen Computer an. Gültige Zeichen sind alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche.

   Namen von virtuellen Computern müssen außerdem die folgenden Anforderungen erfüllen:

   - Seien Sie AWS-Region in Ihrem Lightsail for Research-Konto in jedem Bereich einzigartig.
   - Sie müssen 2–255 Zeichen enthalten.
   - Sie müssen mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
6. Wählen Sie im Bereich Übersicht die Option Virtuellen Computer erstellen aus.

Innerhalb weniger Minuten ist Ihr virtueller Computer mit Lightsail for Research bereit und Sie können über eine Sitzung mit grafischer Benutzeroberfläche (GUI) eine Verbindung zu ihm herstellen. Weitere Informationen zum Herstellen einer Verbindung mit Ihrem virtuellen Lightsail for Research-Computer finden Sie unter. Greifen Sie auf eine virtuelle Computeranwendung von Lightsail for Research zu

> **Important**
>
> Bei neu erstellten virtuellen Computern sind standardmäßig mehrere Firewall-Ports geöffnet. Weitere Informationen zu diesen Ports finden Sie unter Firewall-Ports für virtuelle Lightsail for Research-Computer verwalten.

Details zum virtuellen Computer von Lightsail for Research anzeigen

Gehen Sie wie folgt vor, um eine Liste der virtuellen Computer und ihrer Details in Ihrem Lightsail for Research-Konto anzuzeigen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich Virtuelle Computer aus, um eine Liste der virtuellen Computer in Ihrem Konto zu öffnen.

Wählen Sie den Namen eines virtuellen Computers aus, um zu seiner Verwaltungsseite zu gelangen. Im Folgenden finden Sie die Informationen, die die Verwaltungsseite enthält:

- Name des virtuellen Computers – Der Name Ihres virtuellen Computers.
- Status – Ihr virtueller Computer kann einer der folgenden Statuscodes sein:
  - Wird erstellt
  - In Ausführung
  - Wird angehalten
  - Angehalten
  - Unbekannt
- AWS-Region— Die, in der AWS-Region Ihr virtueller Computer erstellt wurde.
- Anwendung und Hardware – Der Anwendungs- und Hardwareplan des virtuellen Computers.
- Schätzung der monatlichen Nutzung – Die geschätzte stündliche Nutzung dieses virtuellen Computers für den aktuellen Abrechnungszeitraum.
- Kostenvoranschlag seit Monatsbeginn — Die geschätzten Kosten (inUSD) für den virtuellen Computer für diesen Abrechnungszeitraum.
- Dashboard – Über die Registerkarte Dashboard können Sie eine Sitzung starten, um auf die Anwendung des virtuellen Computers zuzugreifen. Sie können sich auch die CPU Auslastung anzeigen lassen. CPUDie Auslastung identifiziert die Rechenleistung, die von den Anwendungen des virtuellen Computers verbraucht wird. Jeder in der Grafik dargestellte Datenpunkt stellt die durchschnittliche CPU Auslastung über einen bestimmten Zeitraum dar.
- Kostenkontrollregeln – Regeln, die Sie für die Nutzung und die Kosten Ihres virtuellen Computers erstellen.
- Nutzung virtueller Computer – Eine Schätzung der Kosten und Nutzung für den jeweiligen Abrechnungszeitraum. Sie können dies nach Datum und Uhrzeit filtern.
- Speicher – Auf der Registerkarte Speicher können Sie virtuelle Computerfestplatten erstellen, anhängen und trennen. Eine Festplatte ist ein Speichervolume, das Sie an einen virtuellen Computer anschließen und als Festplatte bereitstellen können.
- Tags – Verwalten Sie Ihre virtuellen Computer-Tags auf der Registerkarte „Tags“. Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert. Sie können Tags verwenden, um Ihre Ressourcen zu suchen und zu filtern oder Ihre AWS Kosten zu verfolgen.

Greifen Sie auf eine virtuelle Computeranwendung von Lightsail for Research zu

Gehen Sie wie folgt vor, um die Anwendung zu starten, die auf Ihrem virtuellen Lightsail for Research-Computer ausgeführt wird.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im linken Navigationsbereich Virtuelle Computer aus.
3. Suchen Sie den Namen des virtuellen Computers, von dem aus Sie die Anwendung starten möchten.

   > **Note**
   >
   > Wenn der virtuelle Computer gestoppt ist, klicken Sie zunächst auf die Schaltfläche Computer starten, um ihn hochzufahren.

4. Wählen Sie Anwendung starten. Zum Beispiel Launch. JupyterLab Eine Anwendungssitzung wird in einem neuen Webbrowser-Fenster geöffnet.

   > **Important**
   >
   > Wenn in Ihrem Webbrowser ein Popup-Blocker installiert ist, müssen Sie möglicherweise Popups von der Domain aws.amazon.com zulassen, bevor Sie Ihre Sitzung öffnen können.

Greifen Sie auf das Betriebssystem Ihres virtuellen Lightsail for Research-Computers zu

Gehen Sie wie folgt vor, um auf das Betriebssystem Ihres virtuellen Lightsail for Research-Computers zuzugreifen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im linken Navigationsbereich Virtuelle Computer aus.
3. Suchen Sie den Namen Ihres virtuellen Computers und wählen Sie dann unter dem Status des Computers die Dropdownliste mit den Aktionen aus.

> **Note**
>
> Wenn der virtuelle Computer gestoppt ist, klicken Sie zunächst auf die Schaltfläche Starten, um ihn hochzufahren.

4. Wählen Sie Zugriff auf das Betriebssystem. Eine Betriebssystemsitzung wird in einem neuen Browser-Fenster geöffnet.

> **Important**
>
> Wenn in Ihrem Webbrowser ein Popup-Blocker installiert ist, müssen Sie möglicherweise Popups von der Domain aws.amazon.com zulassen, bevor Sie Ihre Sitzung öffnen können.

Firewall-Ports für virtuelle Lightsail for Research-Computer verwalten

Eine Firewall in Amazon Lightsail for Research kontrolliert den Datenverkehr, der eine Verbindung zu Ihrem virtuellen Computer herstellen darf. Sie fügen der Firewall Ihres virtuellen Computers Regeln hinzu, die das Protokoll, die Ports und die Quelle IPv4 oder IPv6 Adressen angeben, mit denen eine Verbindung hergestellt werden darf. Firewall-Regeln sind stets zulassend, Sie können keine Regeln erstellen, die den Zugriff verweigern. Sie geben Ihrer Firewall Regeln, damit der Datenverkehr Ihren virtuellen Computer erreichen kann. Jeder virtuelle Computer hat zwei Firewalls: eine für IPv4 Adressen und eine für IPv6 Adressen. Beide Firewalls sind unabhängig voneinander und enthalten einen vorkonfigurierten Regelsatz, der den in die Instance eingehenden Datenverkehr filtert.

Protokolle

Ein Protokoll ist das Format, in dem Daten zwischen zwei Computern übertragen werden. Sie können die folgenden Protokolle in einer Firewallregel angeben:

- Das Transmission Control Protocol (TCP) wird hauptsächlich für den Aufbau und die Aufrechterhaltung einer Verbindung zwischen Clients und der Anwendung verwendet, die auf Ihrem virtuellen Computer ausgeführt wird. Es handelt sich um ein weit verbreitetes Protokoll, das Sie häufig in den Firewall-Regeln angeben können.
- Das User Datagram Protocol (UDP) wird hauptsächlich zum Herstellen von Verbindungen mit niedriger Latenz und Verlusttoleranz zwischen Clients und der Anwendung verwendet, die auf Ihrem virtuellen Computer ausgeführt wird. Es ist ideal für Netzwerkanwendungen, in denen die empfundene Latenz kritisch ist, wie Spiele, Sprach- und Videokommunikation.
- Das Internet Control Message Protocol (ICMP) wird hauptsächlich zur Diagnose von Netzwerkkommunikationsproblemen verwendet, z. B. um festzustellen, ob Daten rechtzeitig ihr beabsichtigtes Ziel erreichen. Es ist ideal für das Ping-Dienstprogramm, mit dem Sie die Geschwindigkeit der Verbindung zwischen Ihrem lokalen Computer und Ihrem virtuellen Computer testen können. Es gibt an, wie lange Daten benötigen, bis sie Ihren virtuellen Computer erreichen und zu Ihrem lokalen Computer zurückkehren.
- Alle bedeutet, dass der gesamte Protokolldatenverkehr in Ihre Instance fließen kann. Geben Sie dieses Protokoll an, wenn Sie nicht sicher sind, welches Protokoll angegeben werden soll. Dies schließt alle Internetprotokolle ein, nicht nur die hier angegebenen. Weitere Informationen finden Sie unter Protokollnummern auf der Website der Internet Assigned Numbers Authority.

Ports

Ähnlich wie physische Ports auf Ihrem Computer, mit denen Ihr Computer mit Peripheriegeräten wie Tastatur und Maus kommunizieren kann, dienen Firewall-Ports als Internet-Kommunikationsendpunkte für Ihren virtuellen Computer. Wenn ein Client versucht, eine Verbindung mit Ihrem virtuellen Computer herzustellen, wird ein Port verfügbar gemacht, über den die Kommunikation hergestellt werden kann.

Die Ports, die Sie in einer Firewall-Regel angeben können, können zwischen 0 und 65535 liegen. Wenn Sie eine Firewallregel erstellen, die es einem Client ermöglicht, eine Verbindung mit Ihrem virtuellen Computer herzustellen, geben Sie das zu verwendende Protokoll an. Sie geben auch die Portnummern an, über die die Verbindung hergestellt werden kann, und die IP-Adressen, die eine Verbindung herstellen dürfen.

Die folgenden Ports sind standardmäßig für neu erstellte virtuelle Computer geöffnet.

- TCP
  - 22 — Wird für Secure Shell (SSH) verwendet.
  - 80 — Wird für das Hypertext Transfer Protocol (HTTP) verwendet.
  - 443 — Wird für das Hypertext Transfer Protocol Secure () HTTPS verwendet.
  - 8443 — Wird für das Hypertext Transfer Protocol Secure () verwendet. HTTPS

Gründe für das Öffnen und Schließen von Ports

Wenn Sie Ports öffnen, ermöglichen Sie einem Client, eine Verbindung mit Ihrem virtuellen Computer herzustellen. Wenn Sie Ports schließen, blockieren Sie Verbindungen zu Ihrem virtuellen Computer. Um beispielsweise einem SSH Client zu ermöglichen, eine Verbindung zu Ihrem virtuellen Computer herzustellen, konfigurieren Sie eine Firewallregel, die die TCP Übertragung von Port 22 nur von der IP-Adresse des Computers aus zulässt, der eine Verbindung herstellen muss. In diesem Fall möchten Sie nicht zulassen, dass eine IP-Adresse eine SSH Verbindung zu Ihrem virtuellen Computer herstellt. Dies könnte sonst zu einem Sicherheitsrisiko führen. Wenn diese Regel bereits in der Firewall Ihrer Instanz konfiguriert ist, können Sie sie löschen, um zu verhindern, dass der SSH Client eine Verbindung zu Ihrem virtuellen Computer herstellt.

Die folgenden Verfahren zeigen Ihnen, wie Sie die derzeit auf Ihrem virtuellen Computer geöffneten Ports abrufen, neue Ports öffnen sowie Ports schließen können.

Themen

Erfüllen der Voraussetzungen

Sorgen Sie dafür, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie beginnen.

- Erstellen Sie einen virtuellen Computer in Lightsail for Research. Weitere Informationen finden Sie unter Erstellen Sie einen virtuellen Lightsail for Research-Computer.

- Laden Sie das AWS Command Line Interface ()AWS CLI herunter und installieren Sie es. Weitere Informationen finden Sie unter Installieren oder Aktualisieren auf die neueste Version von AWS CLI im AWS Command Line Interface -Benutzerhandbuch für Version 2.
- Konfigurieren Sie die AWS CLI , um auf Ihre zuzugreifen AWS-Konto. Weitere Informationen finden Sie unter Konfigurationsgrundlagen im AWS Command Line Interface -Benutzerhandbuch für Version 2.

Abrufen des Portstatus für einen virtuellen Computer

Führen Sie das folgende Verfahren durch, um die Portstatus für einen virtuellen Computer abzurufen. Dieses Verfahren verwendet den `get-instance-port-states` AWS CLI Befehl, um den Firewall-Portstatus für einen bestimmten virtuellen Lightsail for Research-Computer, die IP-Adressen, die über die Ports eine Verbindung mit dem virtuellen Computer herstellen dürfen, und das Protokoll abzurufen. Weitere Informationen finden Sie get-instance-port-statesin der AWS CLI Befehlsreferenz.

1. Dieser Schritt wird vom Betriebssystem Ihres lokalen Computers bestimmt.
   - Wenn Ihr lokaler Computer ein Windows-Betriebssystem verwendet, öffnen Sie ein Eingabeaufforderungsfenster.
   - Wenn Ihr lokaler Computer ein Linux- oder UNIX-basiertes Betriebssystem (einschließlich macOS) verwendet, öffnen Sie ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um den Firewall-Portstatus und die zulässigen IP-Adressen und Protokolle abzurufen. Ersetzen Sie den Befehl *REGION* durch den Code der AWS -Region, in der der virtuelle Computer erstellt wurde, z. B. `us-east-2`. Ersetzen Sie *NAME* durch den Namen Ihres virtuellen Computers.

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

   Beispiel

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

   In der Antwort werden die offenen Ports und Protokolle sowie die CIDR IP-Bereiche angezeigt, die eine Verbindung zu Ihrem virtuellen Computer herstellen dürfen.

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

Informationen zum Öffnen von Ports finden Sie im nächsten Abschnitt.

Öffnen von Ports für einen virtuellen Computer

Führen Sie das folgende Verfahren durch, um Ports für einen virtuellen Computer zu öffnen. Dieses Verfahren verwendet den `open-instance-public-ports` AWS CLI Befehl. Sie können Firewall-Ports öffnen, damit Verbindungen über eine vertrauenswürdige IP-Adresse oder einen IP-Adressbereich hergestellt werden können. Um die IP-Adresse `192.0.2.44` zu erlauben, geben Sie `192.0.2.44` oder `192.0.2.44/32` an. Um die IP-Adressen `192.0.2.0` bis `192.0.2.255` zu erlauben, geben Sie `192.0.2.0/24` an. Weitere Informationen finden Sie open-instance-public-portsin der AWS CLI Befehlsreferenz.

1. Dieser Schritt wird vom Betriebssystem Ihres lokalen Computers bestimmt.

   - Wenn Ihr lokaler Computer ein Windows-Betriebssystem verwendet, öffnen Sie ein Eingabeaufforderungsfenster.
   - Wenn Ihr lokaler Computer ein Linux- oder UNIX-basiertes Betriebssystem (einschließlich macOS) verwendet, öffnen Sie ein Terminal-Fenster.

2. Geben Sie den folgenden Befehl ein, um Ports zu öffnen.

   Ersetzen Sie im Befehl die folgenden Elemente:

   - *`REGION`*Ersetzen Sie ihn durch den Code der AWS Region, in der der virtuelle Computer erstellt wurde, z. `us-east-2` B.
   - Ersetzen Sie *`NAME`* durch den Namen Ihres virtuellen Computers.
   - Ersetzen Sie *`FROM-PORT`* durch den ersten Port in einer Reihe von Ports, die Sie öffnen möchten.
   - Ersetzen Sie *`PROTOCOL`* durch den IP-Protokollnamen. Zum BeispielTCP.

- Ersetzen Sie *TO-PORT* durch den letzten Port in einer Reihe von Ports, die Sie öffnen möchten.
- Ersetzen Sie *IP* durch die IP-Adresse oder den IP-Adressbereich, die/den Sie für die Verbindung mit Ihrem virtuellen Computer zulassen möchten.

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

Beispiel

```
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
```

In der Antwort werden die neu hinzugefügten Ports, Protokolle und CIDR IP-Bereiche angezeigt, die eine Verbindung zu Ihrem virtuellen Computer herstellen dürfen.

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

Informationen zum Schließen von Ports finden Sie im nächsten Abschnitt.

Schließen von Ports für einen virtuellen Computer

Führen Sie das folgende Verfahren durch, um Ports für einen virtuellen Computer zu schließen. Dieses Verfahren verwendet den `close-instance-public-ports` AWS CLI Befehl. Weitere Informationen finden Sie close-instance-public-portsin der AWS CLI Befehlsreferenz.

1. Dieser Schritt wird vom Betriebssystem Ihres lokalen Computers bestimmt.

- Wenn Ihr lokaler Computer ein Windows-Betriebssystem verwendet, öffnen Sie ein Eingabeaufforderungsfenster.
- Wenn Ihr lokaler Computer ein Linux- oder UNIX-basiertes Betriebssystem (einschließlich macOS) verwendet, öffnen Sie ein Terminal-Fenster.

2. Geben Sie den folgenden Befehl ein, um Ports zu schließen.

   Ersetzen Sie im Befehl die folgenden Elemente:

   - *REGION*Ersetzen Sie ihn durch den Code der AWS Region, in der der virtuelle Computer erstellt wurde, z. `us-east-2` B.
   - Ersetzen Sie *NAME* durch den Namen Ihres virtuellen Computers.
   - Ersetzen Sie *FROM-PORT* durch den ersten Port in einer Reihe von Ports, die Sie schließen möchten.
   - Ersetzen Sie *PROTOCOL* durch den IP-Protokollnamen. Zum BeispielTCP.
   - Ersetzen Sie *TO-PORT* durch den letzten Port in einer Reihe von Ports, die Sie schließen möchten.
   - Ersetzen Sie *IP* durch die IP-Adresse oder den IP-Adressbereich, die/den Sie entfernen möchten.

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

   Beispiel

   ```
   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
   ```

   In der Antwort werden die Ports, Protokolle und CIDR IP-Bereiche angezeigt, die geschlossen wurden und keine Verbindung mehr zu Ihrem virtuellen Computer herstellen dürfen.

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

Fortfahren mit dem nächsten Schritt

Nachdem Sie die Verwaltung der Firewall-Ports für Ihren virtuellen Computer abgeschlossen haben, können Sie die folgenden zusätzlichen Schritte ausführen:

- Holen Sie sich das Schlüsselpaar Ihres virtuellen Computers. Mit dem key pair können Sie eine Verbindung mit zahlreichen SSH Clients wie Open SSHTTY, Pu und Windows Subsystem für Linux herstellen. Weitere Informationen finden Sie unter Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer.
- Connect zu Ihrem virtuellen Computer herSSH, um ihn über die Befehlszeile zu verwalten. Weitere Informationen finden Sie unter Dateien mithilfe von Secure Copy auf virtuelle Lightsail for Research-Computer übertragen.
- Connect zu Ihrem virtuellen Computer herSCP, um Dateien sicher zu übertragen. Weitere Informationen finden Sie unter Dateien mithilfe von Secure Copy auf virtuelle Lightsail for Research-Computer übertragen.

Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer

Ein key pair, bestehend aus einem öffentlichen und einem privaten Schlüssel, ist ein Satz von Sicherheitsanmeldedaten, mit denen Sie Ihre Identität nachweisen, wenn Sie eine Verbindung zu einem virtuellen Amazon Lightsail for Research-Computer herstellen. Der öffentliche Schlüssel wird auf jedem virtuellen Computer in Lightsail for Research gespeichert, und Sie behalten den privaten Schlüssel auf Ihrem lokalen Computer. Mit dem privaten Schlüssel können Sie auf sichere Weise ein Secure Shell-Protokoll (SSH) mit Ihrem virtuellen Computer einrichten. Jeder, der den privaten

Schlüssel besitzt, kann sich mit Ihrem virtuellen Computer verbinden. Daher ist es wichtig, dass Sie den privaten Schlüssel an einem sicheren Ort aufbewahren.

Ein Amazon Lightsail-Standardschlüsselpaar (DKP) wird automatisch erstellt, wenn Sie zum ersten Mal eine Lightsail-Instance oder einen virtuellen Lightsail for Research-Computer erstellen. Das DKP ist spezifisch für jede AWS Region, in der Sie eine Instance oder einen virtuellen Computer erstellen. Lightsail DKP for the US East (Ohio) Region (us-east-2) gilt beispielsweise für alle Computer, die Sie in den Programmen Lightsail und Lightsail for Research in USA Ost (Ohio) erstellen und die bei ihrer Erstellung so konfiguriert waren, dass sie sie verwenden. DKP Lightsail for Research speichert automatisch den öffentlichen Schlüssel von DKP auf den virtuellen Computern, die Sie erstellen. Sie können den privaten Schlüssel von DKP jederzeit herunterladen, indem Sie den Lightsail-Service API anrufen.

In diesem Dokument zeigen wir Ihnen, wie Sie das DKP für einen virtuellen Computer erhalten. Nachdem Sie den installiert habenDKP, können Sie mithilfe zahlreicher SSH Clients wie Open SSHTTY, Pu und Windows Subsystem für Linux eine Verbindung herstellen. Sie können Secure Copy (SCP) auch verwenden, um Dateien sicher von Ihrem lokalen Computer auf Ihren virtuellen Computer zu übertragen.

> **Note**
>
> Mit dem browserbasierten NICE DCV Client können Sie auch eine Verbindung mit dem Remote-Display-Protokoll zu Ihrem virtuellen Computer herstellen. NICEDCVist in der Lightsail for Research-Konsole verfügbar. Für diesen RDP Client müssen Sie kein key pair für Ihren Computer erwerben. Weitere Informationen erhalten Sie unter Greifen Sie auf eine virtuelle Computeranwendung von Lightsail for Research zu und Greifen Sie auf das Betriebssystem Ihres virtuellen Lightsail for Research-Computers zu.

Themen

Erfüllen der Voraussetzungen

Sorgen Sie dafür, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie beginnen.

- Erstellen Sie einen virtuellen Computer in Lightsail for Research. Weitere Informationen finden Sie unter Erstellen Sie einen virtuellen Lightsail for Research-Computer.
- Laden Sie das AWS Command Line Interface ()AWS CLI herunter und installieren Sie es. Weitere Informationen finden Sie unter Installieren oder Aktualisieren auf die neueste Version von AWS CLI im AWS Command Line Interface -Benutzerhandbuch für Version 2.
- Konfigurieren Sie die AWS CLI , um auf Ihre zuzugreifen AWS-Konto. Weitere Informationen finden Sie unter Konfigurationsgrundlagen im AWS Command Line Interface -Benutzerhandbuch für Version 2.
- Laden Sie jq herunter und installieren Sie es. Es ist ein leichter und flexibler JSON Befehlszeilenprozessor, der in den folgenden Verfahren verwendet wird, um Schlüsselpaardetails aus den JSON Ausgaben von zu extrahieren AWS CLI. Weitere Informationen zum Herunterladen und Installieren von jq finden Sie unter Download jq auf der jq-Website.

Erhalten eines Schlüsselpaars für einen virtuellen Computer

Führen Sie eines der folgenden Verfahren aus, um das Lightsail DKP für einen virtuellen Computer in Lightsail for Research zu erhalten.

Erhalten eines Schlüsselpaars für einen virtuellen Computer mithilfe eines lokalen Windows-Computers

Dieses Verfahren ist für Sie relevant, wenn Ihr lokaler Computer ein Windows-Betriebssystem verwendet. Bei diesem Verfahren wird der `download-default-key-pair` AWS CLI Befehl verwendet, um das Lightsail DKP für eine AWS Region abzurufen. Weitere Informationen finden Sie download-default-key-pairin der AWS CLI Befehlsreferenz.

1. Öffnen Sie ein Befehlszeilenfenster.
2. Geben Sie den folgenden Befehl ein, um das Lightsail DKP für eine bestimmte AWS Region abzurufen. Dieser Befehl speichert die Informationen in einer `dkp-details.json`-Datei. Ersetzen Sie den Befehl *`region-code`* durch den Code der AWS Region, in der der virtuelle Computer erstellt wurde, z. B. `us-east-2`

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

   Beispiel

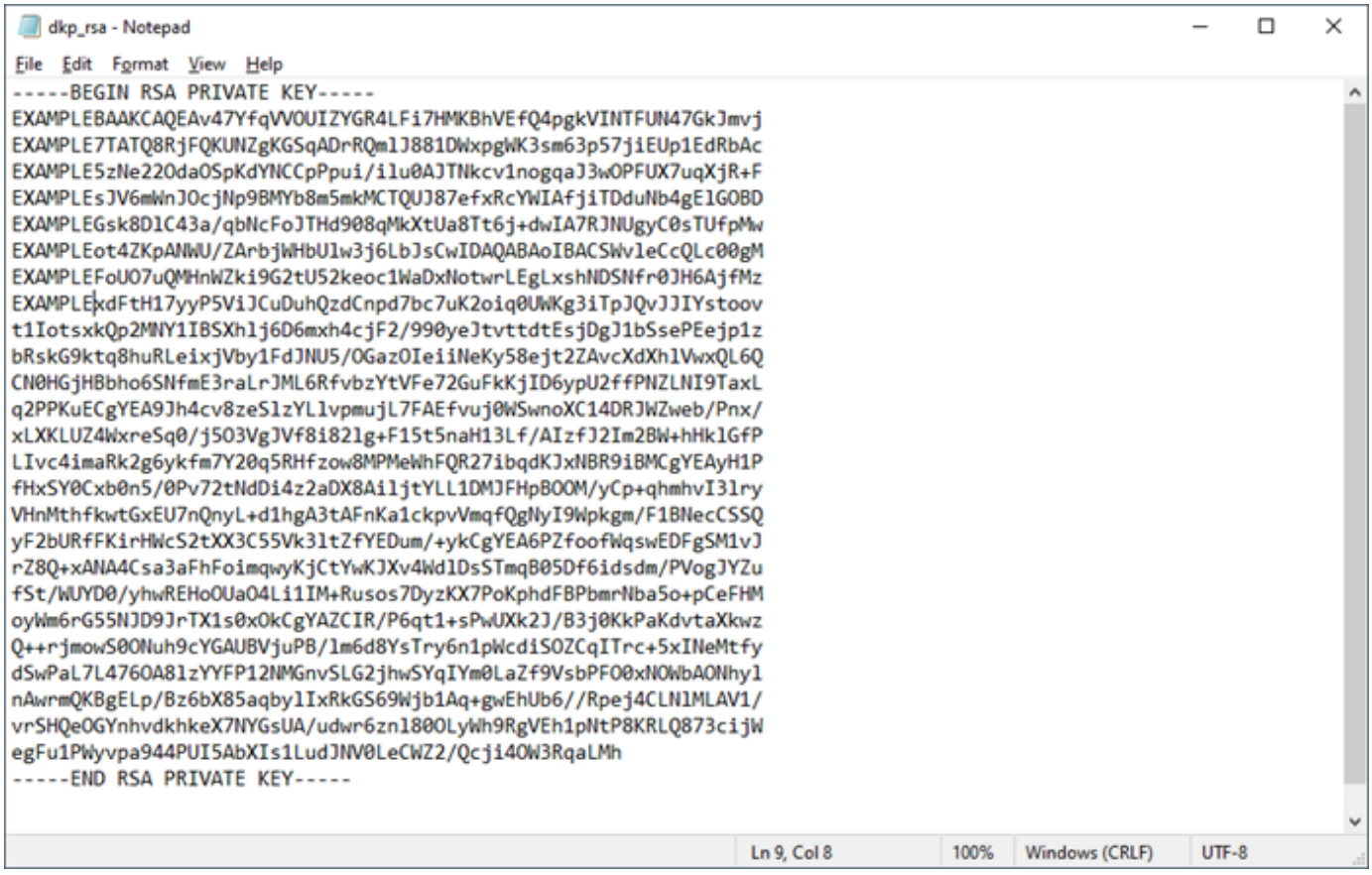
```
aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
```

Es erfolgt keine Antwort auf den Befehl. Sie können überprüfen, ob der Befehl erfolgreich war, indem Sie die `dkp-details.json` Datei öffnen und prüfen, ob die DKP Lightsail-Informationen gespeichert wurden. Der Inhalt der `dkp-details.json`-Datei sollte wie im folgenden Beispiel aussehen. Der Befehl ist fehlgeschlagen, wenn die Datei leer ist.

3. Geben Sie den folgenden Befehl ein, um die Informationen zum privaten Schlüssel aus der `dkp-details.json`-Datei zu extrahieren und zu einer neuen privaten Schlüsseldatei (`dkp_rsa`) hinzuzufügen.

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

Es erfolgt keine Antwort auf den Befehl. Sie können überprüfen, ob der Befehl erfolgreich war, indem Sie die `dkp_rsa`-Dateien öffnen und prüfen, ob sie Informationen enthalten. Der Inhalt der `dkp_rsa`-Datei sollte wie im folgenden Beispiel aussehen. Der Befehl ist fehlgeschlagen, wenn die Datei leer ist.



Sie verfügen jetzt über den erforderlichen privaten Schlüssel, um eine SSH SCP Oder-Verbindung zu Ihrem virtuellen Computer herzustellen. Fahren Sie mit dem nächsten Abschnitt fort, um weitere Schritte zu erfahren.

Erhalten eines Schlüsselpaars für einen virtuellen Computer mithilfe eines lokalen Linux-, Unix- oder macOS-Computers

Dieses Verfahren ist für Sie relevant, wenn Ihr lokaler Computer ein Linux-, Unix- oder macOS-Betriebssystem verwendet. Bei diesem Verfahren wird der `download-default-key-pair` AWS CLI Befehl verwendet, um das Lightsail DKP für eine AWS Region abzurufen. Weitere Informationen finden Sie download-default-key-pairin der AWS CLI Befehlsreferenz.

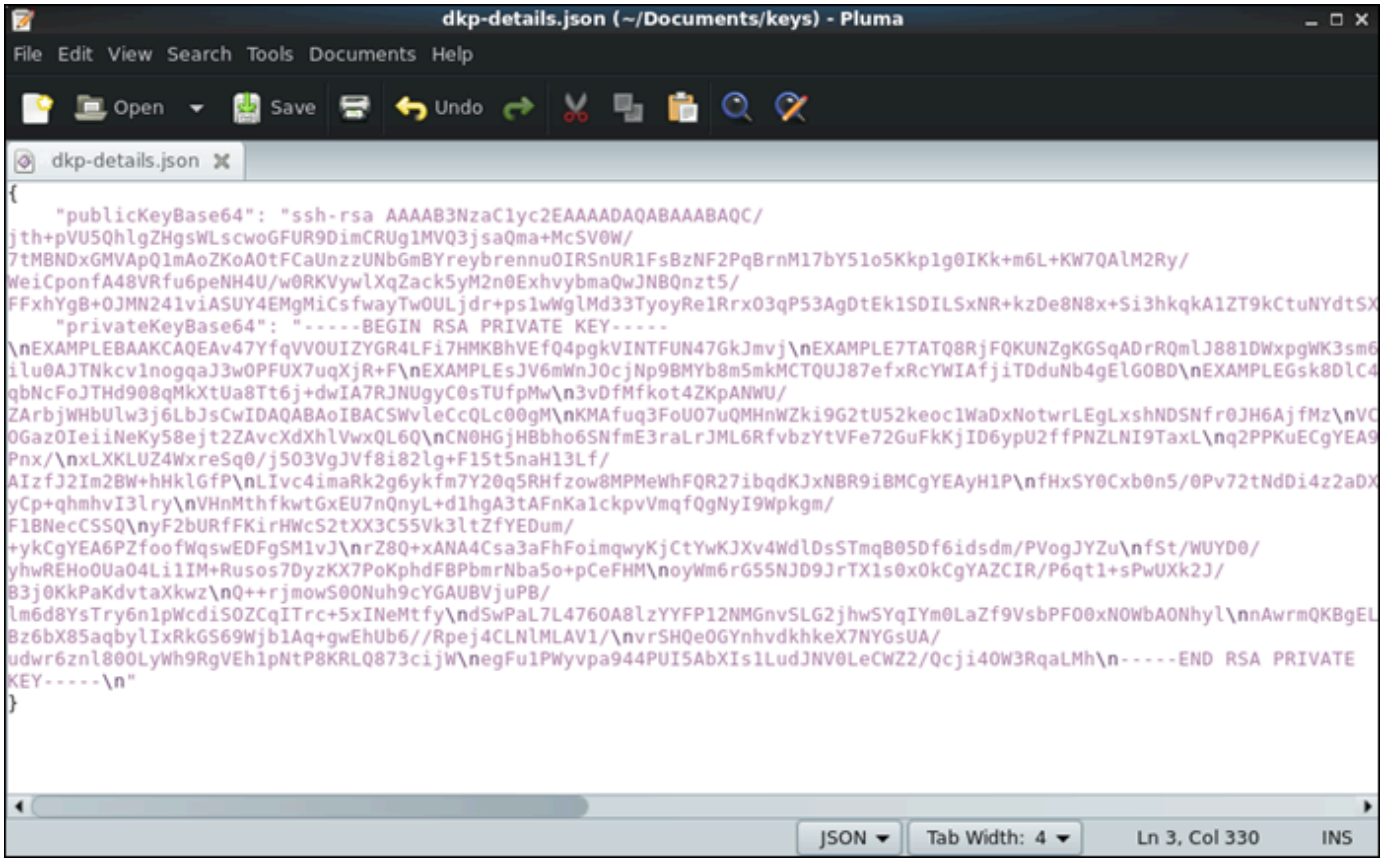
1. Öffnen Sie ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um das Lightsail DKP für eine bestimmte AWS Region abzurufen. Dieser Befehl speichert die Informationen in einer `dkp-details.json`-Datei. Ersetzen Sie den Befehl *`region-code`* durch den Code der AWS Region, in der der virtuelle Computer erstellt wurde, z. B. `us-east-2`

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

Beispiel

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

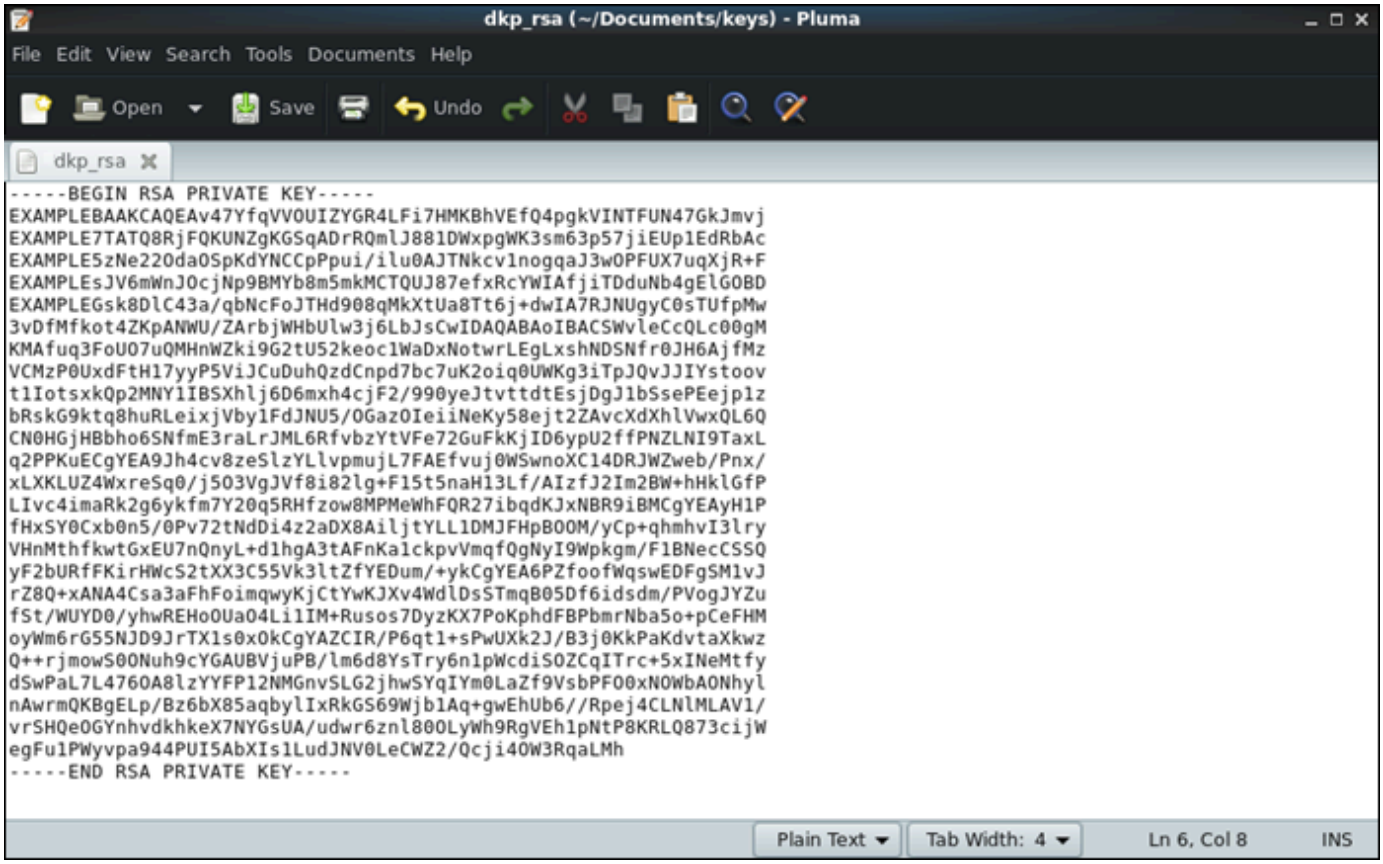
Es erfolgt keine Antwort auf den Befehl. Sie können überprüfen, ob der Befehl erfolgreich war, indem Sie die `dkp-details.json` Datei öffnen und prüfen, ob die DKP Lightsail-Informationen gespeichert wurden. Der Inhalt der `dkp-details.json`-Datei sollte wie im folgenden Beispiel aussehen. Der Befehl ist fehlgeschlagen, wenn die Datei leer ist.



3. Geben Sie den folgenden Befehl ein, um die Informationen zum privaten Schlüssel aus der `dkp-details.json`-Datei zu extrahieren und zu einer neuen privaten Schlüsseldatei (`dkp_rsa`) hinzuzufügen.

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

Es erfolgt keine Antwort auf den Befehl. Sie können überprüfen, ob der Befehl erfolgreich war, indem Sie die `dkp_rsa`-Dateien öffnen und prüfen, ob sie Informationen enthalten. Der Inhalt der `dkp_rsa`-Datei sollte wie im folgenden Beispiel aussehen. Der Befehl ist fehlgeschlagen, wenn die Datei leer ist.



4. Um für die `dkp_rsa`-Datei Berechtigungen festzulegen, geben Sie die folgenden Befehle ein:

```
chmod 600 dkp_rsa
```

Sie verfügen jetzt über den erforderlichen privaten Schlüssel, um eine SSH SCP Oder-Verbindung zu Ihrem virtuellen Computer herzustellen. Fahren Sie mit dem nächsten Abschnitt fort, um weitere Schritte zu erfahren.

Fortfahren mit dem nächsten Schritt

Nachdem Sie die Schlüsselpaare für Ihren virtuellen Computer erhalten haben, können Sie die folgenden zusätzlichen Schritte ausführen:

- Connect zu Ihrem virtuellen Computer herSSH, um ihn über die Befehlszeile zu verwalten. Weitere Informationen finden Sie unter Stellen Sie mithilfe von Secure Shell eine Connect zu einem virtuellen Lightsail for Research-Computer her.
- Connect zu Ihrem virtuellen Computer herSCP, um Dateien sicher zu übertragen. Weitere Informationen finden Sie unter Dateien mithilfe von Secure Copy auf virtuelle Lightsail for Research-Computer übertragen.

Stellen Sie mithilfe von Secure Shell eine Connect zu einem virtuellen Lightsail for Research-Computer her

Sie können mit dem Secure Shell Protocol (SSH) eine Verbindung zu einem virtuellen Computer in Amazon Lightsail for Research herstellen. Sie können SSH damit Ihren virtuellen Computer remote verwalten, sodass Sie sich über das Internet bei Ihrem Computer anmelden und Befehle ausführen können.

> **Note**
>
> Mit dem browserbasierten NICE DCV Client können Sie auch eine Verbindung mit dem Remote-Display-Protokoll zu Ihrem virtuellen Computer herstellen. NICEDCVist in der Lightsail for Research-Konsole verfügbar. Weitere Informationen finden Sie unter Greifen Sie auf das Betriebssystem Ihres virtuellen Lightsail for Research-Computers zu.

Themen

Erfüllen der Voraussetzungen

Sorgen Sie dafür, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie beginnen.

- Erstellen Sie einen virtuellen Computer in Lightsail for Research. Weitere Informationen finden Sie unter Erstellen Sie einen virtuellen Lightsail for Research-Computer.

- Stellen Sie sicher, dass der virtuelle Computer, mit dem Sie sich verbinden möchten, in Betrieb ist. Notieren Sie sich auch den Namen des virtuellen Computers und die AWS Region, in der er erstellt wurde. Sie benötigen diese Informationen später in diesem Prozess. Weitere Informationen finden Sie unter Details zum virtuellen Computer von Lightsail for Research anzeigen.
- Stellen Sie sicher, dass Port 22 auf dem virtuellen Computer geöffnet ist, mit dem Sie sich verbinden möchten. Das ist der Standardport, für den verwendet wirdSSH. Er ist standardmäßig geöffnet. Wenn Sie ihn jedoch geschlossen haben, müssen Sie ihn wieder öffnen, bevor Sie fortfahren können. Weitere Informationen finden Sie unter Firewall-Ports für virtuelle Lightsail for Research-Computer verwalten.
- Holen Sie sich das Lightsail-Standardschlüsselpaar (DKP) für Ihren virtuellen Computer. Weitere Informationen finden Sie unter Erhalten eines Schlüsselpaars für einen virtuellen Computer.

> **Tip**
>
> Informationen dazu, wie Sie damit eine Verbindung AWS CloudShell zu Ihrem virtuellen Computer herstellen möchten, finden Sie Stellen Sie eine Connect zu einem virtuellen Computer her mit AWS CloudShell im nächsten Abschnitt. Weitere Informationen finden Sie unter Was ist AWS CloudShell. Fahren Sie andernfalls mit der nächsten Voraussetzung fort.

- Laden Sie das AWS Command Line Interface (AWS CLI) herunter und installieren Sie es. Weitere Informationen finden Sie unter Installieren oder Aktualisieren auf die neueste Version von AWS CLI im AWS Command Line Interface -Benutzerhandbuch für Version 2.
- Konfigurieren Sie die AWS CLI , um auf Ihre zuzugreifen AWS-Konto. Weitere Informationen finden Sie unter Konfigurationsgrundlagen im AWS Command Line Interface -Benutzerhandbuch für Version 2.
- Laden Sie jq herunter und installieren Sie es. Es ist ein leichter und flexibler JSON Befehlszeilenprozessor, der in den folgenden Verfahren zum Extrahieren von Schlüsselpaardetails verwendet wird. Weitere Informationen zum Herunterladen und Installieren von jq finden Sie unter Download jq auf der jq-Website.

Stellen Sie eine Connect zu einem virtuellen Computer her mit SSH

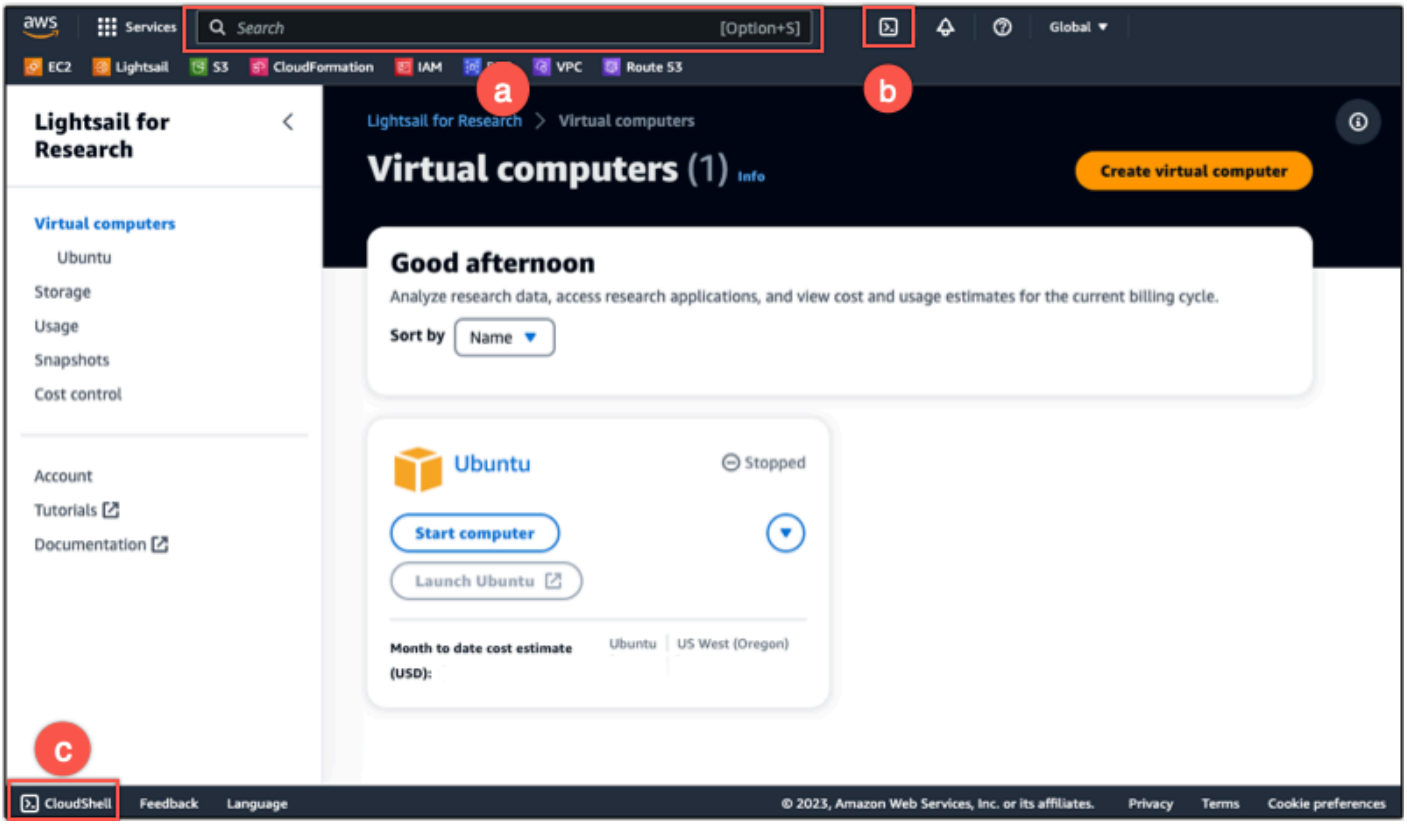
Führen Sie eines der folgenden Verfahren aus, um eine SSH Verbindung zu Ihrem virtuellen Computer in Lightsail for Research herzustellen.

Stellen Sie eine Connect zu einem virtuellen Computer her mit AWS CloudShell

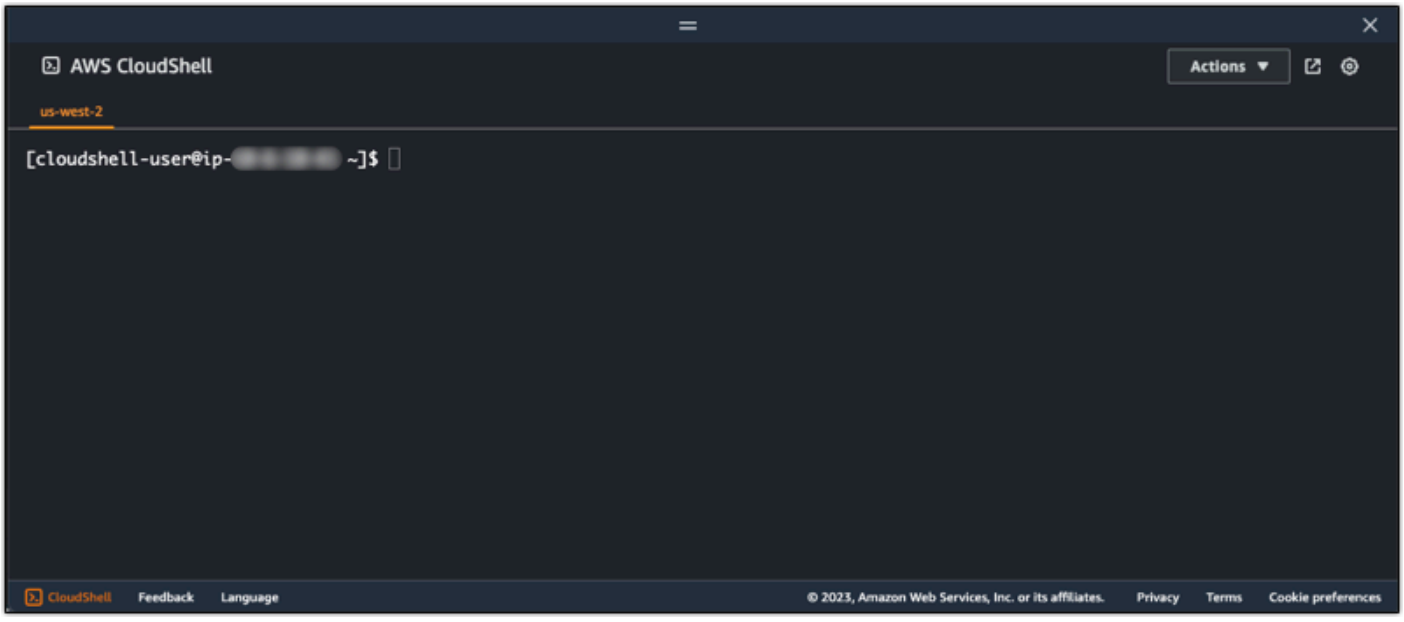
Dieses Verfahren gilt, wenn Sie eine minimale Konfiguration für die Verbindung mit Ihrem virtuellen Computer bevorzugen. AWS CloudShell verwendet eine browserbasierte, vorab authentifizierte Shell, die Sie direkt von der aus starten können. AWS Management Console Sie können AWS CLI Befehle mit Ihrer bevorzugten Shell wie Bash oder Z-Shell ausführen. PowerShell Sie können dies tun, ohne Befehlszeilentools herunterladen oder installieren zu müssen. Weitere Informationen finden Sie unter Erste Schritte in AWS CloudShell im AWS CloudShell -Benutzerhandbuch.

> **Important**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie das Lightsail-Standardschlüsselpaar (DKP) für den virtuellen Computer erhalten, mit dem Sie eine Verbindung herstellen. Weitere Informationen finden Sie unter Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer.

1. Starten Sie von der Lightsail for Research-Konsole aus, CloudShell indem Sie eine der folgenden Optionen wählen:
   a. Geben Sie in das Suchfeld "CloudShell" ein und wählen Sie dann. CloudShell
   b. Wählen Sie in der Navigationsleiste das CloudShellSymbol aus.
   c. Wählen Sie in CloudShellder Konsolen-Symbolleiste unten links in der Konsole.



Wenn die Eingabeaufforderung angezeigt wird, ist die Shell für die Interaktion bereit.



2. Wählen Sie eine vorinstallierte Shell, mit der Sie arbeiten möchten. Um die Standard-Shell zu ändern, geben Sie an der Befehlszeile einen der folgenden Programmnamen ein. Bashist die Standard-Shell, die beim Starten ausgeführt wird AWS CloudShell.

Bash

```
bash
```

Wenn Sie zu wechselnBash, wird das Symbol in der Befehlszeile auf aktualisiert$.

PowerShell

```
pwsh
```

Wenn Sie zu wechseln PowerShell, wird das Symbol in der Befehlszeile auf aktualisiertPS>.

Z shell

```
zsh
```

Wenn Sie zu wechselnZ shell, wird das Symbol in der Befehlszeile auf aktualisiert%.

3. Informationen zum Herstellen einer Verbindung mit einem virtuellen Computer vom CloudShell Terminalfenster aus finden Sie unterStellen Sie mithilfe SSH eines lokalen Linux-, Unix- oder macOS-Computers eine Connect zu einem virtuellen Computer her.

Informationen zur vorinstallierten Software in der CloudShell Umgebung finden Sie im AWS CloudShell Benutzerhandbuch unter AWS CloudShell Computerumgebung.

Stellen Sie mithilfe eines lokalen Windows-Computers eine Connect SSH zu einem virtuellen Computer her

Dieses Verfahren gilt, wenn Ihr lokaler Computer ein Windows-Betriebssystem verwendet. Dieses Verfahren verwendet den `get-instance` AWS CLI Befehl, um den Benutzernamen und die öffentliche IP-Adresse der Instanz abzurufen, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter get-instance in der AWS CLI -Befehlsreferenz.

> **Important**
>
> Stellen Sie sicher, dass Sie das Lightsail-Standardschlüsselpaar (DKP) für den virtuellen Computer erhalten, zu dem Sie eine Verbindung herstellen möchten, bevor Sie dieses Verfahren starten. Weitere Informationen finden Sie unter Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer. Diese Prozedur gibt den privaten Schlüssel der Lightsail DKP in eine `dkp_rsa` Datei aus, die in einem der folgenden Befehle verwendet wird.

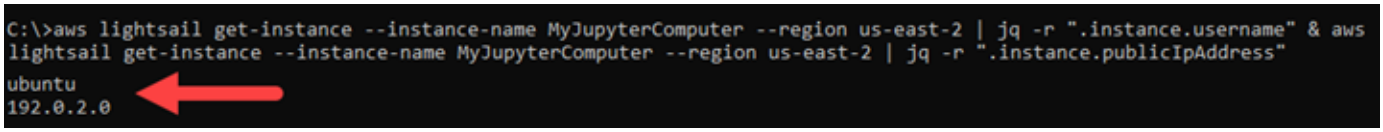
1. Öffnen Sie ein Befehlszeilenfenster.
2. Geben Sie den folgenden Befehl ein, um die öffentliche IP-Adresse und den Benutzernamen Ihres virtuellen Computers anzuzeigen. Ersetzen Sie den Befehl *region-code* durch den Code des Computers, AWS-Region in dem der virtuelle Computer erstellt wurde, z. B. `us-east-2` Ersetzen Sie *computer-name* durch den Namen des virtuellen Computers, mit dem Sie sich verbinden möchten.

```
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"
```

Beispiel

```
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"
```

In der Antwort werden der Benutzername und die öffentliche IP-Adresse des virtuellen Computers angezeigt, wie im folgenden Beispiel gezeigt. Notieren Sie sich diese Werte, da Sie sie im nächsten Schritt dieses Verfahrens benötigen.



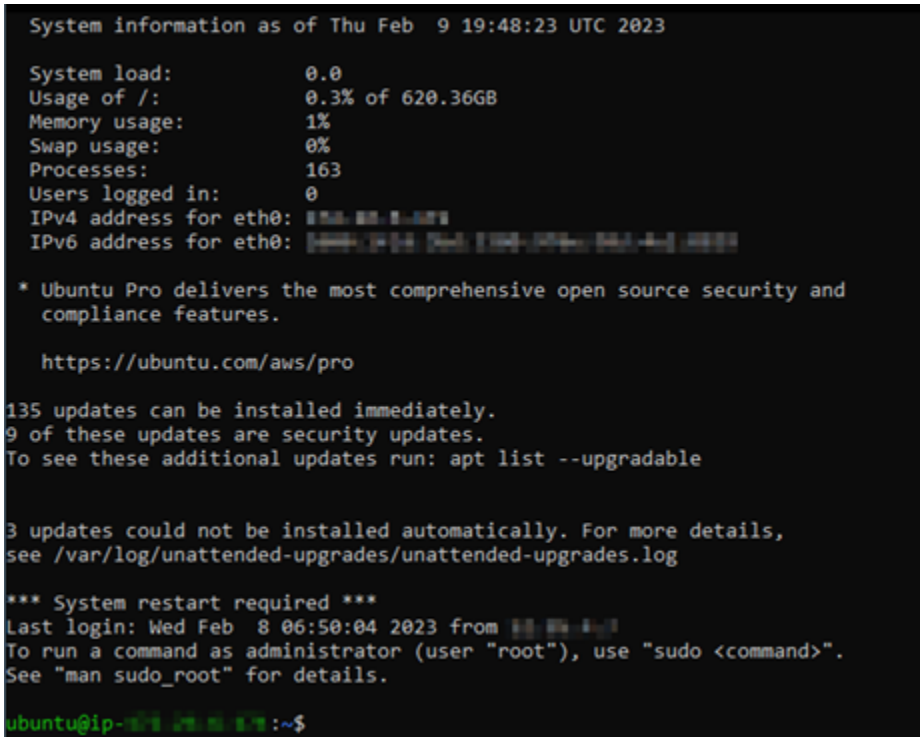
3. Geben Sie den folgenden Befehl ein, um eine SSH Verbindung mit Ihrem virtuellen Computer herzustellen. Ersetzen Sie den Befehl *user-name* durch den Anmeldenamen und *public-ip-address* durch die öffentliche IP-Adresse Ihres virtuellen Computers.

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

Beispiel

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

Sie sollten eine Antwort ähnlich dem folgenden Beispiel sehen, das eine SSH Verbindung zeigt, die mit einem virtuellen Ubuntu-Computer in Lightsail for Research hergestellt wurde.



Nachdem Sie nun erfolgreich eine SSH Verbindung zu Ihrem virtuellen Computer hergestellt haben, fahren Sie mit dem nächsten Abschnitt fort, in dem weitere Schritte beschrieben werden.

Stellen Sie mithilfe SSH eines lokalen Linux-, Unix- oder macOS-Computers eine Connect zu einem virtuellen Computer her

Dieses Verfahren gilt, wenn Ihr lokaler Computer ein Linux-, Unix- oder MacOS-Betriebssystem verwendet. Dieses Verfahren verwendet den `get-instance` AWS CLI Befehl, um den Benutzernamen und die öffentliche IP-Adresse der Instanz abzurufen, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter get-instance in der AWS CLI - Befehlsreferenz.

> **Important**
>
> Stellen Sie sicher, dass Sie das Lightsail-Standardschlüsselpaar (DKP) für den virtuellen Computer erhalten, zu dem Sie eine Verbindung herstellen möchten, bevor Sie dieses Verfahren starten. Weitere Informationen finden Sie unter Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer. Diese Prozedur gibt den privaten Schlüssel der Lightsail DKP in eine `dkp_rsa` Datei aus, die in einem der folgenden Befehle verwendet wird.

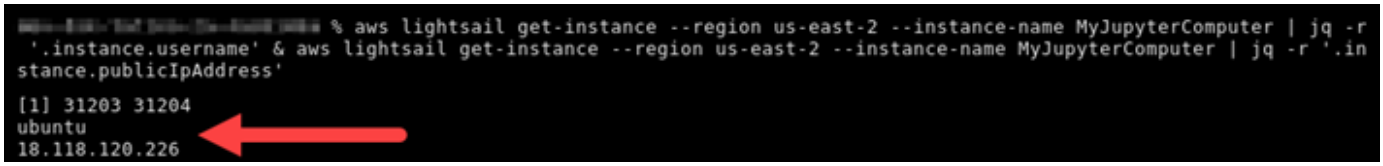
1. Öffnen Sie ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um die öffentliche IP-Adresse und den Benutzernamen Ihres virtuellen Computers anzuzeigen. Ersetzen Sie den Befehl *region-code* durch den Code der AWS Region, in der der virtuelle Computer erstellt wurde, z. B. `us-east-2` Ersetzen Sie *computer-name* durch den Namen des virtuellen Computers, mit dem Sie sich verbinden möchten.

```
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'
```

Beispiel

```
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'
```

In der Antwort werden der Benutzername und die öffentliche IP-Adresse des virtuellen Computers angezeigt, wie im folgenden Beispiel gezeigt. Notieren Sie sich diese Werte, da Sie sie im nächsten Schritt dieses Verfahrens benötigen.



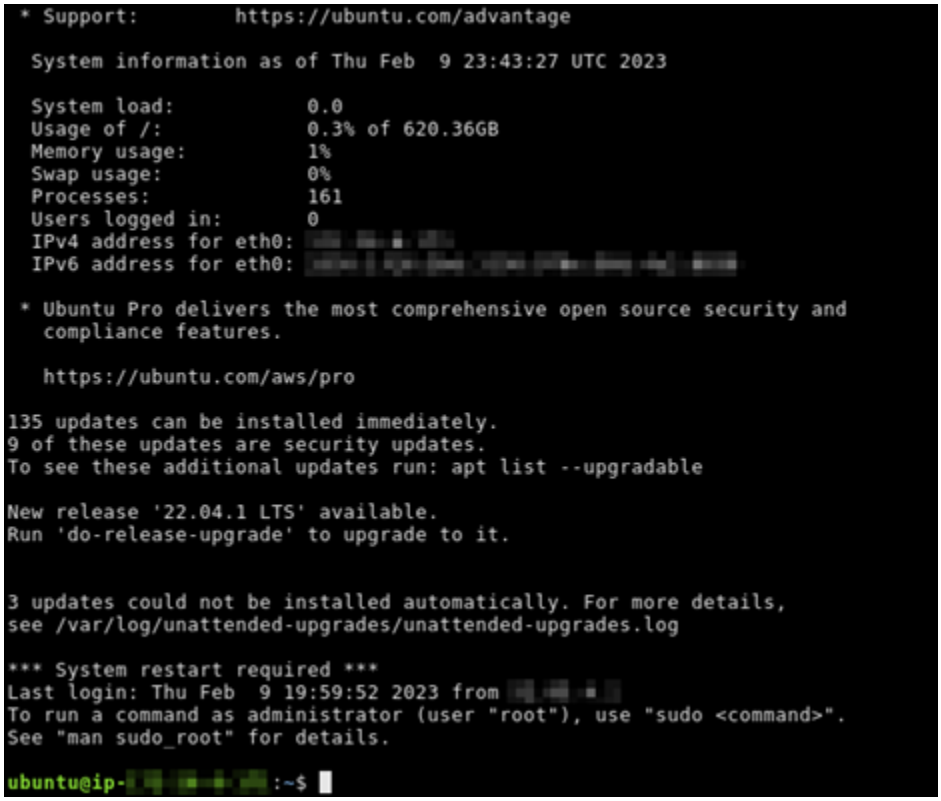
3. Geben Sie den folgenden Befehl ein, um eine SSH Verbindung mit Ihrem virtuellen Computer herzustellen. Ersetzen Sie den Befehl *user-name* durch den Anmeldenamen und *public-ip-address* durch die öffentliche IP-Adresse Ihres virtuellen Computers.

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

Beispiel

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

Sie sollten eine Antwort ähnlich dem folgenden Beispiel sehen, das eine SSH Verbindung zeigt, die mit einem virtuellen Ubuntu-Computer in Lightsail for Research hergestellt wurde.



Nachdem Sie nun erfolgreich eine SSH Verbindung zu Ihrem virtuellen Computer hergestellt haben, fahren Sie mit dem nächsten Abschnitt fort, in dem weitere Schritte beschrieben werden.

Fortfahren mit dem nächsten Schritt

Nachdem Sie erfolgreich eine SSH Verbindung zu Ihrem virtuellen Computer hergestellt haben, können Sie die folgenden zusätzlichen nächsten Schritte ausführen:

- Connect zu Ihrem virtuellen Computer herSCP, um Dateien sicher zu übertragen. Weitere Informationen finden Sie unter Dateien mithilfe von Secure Copy auf virtuelle Lightsail for Research-Computer übertragen.

Dateien mithilfe von Secure Copy auf virtuelle Lightsail for Research-Computer übertragen

Sie können Dateien mit Secure Copy (SCP) von Ihrem lokalen Computer auf einen virtuellen Computer in Amazon Lightsail for Research übertragen. Mit diesem Verfahren können Sie mehrere Dateien oder ganze Verzeichnisse gleichzeitig übertragen.

> **Note**
>
> Sie können mit dem browserbasierten NICE DCV Client, der in der Lightsail for Research-Konsole verfügbar ist, auch eine Remote Display Protocol-Verbindung zu Ihrem virtuellen Computer herstellen. Mit dem NICE DCV Client können Sie schnell einzelne Dateien übertragen. Weitere Informationen finden Sie unter Greifen Sie auf das Betriebssystem Ihres virtuellen Lightsail for Research-Computers zu.

Themen

Erfüllen der Voraussetzungen

Sorgen Sie dafür, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie beginnen.

- Erstellen Sie einen virtuellen Computer in Lightsail for Research. Weitere Informationen finden Sie unter Erstellen Sie einen virtuellen Lightsail for Research-Computer.
- Stellen Sie sicher, dass der virtuelle Computer, mit dem Sie sich verbinden möchten, in Betrieb ist. Notieren Sie sich auch den Namen des virtuellen Computers und die AWS -Region, in der er erstellt wurde. Diese Informationen werden später benötigt. Weitere Informationen finden Sie unter Details zum virtuellen Computer von Lightsail for Research anzeigen.
- Laden Sie das AWS Command Line Interface ()AWS CLI herunter und installieren Sie es. Weitere Informationen finden Sie unter Installieren oder Aktualisieren auf die neueste Version von AWS CLI im AWS Command Line Interface -Benutzerhandbuch für Version 2.
- Konfigurieren Sie die AWS CLI , um auf Ihre zuzugreifen AWS-Konto. Weitere Informationen finden Sie unter Konfigurationsgrundlagen im AWS Command Line Interface -Benutzerhandbuch für Version 2.
- Laden Sie jq herunter und installieren Sie es. Es ist ein leichter und flexibler JSON Befehlszeilenprozessor, der in den folgenden Verfahren zum Extrahieren von Schlüsselpaardetails verwendet wird. Weitere Informationen zum Herunterladen und Installieren von jq finden Sie unter Download jq auf der jq-Website.
- Stellen Sie sicher, dass Port 22 auf dem virtuellen Computer geöffnet ist, mit dem Sie sich verbinden möchten. Dies ist der Standardport, für den verwendet wirdSSH. Er ist standardmäßig

geöffnet. Wenn Sie ihn jedoch geschlossen haben, müssen Sie ihn wieder öffnen, bevor Sie fortfahren können. Weitere Informationen finden Sie unter Firewall-Ports für virtuelle Lightsail for Research-Computer verwalten.

- Holen Sie sich das Lightsail-Standardschlüsselpaar (DKP) für Ihren virtuellen Computer. Weitere Informationen finden Sie unter Erstellen Sie einen virtuellen Lightsail for Research-Computer.

Stellen Sie eine Connect zu einem virtuellen Computer her mit SCP

Führen Sie eines der folgenden Verfahren aus, um mit Lightsail for Research eine Verbindung zu Ihrem virtuellen Computer herzustellen. SCP

Stellen Sie mithilfe eines lokalen Windows-Computers eine Connect SCP zu einem virtuellen Computer her

Dieses Verfahren ist für Sie relevant, wenn Ihr lokaler Computer ein Windows-Betriebssystem verwendet. Dieses Verfahren verwendet den `get-instance` AWS CLI Befehl, um den Benutzernamen und die öffentliche IP-Adresse der Instanz abzurufen, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter get-instance in der AWS CLI - Befehlsreferenz.

> **Important**
>
> Stellen Sie sicher, dass Sie das Lightsail-Standardschlüsselpaar (DKP) für den virtuellen Computer erhalten, zu dem Sie eine Verbindung herstellen möchten, bevor Sie dieses Verfahren starten. Weitere Informationen finden Sie unter Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer. Diese Prozedur gibt den privaten Schlüssel der Lightsail DKP in eine `dkp_rsa` Datei aus, die in einem der folgenden Befehle verwendet wird.

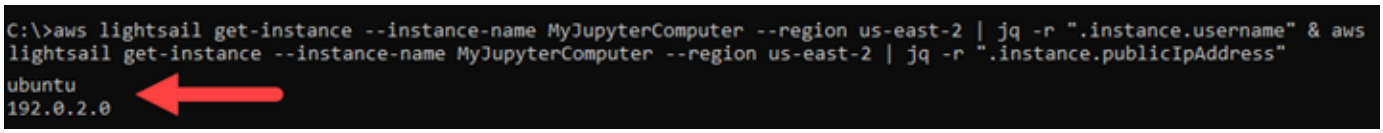
1. Öffnen Sie ein Befehlszeilenfenster.
2. Geben Sie den folgenden Befehl ein, um die öffentliche IP-Adresse und den Benutzernamen Ihres virtuellen Computers anzuzeigen. Ersetzen Sie den Befehl *`region-code`* durch den Code der AWS Region, in der der virtuelle Computer erstellt wurde, z. B. `us-east-2` Ersetzen Sie *`computer-name`* durch den Namen des virtuellen Computers, mit dem Sie sich verbinden möchten.

```
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"
```

Beispiel

```
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"
```

In der Antwort werden der Benutzername und die öffentliche IP-Adresse des virtuellen Computers angezeigt, wie im folgenden Beispiel gezeigt. Notieren Sie sich diese Werte, da Sie sie im nächsten Schritt dieses Verfahrens benötigen.



3. Geben Sie den folgenden Befehl ein, um eine SCP Verbindung zu Ihrem virtuellen Computer herzustellen und Dateien darauf zu übertragen.

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

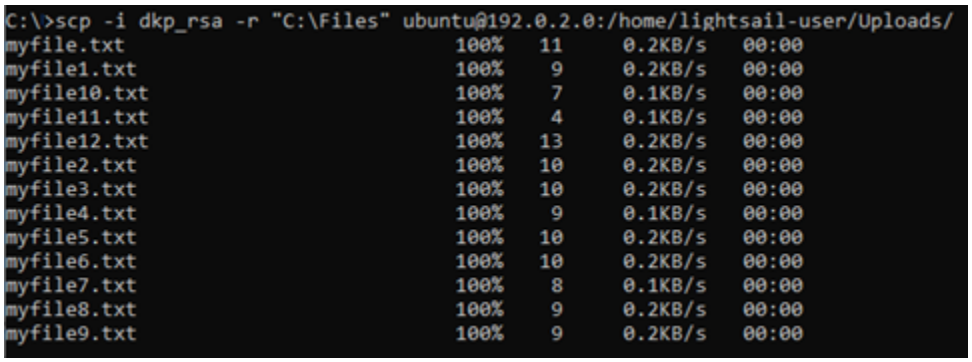
Ersetzen Sie im Befehl Folgendes:

- *source-folder* mit dem Ordner auf Ihrem lokalen Computer, der die Dateien enthält, die Sie übertragen möchten.
- *user-name* mit dem Benutzernamen aus dem vorherigen Schritt dieses Verfahrens (z. B. `ubuntu`).
- *public-ip-address* mit der öffentlichen IP-Adresse Ihres virtuellen Computers aus dem vorherigen Schritt dieses Verfahrens.
- *destination-directory* mit dem Pfad zu dem Verzeichnis auf dem virtuellen Computer, in das Sie Ihre Dateien kopieren möchten.

Im folgenden Beispiel werden alle Dateien aus dem Ordner `C:\Files` auf dem lokalen Computer in das Verzeichnis `/home/lightsail-user/Uploads/` auf dem virtuellen Remotecomputer kopiert.

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

Sie sollten eine Antwort ähnlich dem folgenden Beispiel erhalten. Sie zeigt jede Datei, die vom Ursprungsordner in das Zielverzeichnis übertragen wurde. Sie sollten jetzt auf Ihrem virtuellen Computer auf diese Dateien zugreifen können.



Stellen Sie mithilfe SCP eines lokalen Linux-, Unix- oder macOS-Computers eine Connect zu einem virtuellen Computer her

Dieses Verfahren ist für Sie relevant, wenn Ihr lokaler Computer ein Linux-, Unix- oder macOS-Betriebssystem verwendet. Dieses Verfahren verwendet den `get-instance` AWS CLI Befehl, um den Benutzernamen und die öffentliche IP-Adresse der Instanz abzurufen, zu der Sie eine Verbindung herstellen möchten. Weitere Informationen finden Sie unter get-instance in der AWS CLI - Befehlsreferenz.

> **Important**
>
> Stellen Sie sicher, dass Sie das Lightsail-Standardschlüsselpaar (DKP) für den virtuellen Computer erhalten, zu dem Sie eine Verbindung herstellen möchten, bevor Sie dieses Verfahren starten. Weitere Informationen finden Sie unter Holen Sie sich ein key pair für einen virtuellen Lightsail for Research-Computer. Diese Prozedur gibt den privaten Schlüssel der Lightsail DKP in eine `dkp_rsa` Datei aus, die in einem der folgenden Befehle verwendet wird.

1. Öffnen Sie ein Terminal-Fenster.
2. Geben Sie den folgenden Befehl ein, um die öffentliche IP-Adresse und den Benutzernamen Ihres virtuellen Computers anzuzeigen. Ersetzen Sie den Befehl *`region-code`* durch den

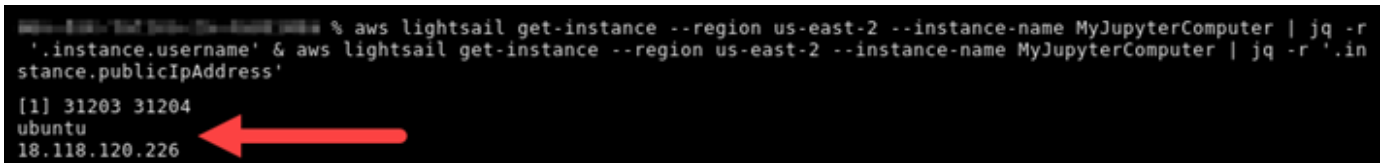
Code der AWS Region, in der der virtuelle Computer erstellt wurde, z. B. `us-east-2` Ersetzen Sie *computer-name* durch den Namen des virtuellen Computers, mit dem Sie sich verbinden möchten.

```
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'
```

Beispiel

```
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'
```

In der Antwort werden der Benutzername und die öffentliche IP-Adresse des virtuellen Computers angezeigt, wie im folgenden Beispiel gezeigt. Notieren Sie sich diese Werte, da Sie sie im nächsten Schritt dieses Verfahrens benötigen.



3. Geben Sie den folgenden Befehl ein, um eine SCP Verbindung zu Ihrem virtuellen Computer herzustellen und Dateien darauf zu übertragen.

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

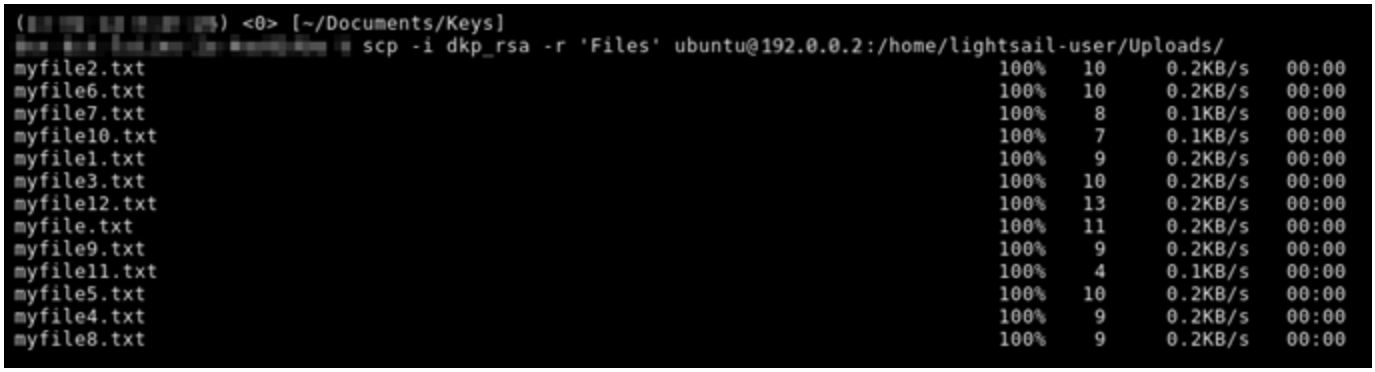
Ersetzen Sie im Befehl Folgendes:

- *source-folder* mit dem Ordner auf Ihrem lokalen Computer, der die Dateien enthält, die Sie übertragen möchten.
- *user-name* mit dem Benutzernamen aus dem vorherigen Schritt dieses Verfahrens (z. B. `ubuntu`).
- *public-ip-address* mit der öffentlichen IP-Adresse Ihres virtuellen Computers aus dem vorherigen Schritt dieses Verfahrens.
- *destination-directory* mit dem Pfad zu dem Verzeichnis auf dem virtuellen Computer, in das Sie Ihre Dateien kopieren möchten.

Im folgenden Beispiel werden alle Dateien aus dem Ordner `C:\Files` auf dem lokalen Computer in das Verzeichnis `/home/lightsail-user/Uploads/` auf dem virtuellen Remotecomputer kopiert.

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

Sie sollten eine Antwort ähnlich dem folgenden Beispiel erhalten. Sie zeigt jede Datei, die vom Ursprungsordner in das Zielverzeichnis übertragen wurde. Sie sollten jetzt auf Ihrem virtuellen Computer auf diese Dateien zugreifen können.



Löschen Sie einen virtuellen Lightsail for Research-Computer

Gehen Sie wie folgt vor, um Ihren virtuellen Lightsail for Research-Computer zu löschen, wenn Sie ihn nicht mehr benötigen. Sobald der virtuelle Computer gelöscht wurde, fallen keine weiteren Kosten für ihn mehr an. Ressourcen, die an den gelöschten Computer angehängt sind, wie statische IPs und Snapshots, verursachen jedoch weiterhin Kosten, bis Sie sie löschen.

> **Important**
>
> Das Löschen eines virtuellen Computers ist permanent. Der Computer kann danach nicht wiederhergestellt werden. Wenn Sie die Daten später benötigen, erstellen Sie einen Snapshot Ihres virtuellen Computers, bevor Sie ihn löschen. Weitere Informationen finden Sie unter Erstellen eines Snapshots.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im linken Navigationsbereich Virtuelle Computer aus.

3. Wählen Sie den zu löschenden virtuellen Computer aus.
4. Wählen Sie Aktionen und anschließend Virtuellen Computer löschen.
5. Geben Sie confirm in den Textblock ein. Wählen Sie dann Virtuellen Computer löschen.

Daten sichern und speichern mit Lightsail for Research-Volumen

Amazon Lightsail for Research stellt Speichervolumes (Festplatten) auf Blockebene bereit, die Sie an einen laufenden virtuellen Lightsail for Research-Computer anhängen können. Sie können einen Datenträger als ein primäres Speichergerät für Daten verwenden, die häufige Aktualisierungen mit hoher Granularität erfordern. Festplatten sind beispielsweise die empfohlene Speicheroption, wenn Sie eine Datenbank auf einem virtuellen Lightsail for Research-Computer ausführen.

Ein Datenträger verhält sich wie ein unformatiertes externes Blockgerät, das Sie einem einzelnen virtuellen Computer anfügen können. Das Volume bleibt unabhängig von der Betriebsdauer eines Computers erhalten. Nachdem Sie einem Computer einen Datenträger angefügt haben, können Sie sie wie eine echte Festplatte verwenden.

Sie können mehrere Datenträger an einen Computer anschließen. Sie können einen Datenträger auch von einem Computer trennen und an einen anderen Computer anschließen.

Sie können eine Sicherungskopie Ihrer Daten anfertigen, indem Sie einen Snapshot des Datenträgers erstellen. Aus einem Snapshot können Sie einen neuen Datenträger erstellen und an einen anderen Computer anfügen.

Themen

Erstellen Sie eine Speicherfestplatte in der Lightsail for Research-Konsole

Gehen Sie wie folgt vor, um eine Festplatte für Ihren virtuellen Lightsail for Research-Computer zu erstellen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.

2. Wählen Sie im Navigationsbereich die Option Speicher aus.
3. Klicken Sie auf Datenträger erstellen.
4. Geben Sie einen Namen für Ihren Datenträger ein. Gültige Zeichen sind alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche.

   Datenträger-Namen müssen außerdem die folgenden Anforderungen erfüllen:

   - Seien Sie AWS-Region in Ihrem Lightsail for Research-Konto in jedem Bereich einzigartig.
   - Sie müssen 2–255 Zeichen enthalten.
   - Sie müssen mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
5. Wählen Sie einen AWS-Region für Ihre Festplatte.

   Der Datenträger muss sich in derselben Region befinden wie der virtuelle Computer, an den Sie sie anfügen.
6. Wählen Sie die Datenträgergröße in GB.
7. Weitere Informationen zum Anfügen von Datenträgern an Ihren virtuellen Computer finden Sie im Abschnitt Anfügen eines Datenträgers an einen virtuellen Computer.

Details zur Speicherfestplatte in der Lightsail for Research-Konsole anzeigen

Gehen Sie wie folgt vor, um die Festplatten in Ihrem Lightsail for Research-Konto und deren Details anzuzeigen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Speicher aus.

   Die Speicherseite bietet einen umfassenden Überblick über die Festplatten in Ihrem Lightsail for Research-Konto.

   Es werden die folgenden Informationen angezeigt:

   - Name – Der Name des Datenträgers.
   - Größe – Die Größe des Datenträgers (in GB).
   - AWS-Region – Die AWS-Region , in der Ihr Datenträger erstellt wurde.
   - Angeschlossen an — Der Lightsail-Computer, an den Ihre Festplatte angeschlossen ist.

- Erstellungsdatum – Das Datum, an dem der Datenträger erstellt wurde.

Hinzufügen von Speicherplatz zu einem virtuellen Computer in Lightsail for Research

Gehen Sie wie folgt vor, um eine Festplatte an einen virtuellen Computer in Lightsail for Research anzuhängen. Sie können bis zu 15 Datenträger an einen virtuellen Computer anfügen. Wenn Sie mit der Lightsail for Research-Konsole eine Festplatte an Ihren virtuellen Computer anschließen, wird sie automatisch formatiert und vom Dienst bereitgestellt. Dieser Vorgang dauert einige Minuten. Sie sollten sich daher vergewissern, dass die Festplatte den Bereitstellungsstatus Mounted erreicht hat, bevor Sie sie verwenden. Standardmäßig mountet Lightsail for Research Festplatten in das `/home/lightsail-user/<disk-name>` Verzeichnis. Dabei `<disk-name>` handelt es sich um den Namen, den Sie Ihrer Festplatte gegeben haben.

> **Important**
>
> Bevor Sie einen Datenträger an einen virtuellen Computer anschließen können, muss sich der virtuelle Computer im Status Wird ausgeführt befinden. Wenn Sie einen Datenträger an einen virtuellen Computer anschließen, während er sich im Status Angehalten befindet, wird der Datenträger zwar angeschlossen, aber das Mounten schlägt fehl. Wenn der Mountingstatus des Datenträgers Fehlgeschlagen lautet, müssen Sie den Datenträger trennen und ihn dann wieder anschließen, wenn sich der virtuelle Computer im Status Wird ausgeführt befindet.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im linken Navigationsbereich Virtuelle Computer aus.
3. Wählen Sie den Computer aus, an den der Datenträger angeschlossen werden soll.
4. Wählen Sie die Registerkarte Speicher.
5. Wählen Sie Datenträger anfügen.
6. Wählen Sie den Namen des Datenträgers aus, der an den Computer angeschlossen werden soll.
7. Wählen Sie Anfügen aus.

Trennen Sie in Lightsail for Research eine Festplatte von einem virtuellen Computer

Gehen Sie folgendermaßen vor, um einen Datenträger von einem Computer zu trennen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Speicher aus.
3. Suchen Sie den Datenträger, der getrennt werden soll. Wählen Sie in der Spalte Angefügt an den Namen des Computers aus, an den der Datenträger angefügt ist.
4. Wählen Sie Anhalten, um den Computer anzuhalten. Sie müssen den Computer anhalten, bevor Sie den Datenträger trennen können.
5. Bestätigen Sie, dass Sie den Computer anhalten möchten, und wählen Sie dann Computer stoppen.
6. Wählen Sie die Registerkarte Speicher.
7. Wählen Sie den Datenträger aus, die Sie trennen möchten, und klicken Sie dann auf Trennen.
8. Bestätigen Sie, dass Sie den Datenträger vom Computer trennen möchten, und wählen Sie dann Trennen.

Löschen Sie ungenutzte Speicherplatten in Lightsail for Research

Gehen Sie folgendermaßen vor, um einen Datenträger zu löschen, wenn Sie ihn nicht mehr benötigen. Sobald der Datenträger gelöscht wurde, fallen keine weiteren Kosten mehr dafür an.

Wenn der Datenträger an einen Computer angeschlossen ist, müssen Sie ihn zuerst trennen, bevor Sie ihn löschen können. Weitere Informationen finden Sie unter Trennen Sie in Lightsail for Research eine Festplatte von einem virtuellen Computer.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Speicher aus.
3. Suchen Sie den Datenträger, den Sie löschen möchten, und wählen Sie ihn aus.
4. Wählen Sie Datenträger löschen aus.
5. Bestätigen Sie, dass Sie den Datenträger löschen möchten. Wählen Sie dann Löschen aus.

Backup virtuelle Computer und Festplatten mit Lightsail for Research-Snapshots

Schnappschüsse sind eine point-in-time Kopie Ihrer Daten. Sie können Snapshots Ihrer virtuellen Computer und Speicherfestplatten mit Amazon Lightsail for Research erstellen und diese als Basisdaten für die Erstellung neuer Computer oder für Datensicherungen verwenden.

Ein Snapshot enthält alle Daten, die erforderlich sind, um Ihre virtuellen Computer wiederherzustellen (von dem Zeitpunkt, an dem der Snapshot erstellt wurde). Wenn Sie einen neuen virtuellen Computer anhand eines Snapshots erstellen, ist der Computer zunächst eine identische Kopie des Original-Computers, der für die Erstellung des Snapshots verwendet wurde.

Da Ihre Ressourcen jederzeit ausfallen können, empfehlen wir, regelmäßig Snapshots zu erstellen, um dauerhaften Datenverlust zu vermeiden.

Themen

Erstellen Sie Schnappschüsse von virtuellen Computern oder Festplatten mit Lightsail for Research

Gehen Sie wie folgt vor, um einen Snapshot Ihres virtuellen Computers oder Ihrer Festplatte mit Lightsail for Research zu erstellen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Führen Sie die folgenden Schritte aus:

    - Suchen Sie unter Snapshots virtueller Computer nach dem Namen des Computers, für den Sie einen Snapshot erstellen möchten, und wählen Sie Snapshot erstellen aus.
    - Suchen Sie unter Datenträger-Snapshots nach dem Namen des Datenträgers, für den Sie einen Snapshot erstellen möchten, und wählen Sie Snapshot erstellen aus.

4. Geben Sie einen Namen für den Snapshot ein. Gültige Zeichen sind alphanumerische Zeichen, Zahlen, Punkte, Bindestriche und Unterstriche.

   Datenträger-Snapshots-Namen müssen außerdem die folgenden Anforderungen erfüllen:

   - Seien Sie AWS-Region in Ihrem Lightsail for Research-Konto in jedem Bereich einzigartig.
   - Sie müssen 2–255 Zeichen enthalten.
   - Sie müssen mit einem alphanumerischen Zeichen oder einer Zahl beginnen und enden.
5. Wählen Sie Snapshot erstellen aus.

Virtuelle Computer- und Festplatten-Snapshots in Lightsail for Research anzeigen und verwalten

Gehen Sie wie folgt vor, um Snapshots Ihrer virtuellen Computer und Datenträger anzuzeigen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Snapshots.

   Auf der Seite Snapshots werden virtuelle Computer- und Datenträger-Snapshots angezeigt, die Sie erstellt haben.

   Archivierte Snapshots befinden sich ebenfalls auf dieser Seite. Archivierte Snapshots sind Momentaufnahmen von Ressourcen, die aus Ihrem Konto gelöscht wurden.

Einen virtuellen Computer oder einen virtuellen Datenträger aus einem Snapshot erstellen

Gehen Sie wie folgt vor, um einen neuen virtuellen Computer oder eine Festplatte mit Lightsail for Research aus einem Snapshot zu erstellen.

Wenn Sie einen virtuellen Computer aus einem Snapshot erstellen, verwenden Sie einen Plan, der genauso groß oder größer ist als der Plan, der für den ursprünglichen Computer verwendet wurde. Sie können keinen „kleineren“ Plan als der ursprüngliche virtuelle Computer verwenden.

Wenn Sie einen Datenträger aus einem Snapshot erstellen, wählen Sie eine Datenträgergröße, die größer ist als der ursprüngliche Datenträger. Sie können keinen kleineren Datenträger als das Original verwenden.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Suchen Sie auf der Seite Snapshots nach dem Namen des Computer- oder Datenträger-Snapshots, den Sie zum Erstellen des neuen Computers bzw. des neuen Datenträgers verwenden möchten. Wählen Sie das Drop-down-menü Snapshots, um eine Liste der verfügbaren Snapshots für diese Ressource anzuzeigen.
4. Wählen Sie den Snapshot aus, den Sie zum Erstellen des virtuellen Computers verwenden möchten.
5. Gehen Sie zum Drop-down-Menü Aktionen. Wählen Sie dann Virtuellen Computer erstellen oder Datenträger erstellen.

Löschen Sie einen Snapshot in der Lightsail for Research-Konsole

Führen Sie zum Löschen eines Snapshots die folgenden Schritte aus.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Suchen Sie auf der Seite Snapshots den Namen des Computers oder des Datenträger-Snapshots, den Sie löschen möchten. Wählen Sie das Drop-down-menü Snapshots, um eine Liste der verfügbaren Snapshots für diese Ressource anzuzeigen.
4. Wählen Sie den Snapshot aus, den Sie löschen möchten.
5. Gehen Sie zum Drop-down-Menü Aktionen. Wählen Sie Snapshot löschen aus.
6. Stellen Sie sicher, dass der Snapshot-Name der richtige ist. Wählen Sie Snapshot löschen aus.

Kosten- und Nutzungsschätzungen in Lightsail for Research

Amazon Lightsail for Research bietet Kosten- und Nutzungsschätzungen für Ihre AWS Ressourcen. Sie können diese Schätzungen verwenden, um Ihre Ausgaben zu planen, Möglichkeiten zur Kosteneinsparung zu finden und fundierte Entscheidungen zu treffen, wenn Sie Lightsail for Research verwenden.

Wenn Sie einen virtuellen Computer oder eine virtuelle Festplatte erstellen, werden Kosten- und Nutzungsschätzungen für diese Ressource angezeigt. Eine Kosten- und Nutzungsschätzung wird erfasst, sobald eine Ressource erstellt wurde und sich im Status Verfügbar oder Wird ausgeführt befindet. Die Schätzung wird innerhalb von 15 Minuten nach der Erstellung der Ressource in der AWS Management Console angezeigt. Ressourcen, die gelöscht wurden, sind nicht in einer Schätzung enthalten.

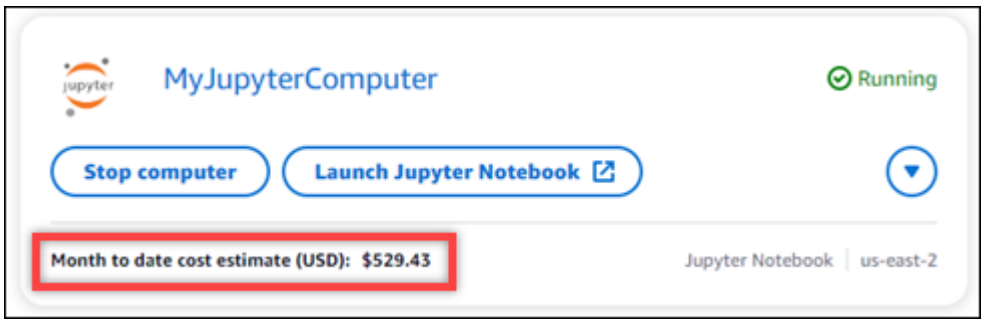
> **Important**
>
> Bei einer Schätzung handelt es sich um geschätzte Kosten, die auf der Nutzung der Ressource basieren. Ihre tatsächlichen Kosten basieren auf der tatsächlichen Nutzung Ihrer Ressourcen und nicht auf der Schätzung, die in der Lightsail for Research-Konsole angezeigt wird. Die tatsächlichen Kosten werden auf Ihrem AWS Billing Kontoauszug ausgewiesen. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Billing Konsole unter https://console.aws.amazon.com/billing/.

Themen

Kosten- und Nutzungsschätzungen für Ihre Ressourcen in Lightsail for Research anzeigen

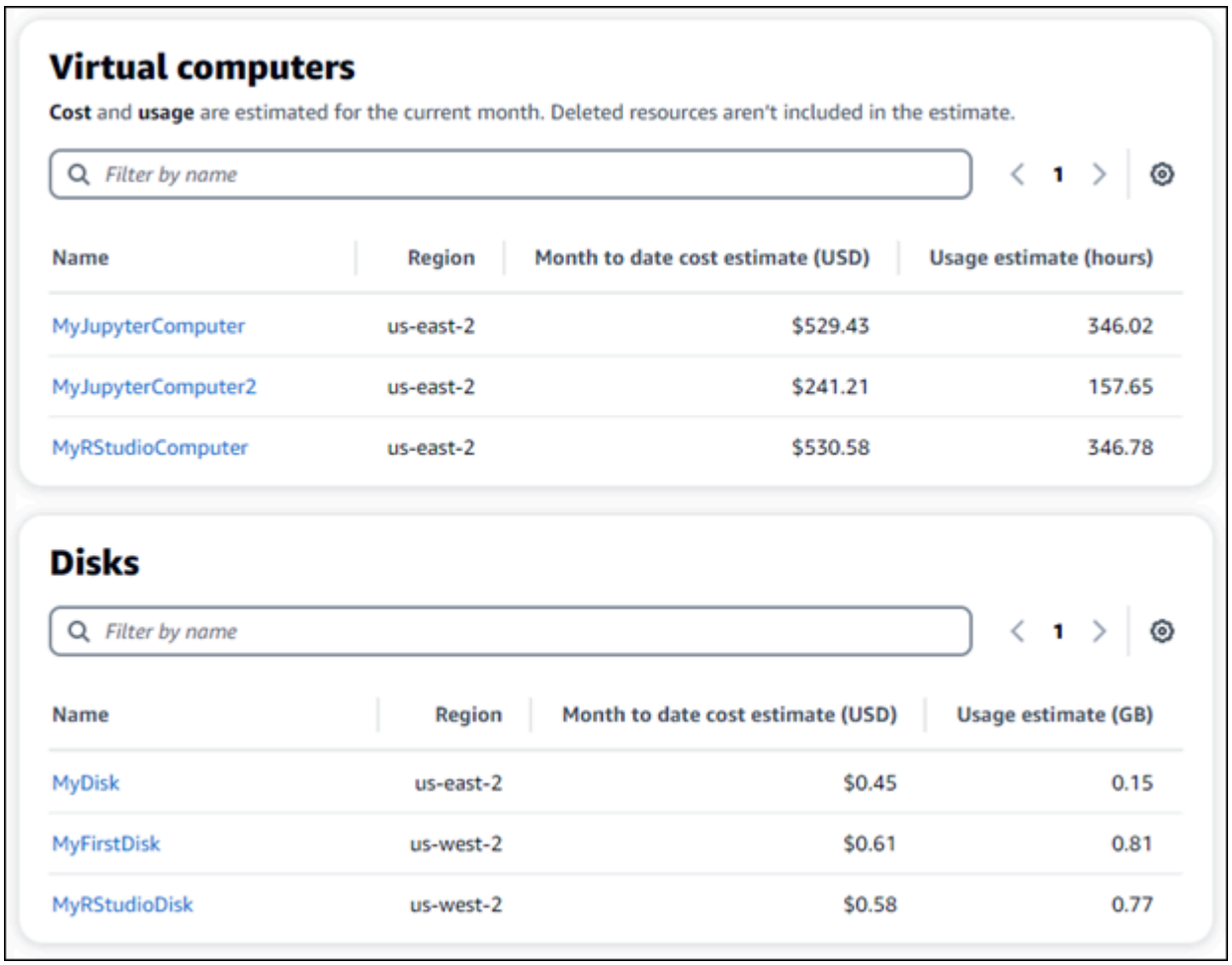
Die Kosten- und Nutzungsschätzungen für Ihre Lightsail for Research-Ressourcen seit Monatsbeginn werden in den folgenden Bereichen der Lightsail for Research-Konsole angezeigt.

1. Wählen Sie im Navigationsbereich der Lightsail for Research-Konsole die Option Virtuelle Computer aus. Der Kostenvoranschlag für Ihre virtuellen Computer seit Monatsbeginn ist unter jedem laufenden virtuellen Computer aufgeführt.



2. Um die CPU Auslastung eines virtuellen Computers anzuzeigen, wählen Sie den Namen des virtuellen Computers und dann die Registerkarte Dashboard aus.

3. Um die Kosten- und Nutzungsschätzungen für alle Ihre Lightsail for Research-Ressourcen seit Monatsbeginn anzuzeigen, wählen Sie im Navigationsbereich Nutzung aus.


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

Regeln zur Kostenkontrolle in Lightsail for Research verwalten

Die Kostenkontrolle verwendet Regeln, die Sie definieren, um die Nutzung und die Kosten Ihrer virtuellen Lightsail for Research-Computer zu verwalten.

Sie können die Regel „Virtuellen Computer im Leerlauf beenden“ erstellen, die einen laufenden Computer stoppt, wenn er in einem bestimmten Zeitraum einen bestimmten Prozentsatz seiner CPU Auslastung erreicht hat. Mit einer Regel kann beispielsweise ein bestimmter Computer automatisch gestoppt werden, wenn seine CPU Auslastung innerhalb von 30 Minuten 5% oder weniger beträgt. Dies bedeutet, dass der Computer inaktiv ist und Lightsail for Research den Computer stoppt. Nach dem Stoppen des virtuellen Computers fallen für Sie nicht mehr die üblichen Stundengebühren an.

Themen

Erstellen Sie Regeln zur Kostenkontrolle für Ihre virtuellen Lightsail for Research-Computer

Gehen Sie wie folgt vor, um eine Regel für Ihren virtuellen Lightsail for Research-Computer zu erstellen.

> **Note**
>
> Die einzige unterstützte Regelaktion ist derzeit das Stoppen eines virtuellen Computers. CPUDie Auslastung ist die einzige Metrik, die derzeit durch Regeln überwacht wird, und der einzige unterstützte Vorgang ist kleiner oder gleich.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Kostenkontrolle aus.
3. Wählen Sie Regel erstellen.
4. Wählen Sie die Ressource aus, auf die die Regel angewendet werden soll.

5. Geben Sie den CPU Nutzungsprozentsatz und den Zeitraum an, in dem die Regel ausgeführt werden soll.

   Sie können beispielsweise 5 Prozent und 30 Minuten angeben. Lightsail for Research stoppt den Computer automatisch, wenn er innerhalb von 30 Minuten weniger als oder gleich 5 Prozent CPU ausgelastet ist.
6. Wählen Sie Regel erstellen aus.
7. Vergewissern Sie sich, dass die Informationen für Ihre neue Regel korrekt sind, und wählen Sie dann Bestätigen.

Löschen Sie die Regeln zur Kostenkontrolle für Ihre virtuellen Lightsail for Research-Computer

Gehen Sie wie folgt vor, um eine Regel für Ihren virtuellen Lightsail for Research-Computer zu löschen.

1. Melden Sie sich bei der Lightsail for Research-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Kostenkontrolle aus.
3. Wählen Sie die zu löschende Regel aus.
4. Wählen Sie Löschen.
5. Überprüfen Sie, ob Sie die Regel löschen möchten, und wählen Sie Löschen.

Organisieren Sie Lightsail for Research-Ressourcen mit Tags

Mit Amazon Lightsail for Research können Sie Ihren Ressourcen Tags zuweisen. Jedes Tag ist ein Label, das aus einem Schlüssel und einem optionalen Wert besteht. Damit lässt sich die Verwaltung, Suche und Filterung von Ressourcen effizient gestalten. Ein Schlüssel ohne Wert wird als Key-Only-Tag bezeichnet, ein Schlüssel mit einem Wert wird als Key-Value-Tag bezeichnet. Obwohl es keine inhärenten Typen von Tags gibt, können Sie Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien kategorisieren. Dies ist nützlich, wenn Sie viele Ressourcen desselben Typs haben. Sie können eine bestimmte Ressource anhand der ihr zugewiesenen Tags schnell identifizieren. Definieren Sie beispielsweise einen Satz von Tags, mit denen Sie das Projekt oder die Priorität jeder Ressource verfolgen können.

Die folgenden Ressourcen können in der Amazon Lightsail for Research-Konsole mit Tags versehen werden:

- Virtuelle Computer
- Datenträger
- Snapshots

Für Tags gelten die folgenden Einschränkungen:

- Die maximale Anzahl an Tags pro Ressource beträgt 50.
- Für jede Ressource muss jeder Tag-Schlüssel eindeutig sein. Jeder Tag-Schlüssel kann nur einen Wert haben.
- Die maximale Schlüssellänge beträgt 128 Unicode-Zeichen in UTF -8.
- Die maximale Wertelänge beträgt 256 Unicode-Zeichen in UTF -8.
- Wenn Ihr Markierungsschema für mehrere Services und Ressourcen verwendet wird, denken Sie daran, dass die zulässigen Zeichen bei anderen Services möglicherweise eingeschränkt sind. Allgemein erlaubte Zeichen sind: Buchstaben, Zahlen, Leerzeichen und die folgenden Sonderzeichen: `+ - = . _ : / @`
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Verwenden Sie nicht das `aws:`-Präfix für Schlüssel oder Werte. Dieses Präfix ist für die AWS Verwendung reserviert.

Themen

Schlagwort: Lightsail for Research-Ressourcen

Gehen Sie wie folgt vor, um ein Tag für Ihren virtuellen Lightsail for Research-Computer zu erstellen. Die Schritte sind für Lightsail for Research-Disketten und -Snapshots ähnlich.

1. Melden Sie sich bei der Lightsail for Research-Konsole auf der Lightsail for Research-Konsole an.
2. Wählen Sie im linken Navigationsbereich Virtuelle Computer aus.
3. Wählen Sie den virtuellen Computer aus, für den Sie ein Tag erstellen möchten.
4. Wählen Sie die Registerkarte Tags aus.
5. Wählen Sie Tags verwalten aus.
6. Wählen Sie Neues Tag hinzufügen aus.
7. Geben Sie einen Schlüsselnamen in das Feld Schlüssel ein. Zum Beispiel Projekt.
8. (Optional) Geben Sie einen Wertnamen in das Feld Wert ein. Zum Beispiel Blog.
9. Wählen Sie Änderungen speichern, um den Schlüssel auf Ihrem virtuellen Computer zu speichern.

Tags aus den Ressourcen von Lightsail for Research entfernen

Gehen Sie wie folgt vor, um ein Tag von Ihrem virtuellen Lightsail for Research-Computer zu löschen. Die Schritte sind für Lightsail for Research-Disketten und -Snapshots ähnlich.

1. Melden Sie sich bei der Lightsail for Research-Konsole auf der Lightsail for Research-Konsole an.
2. Wählen Sie im linken Navigationsbereich Virtuelle Computer aus.
3. Wählen Sie den virtuellen Computer aus, von dem Sie das Tag löschen möchten.
4. Wählen Sie die Registerkarte Tags aus.
5. Wählen Sie Tags verwalten aus.
6. Wählen Sie Entfernen aus, um das Tag von der Ressource zu löschen.

> **Note**
>
> Wenn Sie nur den Wert des Tags entfernen möchten, suchen Sie den Wert und wählen Sie dann das X-Symbol neben dem Tag aus.

7. Wählen Sie Änderungen speichern.

Sicherheit in Amazon Lightsail for Research

Cloud-Sicherheit hat höchste AWS Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon Lightsail for Research gelten, finden Sie unter AWS Services im Bereich nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Lightsail for Research anwenden können. In den folgenden Themen erfahren Sie, wie Sie Lightsail for Research konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen helfen, Ihre Lightsail for Research-Ressourcen zu überwachen und zu sichern.

Themen

Datenschutz in Amazon Lightsail for Research

Das AWS Modell der gilt für den Datenschutz in Amazon Lightsail for Research. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen. AWS Cloud Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie im Abschnitt Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im GDPR Blogbeitrag auf dem AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden SieSSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter Federal Information Processing Standard () 140-3. FIPS

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Lightsail for Research oder auf andere Weise AWS-Services über die Konsole arbeiten, API AWS CLI, oder. AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen angeben, URL um Ihre Anfrage an diesen Server zu überprüfen.

Identity and Access Management für Amazon Lightsail for Research

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Lightsail for Research-Ressourcen zu verwenden. IAMist eine AWS-Service , die Sie ohne zusätzliche Kosten nutzen können.

> **Note**
>
> Amazon Lightsail und Lightsail for Research haben dieselben Richtlinienparameter. IAM Änderungen an den Richtlinien von Lightsail for Research werden sich auch auf die Richtlinien von Lightsail for Research auswirken. Wenn ein Benutzer beispielsweise berechtigt ist, eine Festplatte in Lightsail for Research zu erstellen, kann derselbe Benutzer auch eine Festplatte in Lightsail erstellen.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Lightsail for Research ausführen.

Dienstbenutzer — Wenn Sie den Lightsail for Research-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie

benötigen. Da Sie für Ihre Arbeit mehr Funktionen von Lightsail for Research verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie in Lightsail for Research nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter. Fehlerbehebung bei Identität und Zugriff auf Amazon Lightsail for Research

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Ressourcen von Lightsail for Research verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Lightsail for Research. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Lightsail for Research Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen Lightsail for Research nutzen IAM kann, finden Sie unter. So funktioniert Amazon Lightsail for Research mit IAM

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Lightsail for Research zu verwalten. Beispiele für identitätsbasierte Lightsail for Research-Richtlinien, die Sie in verwenden können, finden Sie unter. IAM Beispiele für identitätsbasierte Richtlinien für Amazon Lightsail for Research

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAMBenutzerhandbuch unter AWS API Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe ist eine Identität, die eine Sammlung von IAM Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

IAMRollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Verwenden von IAM Rollen im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um jemandem (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.
- Dienstbezogene Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.
- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen AWS Organizations. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Geräte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAMBenutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Amazon Lightsail for Research mit IAM

Bevor Sie Lightsail for Research verwendenIAM, um den Zugriff auf Lightsail for Research zu verwalten, sollten Sie sich darüber informieren, welche IAM Funktionen für Lightsail for Research verfügbar sind.

IAMFunktionen, die Sie mit Amazon Lightsail for Research verwenden können

IAMFunktion	Lightsail zur Forschungsunterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC(Schlagworte in Richtlinien)	Teilweise

IAMFunktion	Lightsail zur Forschungsunterstützung
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Nein
Servicerollen	Nein
Serviceverknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie Lightsail for Research und andere AWS Dienste mit den meisten IAM Funktionen funktionieren, finden Sie IAM im IAMBenutzerhandbuch unter AWS Dienste, die mit funktionieren.

Identitätsbasierte Richtlinien für Lightsail for Research

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen Benutzer, eine IAM Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen und Ressourcen sowie die Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden können, finden Sie im IAMBenutzerhandbuch unter Referenz zu IAM JSON Richtlinienelementen.

Identitätspolitische Beispiele für Lightsail for Research

Beispiele für identitätsbasierte Politiken von Lightsail for Research finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Lightsail for Research

Ressourcenbasierte Richtlinien innerhalb von Lightsail for Research

Unterstützt ressourcenbasierte Richtlinien: Nein

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um den kontoübergreifenden Zugriff zu ermöglichen, können Sie in einer ressourcenbasierten Richtlinie ein ganzes Konto oder IAM Entitäten in einem anderen Konto als Prinzipal angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource gewähren. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie IAMim IAMBenutzerhandbuch unter Kontoübergreifender Ressourcenzugriff.

Politische Maßnahmen für Lightsail for Research

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Lightsail for Research-Aktionen finden Sie unter Von Amazon Lightsail for Research definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in Lightsail for Research verwenden das folgende Präfix vor der Aktion:

```
lightsail
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Beispiele für identitätsbasierte Politiken von Lightsail for Research finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Lightsail for Research

Politische Ressourcen für Lightsail for Research

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der Lightsail for Research-Ressourcentypen und ihrer ARNs Typen finden Sie unter Von Amazon Lightsail for Research definierte Ressourcen in der Service Authorization Reference.

Informationen darüber, mit welchen Aktionen Sie die ARN einzelnen Ressourcen spezifizieren können, finden Sie unter Von Amazon Lightsail for Research definierte Aktionen.

Beispiele für identitätsbasierte Politiken von Lightsail for Research finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Lightsail for Research

Schlüssel zu den Policy-Bedingungen für Lightsail for Research

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.

Eine Liste der Zustandsschlüssel für Lightsail for Research finden Sie unter Condition Keys for Amazon Lightsail for Research in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon Lightsail for Research definierte Aktionen.

Beispiele für identitätsbasierte Politiken von Lightsail for Research finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon Lightsail for Research

ACLsin Lightsail for Research

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

ABACmit Lightsail for Research

Unterstützungen ABAC (Tags in Richtlinien): Teilweise

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Attributen definiert werden. In werden AWS diese Attribute als Tags bezeichnet. Sie können Tags an IAM Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt vonABAC. Anschließend entwerfen Sie ABAC Richtlinien, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt, auf die er zugreifen möchte.

ABACist hilfreich in Umgebungen, die schnell wachsen, und hilft in Situationen, in denen die Richtlinienverwaltung umständlich wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu finden Sie ABAC unter Was ist? ABAC im IAMBenutzerhandbuch. Ein Tutorial mit Schritten zur Einrichtung finden Sie im ABAC Benutzerhandbuch unter Verwenden der attributebasierten Zugriffskontrolle (ABAC). IAM

Temporäre Anmeldeinformationen mit Lightsail for Research verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen darüber, AWS-Services wie Sie mit temporären Anmeldeinformationen arbeiten können AWS-Services , finden Sie IAM im IAMBenutzerhandbuch unter Diese Informationen.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Kennwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Rollenwechsel finden Sie unter Wechseln zu einer Rolle (Konsole) im IAMBenutzerhandbuch.

Mit dem AWS CLI oder können Sie manuell temporäre Anmeldeinformationen erstellen AWS API. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen unter IAM.

Serviceübergreifende Hauptberechtigungen für Lightsail for Research

Unterstützt Forward-Access-Sitzungen () FAS: Nein

Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Lightsail for Research

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Lightsail for Research beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Lightsail for Research Sie dazu anleitet.

Servicebezogene Rollen für Lightsail for Research

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS Dienste, die mit funktionieren. IAM Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für Amazon Lightsail for Research

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Lightsail for Research-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe von AWS Management Console, AWS Command Line Interface (AWS CLI) oder ausführen. AWS API Um Benutzern die Berechtigung zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

Informationen zum Erstellen einer IAM identitätsbasierten Richtlinie anhand dieser JSON Beispieldokumente finden Sie unter IAMRichtlinien erstellen im IAMBenutzerhandbuch.

Einzelheiten zu den von Lightsail for Research definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon Lightsail for Research in der Service Authorization Reference.

Themen

- Bewährte Methoden für Richtlinien
- Die Lightsail for Research-Konsole verwenden
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Lightsail for Research-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie AWS im IAMBenutzerhandbuch unter AWS Verwaltete Richtlinien oder Verwaltete Richtlinien für Jobfunktionen.
- Berechtigungen mit den geringsten Rechten anwenden — Wenn Sie Berechtigungen mit IAM Richtlinien festlegen, gewähren Sie nur die Berechtigungen, die für die Ausführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung IAM zum Anwenden von Berechtigungen finden Sie IAMim Benutzerhandbuch unter Richtlinien und Berechtigungen. IAM
- Verwenden Sie Bedingungen in IAM Richtlinien, um den Zugriff weiter einzuschränken — Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen einzuschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um anzugeben, dass alle Anfragen mit gesendet werden müssenSSL. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMJSONRichtlinienelemente: Bedingung.
- Verwenden Sie IAM Access Analyzer, um Ihre IAM Richtlinien zu validieren, um sichere und funktionale Berechtigungen zu gewährleisten. IAM Access Analyzer validiert neue und bestehende Richtlinien, sodass die Richtlinien der IAM Richtliniensprache (JSON) und den IAM bewährten Methoden entsprechen. IAMAccess Analyzer bietet mehr als 100 Richtlinienprüfungen und

umsetzbare Empfehlungen, um Sie bei der Erstellung sicherer und funktionaler Richtlinien zu unterstützen. Weitere Informationen finden Sie unter IAMAccess Analyzer-Richtlinienvalidierung im IAMBenutzerhandbuch.

- Multi-Faktor-Authentifizierung erforderlich (MFA) — Wenn Sie ein Szenario haben, in dem IAM Benutzer oder ein Root-Benutzer erforderlich sind AWS-Konto, aktivieren Sie die Option MFA für zusätzliche Sicherheit. Um festzulegen, MFA wann API Operationen aufgerufen werden, fügen Sie MFA Bedingungen zu Ihren Richtlinien hinzu. Weitere Informationen finden Sie unter Konfiguration des MFA -geschützten API Zugriffs im IAMBenutzerhandbuch.

Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Sicherheitsmethoden IAM im IAM Benutzerhandbuch. IAM

Die Lightsail for Research-Konsole verwenden

Um auf die Amazon Lightsail for Research-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Lightsail for Research-Ressourcen in Ihrem aufzulisten und anzuzeigen. AWS-Konto Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur Anrufe an AWS CLI oder am tätigen, keine Mindestberechtigungen für die Konsole gewähren. AWS API Erlauben Sie stattdessen nur den Zugriff auf die Aktionen, die dem API Vorgang entsprechen, den sie ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Lightsail for Research-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die Lightsail for Research *ConsoleAccess* - oder *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie im Benutzerhandbuch unter Hinzufügen von Berechtigungen für einen Benutzer. IAM

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die es IAM Benutzern ermöglicht, die Inline-Richtlinien und verwalteten Richtlinien einzusehen, die mit ihrer Benutzeridentität verknüpft sind. Diese Richtlinie umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe von oder. 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": "*"
        }
    ]
}
```

Fehlerbehebung bei Identität und Zugriff auf Amazon Lightsail for Research

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Lightsail for Research und auftreten können. IAM

Themen

- Ich bin nicht berechtigt, eine Aktion in Lightsail for Research durchzuführen
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Lightsail for Research-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in Lightsail for Research durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM Benutzer versucht, die Konsole zu verwenden, um Details zu einer fiktiven *`my-example-widget`* Ressource anzuzeigen, aber nicht über die fiktiven Berechtigungen verfügt. `lightsail:`*`GetWidget`*

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `lightsail:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Lightsail for Research-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Lightsail for Research diese Funktionen unterstützt, finden Sie unter. So funktioniert Amazon Lightsail for Research mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM Benutzerhandbuch unter Gewähren des Zugriffs auf einen anderen Benutzer AWS-Konto , der IAM Ihnen gehört.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAMBenutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie Zugriff über einen Identitätsverbund gewähren, finden Sie im Benutzerhandbuch unter Zugriff für extern authentifizierte Benutzer (Identitätsverbund). IAM

- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM

Konformitätsprüfung für Amazon Lightsail for Research

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen Anwendungen erstellen HIPAA können, die AWS für sie in Frage kommen.

> **Note**
>
> Nicht alle sind berechtigt AWS-Services . HIPAA Weitere Informationen finden Sie in der Referenz für HIPAA qualifizierte Dienste.

- AWS Ressourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien für Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National

Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zusammengefasst.

- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen zu erfüllen PCIDSS, z. B. durch die Erfüllung der Anforderungen zur Erkennung von Eindringlingen, die in bestimmten Compliance-Frameworks vorgeschrieben sind.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in Amazon Lightsail for Research

Die AWS globale Infrastruktur basiert AWS-Regionen auf Availability Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet Lightsail for Research mehrere Funktionen, um Ihre Datenstabilität und Backup-Anforderungen zu erfüllen. Weitere Informationen erhalten Sie unter Backup virtuelle Computer und Festplatten mit Lightsail for Research-Snapshots und Erstellen Sie Schnappschüsse von virtuellen Computern oder Festplatten mit Lightsail for Research.

Infrastruktursicherheit in Amazon Lightsail for Research

Als verwalteter Service ist Amazon Lightsail for Research durch die AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API Aufrufe, um über das Netzwerk auf Lightsail for Research zuzugreifen. Kunden müssen Folgendes unterstützen:

- Sicherheit auf Transportschicht ()TLS. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit perfekter Vorwärtsgeheimhaltung (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Konfiguration und Schwachstellenanalyse in Amazon Lightsail for Research

Konfiguration und IT-Steuerung liegen in der gemeinsamen Verantwortung von AWS Ihnen, unserem Kunden. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Bewährte Sicherheitsmethoden für Amazon Lightsail for Research

Lightsail for Research bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Um potenzielle Sicherheitsereignisse im Zusammenhang mit Ihrer Nutzung von Lightsail for Research zu verhindern, befolgen Sie diese bewährten Methoden:

- Greifen Sie auf die Lightsail for Research-Konsole zu, indem Sie sich bei der ersten authentifizieren. AWS Management Console Teilen Sie Ihre persönlichen Konsolenanmeldedaten nicht mit anderen. Jeder Benutzer im Internet kann die Konsole aufrufen, aber er kann sich nur anmelden oder eine Sitzung starten, wenn er über gültige Anmeldeinformationen für die Konsole verfügt.

Dokumentverlauf für das Benutzerhandbuch zu Lightsail for Research

Die folgende Tabelle beschreibt die Dokumentationsversionen für Lightsail for Research.

Änderung	Beschreibung	Datum
Erstversion	Erstveröffentlichung des Benutzerhandbuchs für Lightsail for Research.	28. Februar 2023

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.