aws

ユーザーガイド

Amazon Lightsail for Research

Amazon Lightsail for Research: ユーザーガイド

Table of Contents

Amazon Lightsail for Research とは

Amazon Lightsail for Research を使用すると、学者や研究者は Amazon Web Services (AWS) クラウドで強力な仮想コンピュータを作成できます。これらの仮想コンピュータには、RStudio や Scilab などの研究用アプリケーションがプリインストールされています。

Lightsail for Research では、ウェブブラウザから直接データをアップロードして作業を開始できます。仮想コンピュータはいつでも作成および削除できるため、強力なコンピューティングリソースにオンデマンドでアクセスできます。

お支払いいただくのは、仮想コンピュータが必要な期間のみです。Lightsail for Research は、事前に設定されたコスト制限に達したときにコンピュータを自動的に停止できる予算管理コントロールを提供するため、超過料金について心配する必要はありません。

Lightsail for Research コンソールで行ったことは、一般公開されている API によってバックアップされます。Amazon Lightsail の および API をインストールAWS CLIして使用する方法について説明します。

料金

Lightsail for Research では、作成して使用したリソースに対してのみ料金が発生します。詳細については、「Lightsail for Research の料金」を参照してください。

可用性

Lightsail for Research は、米国東部 (バージニア北部) AWS リージョンを除き、Amazon Lightsail と同じリージョンで利用できます。また、Lightsail for Research は、Lightsail と同じエンドポイントを使用します。Lightsail で現在サポートされている AWS リージョンとエンドポイントを確認するには、「 AWS 全般のリファレンス」の「Lightsail エンドポイントとクォータ」を参照してください。

Amazon Lightsail for Research のセットアップ

新規の AWS お客様は、Amazon Lightsail for Research の使用を開始する前に、このページに記載されているセットアップの前提条件を完了してください。これらのセットアップ手順では、 AWS Identity and Access Management (IAM) サービスを使用します。IAM の詳細については、「IAM ユーザーガイド」を参照してください。

トピック

にサインアップする AWS

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

IAM ユーザーの作成

管理者ユーザーを作成するには、以下のいずれかのオプションを選択します。

管理者を管理する方法を 1 つ選択します	目的	方法	以下の操作も可能
IAM Identity Center 内 (推奨)	短期の認証情報を使用して AWSにアクセスします。 これはセキュリティのベストプラクティスと一致しています。ベストプラクティスの詳細については、IAM ユーザーガイドの「IAM でのセキュリティのベストプラクティス」を参照してください。	AWS IAM Identity Center ユーザーガイドの「開始方法」の手順に従います。	ユーザーガイド の を使用する AWS CLI ように を設定 AWS IAM Identity Centerして、プログラムによるアクセスを設定します。 AWS Command Line Interface
IAM 内 (非推奨)	長期認証情報を使用して AWSにアクセスする。	IAM ユーザーガイドの「最初の IAM 管理者のユーザーおよびグループの作成」の手順に従います。	IAM ユーザーガイドの「IAM ユーザーのアクセスキーの管理」に従って、プログラムによるアクセスを設定します。

チュートリアル: Lightsail for Research 仮想コンピュータの使用を開始する

このチュートリアルを使用して、Amazon Lightsail for Research 仮想コンピュータの使用を開始します。仮想コンピュータの作成、接続、使用の方法について説明します。Lightsail for Research の仮想コンピュータは AWS クラウドで作成して管理する研究用ワークステーションです。仮想コンピュータは Ubuntu オペレーティングシステムを搭載した Lightsail インスタンスをベースにしています。仮想コンピュータでは、JupyterLab、RStudio、Scilab などの研究用アプリケーションを事前構成できます。

このチュートリアルで作成した仮想コンピュータには、仮想コンピュータを作成してから削除するまでの間、使用料が発生します。削除はこのチュートリアルの最後のステップになります。料金の詳細については、「Lightsail の料金」を参照してください。

トピック

ステップ 1: 前提条件を満たす

初めてAWS を利用する方は、Amazon Lightsail for Research の使用を始める前に、セットアップの前提条件を完了させてください。詳細については、「Amazon Lightsail for Research のセットアップ」を参照してください。

ステップ 2: 仮想コンピュータを作成する

以下に説明する手順で、Lightsail for Research コンソールを使用して仮想コンピュータを作成できます。このチュートリアルは、初めての仮想コンピュータを素早く起動できるように構成されていま

す。また、利用可能なアプリケーションとハードウェアプランについて調べておくことをお勧めします。詳細については、アプリケーションとハードウェアプラン および 仮想コンピュータを作成する を参照してください。

1. Lightsail for Research コンソールにサインインします。
2. ホームページで [仮想コンピュータを作成] を選択します。
3. 仮想コンピュータの AWS リージョン を選択します。

   レイテンシーを改善するには、実際の場所に最も近いリージョンを選択します。
4. アプリケーションを選択します (Lightsail API ではブループリントとも呼ばれます)。

   選択したアプリケーションは、作成時に仮想コンピュータにインストールされ、構成されます。
5. ハードウェアプランを選択します (Lightsail API ではバンドルとも呼ばれます)。

   ハードウェアプランでは、vCPU コア、メモリ、ストレージ、毎月のデータ転送など、さまざまな処理に関わる機能が提供されます。Lightsail for Research では、仮想コンピュータ用にスタンダードプランと GPU プランを提供しています。作業に必要な計算能力が少ない場合は、スタンダードプランを選択してください。機械学習モデルなど、高度な計算能力が要求されるタスクを実行する場合は、GPU プランを選択してください。
6. 仮想コンピュータの名前を入力します。
7. [概要] パネルで [仮想コンピュータを作成] を選択します。

新しい仮想コンピュータを起動したら、このチュートリアルの次のステップで、コンピュータのアプリケーションを起動する方法を確認します。

ステップ 3: 仮想コンピュータのアプリケーションを起動する

仮想コンピュータを作成して [実行中] の状態になったら、ウェブブラウザで仮想セッションを起動できます。このセッションでは、仮想コンピュータにインストールされているアプリケーションの操作と管理ができます。

1. Lightsail for Research コンソールのナビゲーションペインで [仮想コンピュータ] を選択します。
2. ステップ 1 で作成した仮想コンピュータの名前を探し、[アプリケーションを起動] を選択します。例えば、[JupyterLab を起動] を選択します。アプリケーションセッションが新しいウェブブラウザウィンドウで開きます。

> **Important**
>
> ウェブブラウザにポップアップブロッカーがインストールされている場合は、セッションを開く前に aws.amazon.com ドメインのポップアップを許可する必要がある場合があります。

仮想コンピュータへの接続方法については、このチュートリアルの次のステップで説明します。

ステップ 4: 仮想コンピュータに接続する

仮想コンピュータには、次の方法を使用して接続できます。

- Lightsail for Research コンソールで利用できる、ブラウザベースの NICE DCV クライアントを使用する。NICE DCV では、グラフィカルユーザーインターフェイス (GUI) を使用して研究用アプリケーションや仮想コンピュータのオペレーティングシステムを操作できます。
- OpenSSH、PuTTY、Linux 用 Windows サブシステムなどの Secure Shell (SSH) クライアントを使用して、仮想コンピュータのコマンドラインインターフェイスにアクセスする。SSH クライアントでは、スクリプトや設定ファイルを編集できます。
- Secure Copy (SCP) を使用して、ローカルコンピュータと仮想コンピュータの間でファイルを安全に転送する。SCP を使用すると、ローカルで開始した作業を仮想コンピュータで続行できます。仮想コンピュータからファイルをダウンロードして、作業内容をローカルコンピュータにコピーすることもできます。

> **Note**
>
> また、ブラウザベースの NICE DCV クライアントを使用すれば、仮想コンピュータのコマンドラインインターフェイスにアクセスしてファイルを転送することもできます。

SSH を使用して接続したり、SCP を使用してファイルを転送したりするには、仮想コンピュータのキーペアを指定する必要があります。キーペアは、Lightsail for Research 仮想コンピュータへの接続時にユーザーのアイデンティティを証明するために使用する一連のセキュリティ認証情報です。キーペアはパブリックキーとプライベートキーで構成されます。

仮想コンピュータへの接続の詳細については、以下のドキュメントを参照してください。

- リモートディスプレイプロトコル接続を確立する:
  - 仮想コンピュータのアプリケーションを起動する
  - 仮想コンピュータのオペレーティングシステムにアクセスする
- SSH 接続を確立するか、SCP を使用してファイルを転送する:
  - 仮想コンピュータのキーペアを取得する
  - Secure Shell を使用して仮想コンピュータに接続する
  - Secure Copy を使用してファイルを仮想コンピュータに転送する

仮想コンピュータのストレージについては、このチュートリアルの次のステップで説明します。

ステップ 5: 仮想コンピュータにストレージを追加する

Lightsail for Research は、仮想コンピュータに接続できるブロックレベルのストレージボリューム (ディスク) を提供します。仮想コンピュータにはシステムディスクが付属していますが、ストレージの需要の変化に応じて、追加のディスクを仮想コンピュータに接続できます。また、仮想コンピュータからディスクを切り離し、別の仮想コンピュータに接続することもできます。

コンソールを使用してディスクを仮想コンピュータに接続すると、Lightsail for Research はディスクを自動的にフォーマットし、オペレーティングシステムにマウントします。この処理には数分かかるため、使用を開始する前に、ディスクが [マウント済み] の状態であることを確認する必要があります。

ディスクの作成、接続、管理に関する詳細については、以下のドキュメントを参照してください。

- ディスクの作成
- ディスクを表示する
- ディスクを仮想コンピュータに接続する
- 仮想コンピュータからディスクを切り離す
- ディスクの削除

仮想コンピュータのバックアップについては、このチュートリアルの次のステップで説明します。

ステップ 6: スナップショットを作成する

スナップショットは、データのポイントインタイムコピーです。仮想コンピュータのスナップショットを作成し、それをベースラインとして使用して、新しいコンピュータを作成したり、データをバックアップしたりできます。スナップショットには、コンピュータの復元に必要なすべてのデータ (スナップショットが作成された時点のデータ) が含まれます。

スナップショットの作成および管理に関する詳細については、以下のドキュメントを参照してください。

- スナップショットを作成する
- スナップショットを表示する
- スナップショットから仮想コンピュータまたはディスクを作成する
- スナップショットの削除

仮想コンピュータリソースのクリーンアップについては、このチュートリアルの次のステップで説明します。

ステップ 7: クリーンアップする

このチュートリアルで作成した仮想コンピュータは、作業完了後に削除することができます。これにより、必要のない仮想コンピュータの料金が発生しなくなります。

仮想コンピュータを削除しても、関連するスナップショットやアタッチされたディスクは削除されません。スナップショットとディスクを作成した場合、料金の発生を停止するには手動で削除する必要があります。

仮想コンピュータを後で使用できるように保存しつつ、標準の時間料金で課金されないために、仮想コンピュータを削除するのではなく停止することができます。これは後で再起動できます。詳細については、「仮想コンピュータの詳細を表示する」を参照してください。料金の詳細については、「Lightsail の料金」を参照してください。

> **Important**
>
> Lightsail for Research リソースの削除は永続的なアクションです。削除されたデータは復元できません。後でデータが必要になる可能性がある場合は、削除する前に仮想コンピュータ

のスナップショットを作成します。詳細については、「スナップショットを作成する」を参照してください。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[仮想コンピュータ] を選択します。
3. 削除する仮想コンピュータを選択します。
4. [アクション]、[仮想コンピュータを削除] の順に選択します。
5. テキストブロックに「confirm」と入力します。次に、[仮想コンピュータを削除] を選択します。

Amazon Lightsail for Research の開始方法のチュートリアル

以下のチュートリアルでは、Lightsail for Research で利用できる特定のアプリケーションの使用を開始する方法に関する追加情報を提供します。

トピック

- の開始方法 JupyterLab
- RStudio の使用を開始する

> **Note**
>
> Lightsail for Research と RStudio の使用を開始するための詳細なチュートリアルは、 AWS Public Sector Blog に公開されています。詳細については、「Getting started with Amazon Lightsail for Research: A tutorial using RStudio」を参照してください。

の開始方法 JupyterLab

このチュートリアルでは、Amazon Lightsail for Research で JupyterLab 仮想コンピュータの管理と使用を開始する方法について説明します。

トピック

- ステップ 1: 前提条件を満たす
- ステップ 2: (オプション) ストレージ領域を追加する
- ステップ 3: ファイルをアップロードおよびダウンロードする
- ステップ 4: アプリケーションを起動する JupyterLab
- ステップ 5: ドキュメントを読み取る JupyterLab
- ステップ 6: (オプション) 使用量とコストをモニタリングする
- ステップ 7: (オプション) コスト管理ルールを作成する
- ステップ 8: (オプション) スナップショットを作成する
- ステップ 9: (オプション) 仮想コンピュータを停止または削除する

ステップ 1: 前提条件を満たす

JupyterLab アプリケーションを使用して仮想コンピュータをまだ作成していない場合は、作成します。詳細については、「仮想コンピュータを作成する」を参照してください。

新しい仮想コンピュータが稼働したら、このチュートリアルの JupyterLab 「アプリケーションを起動する」セクションに進みます。

ステップ 2: (オプション) ストレージ領域を追加する

仮想コンピュータにはシステムディスクが付属しています。ただし、ストレージのニーズが変化したら、仮想コンピュータに追加のディスクをアタッチしてストレージ領域を増やすことができます。

作業ファイルをアタッチされたディスクに保存することもできます。その後、ディスクをデタッチして別の仮想コンピュータにアタッチすると、ファイルをあるコンピュータから別のコンピュータにすばやく移動できます。

または、作業ファイルのあるアタッチされたディスクのスナップショットを作成し、そのスナップショットから複製ディスクを作成することもできます。その後、新しい複製ディスクを別のコンピュータにアタッチして、作業を別の仮想コンピュータに複製できます。詳細については、ディスクの作成およびディスクを仮想コンピュータに接続するを参照してください。

> **Note**
>
> コンソールを使用してディスクを仮想コンピュータに接続すると、Lightsail for Research は自動的にディスクをフォーマットしてマウントします。この処理には数分かかるため、使用を開始する前に、ディスクのマウント状態が [マウント済み] になっていることを確認する必要があります。デフォルトでは、Lightsail for Research はディスクを `/home/lightsail-user/<disk-name>` ディレクトリにマウントします。 *`<disk-name>`*はディスクに付けた名前です。

ステップ 3: ファイルをアップロードおよびダウンロードする

JupyterLab 仮想コンピュータにファイルをアップロードし、そこからファイルをダウンロードすることができます。そのためには、以下の手順を実行します。

1. Amazon Lightsail からキーペアを取得します。詳細については、「仮想コンピュータのキーペアを取得する」を参照してください。

2. キーペアを入手したら、それを使用して Secure Copy (SCP) ユーティリティを使用して接続を確立できます。SCP では、コマンドプロンプトまたはターミナルを使用してファイルをアップロードおよびダウンロードできます。詳細については、「Secure Copy を使用してファイルを仮想コンピュータに転送する」を参照してください。
3. (オプション) キーペアを使用して、SSH で仮想コンピュータに接続することもできます。詳細については、「Secure Shell を使用して仮想コンピュータに接続する」を参照してください。

> **Note**
>
> また、ブラウザベースの NICE DCV クライアントを使用すれば、仮想コンピュータのコマンドラインインターフェイスにアクセスしてファイルを転送することもできます。NICE DCV は Lightsail for Research コンソールで使用できます。詳細については、仮想コンピュータのアプリケーションを起動するおよび仮想コンピュータのオペレーティングシステムにアクセスするを参照してください。

アタッチされたストレージディスク内でプロジェクトファイルを管理するには、アタッチされているディスクの正しいマウントディレクトリにアップロードしてください。コンソールを使用してディスクを仮想コンピュータに接続すると、Lightsail for Research はディスクを自動的にフォーマットして /home/lightsail-user/*<disk-name>* ディレクトリにマウントします。 *<disk-name>*はディスクに付けた名前です。

ステップ 4: アプリケーションを起動する JupyterLab

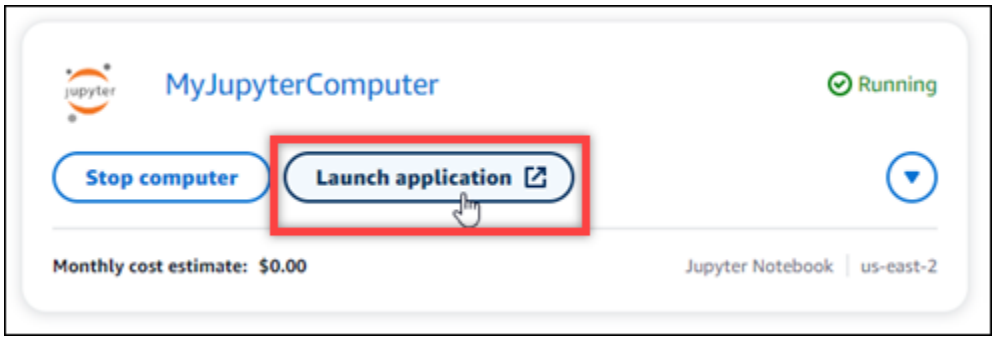
新しい仮想コンピュータで JupyterLab アプリケーションを起動するには、以下の手順を実行します。

> **Important**
>
> オペレーティングシステムや JupyterLab アプリケーションの更新を求められた場合でも、更新しないでください。更新せず、これらのプロンプトを閉じるか無視するよう選択してください。さらに、/home/lightsail-admin/ ディレクトリにあるファイルは変更しないでください。これらの操作により、仮想コンピュータが使用できなくなる可能性があります。

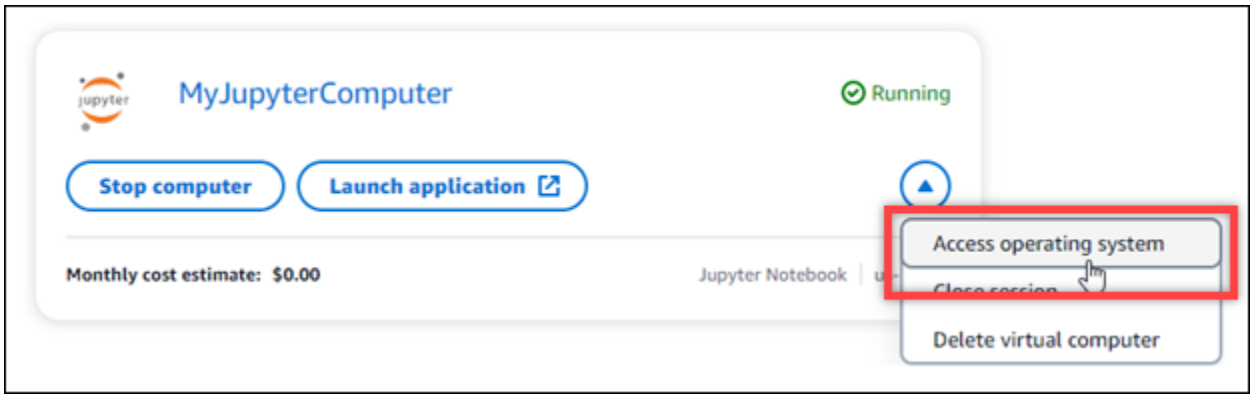
1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで [仮想コンピュータ] を選択すると、アカウントで使用可能な仮想コンピュータが表示されます。

3. [仮想コンピュータ] ページで仮想コンピュータを探し、以下のいずれかのオプションを選択して接続します。

   a. （推奨) アプリケーションの起動 を選択して、アプリケーションを JupyterLab フォーカスモードで起動します。仮想コンピュータに最近接続していない場合は、Lightsail for Research がセッションを準備するまで数分かかることがあります。



   b. コンピュータのドロップダウンメニューを選択し、[オペレーティングシステムにアクセス] を選択して仮想コンピュータのデスクトップにアクセスします。

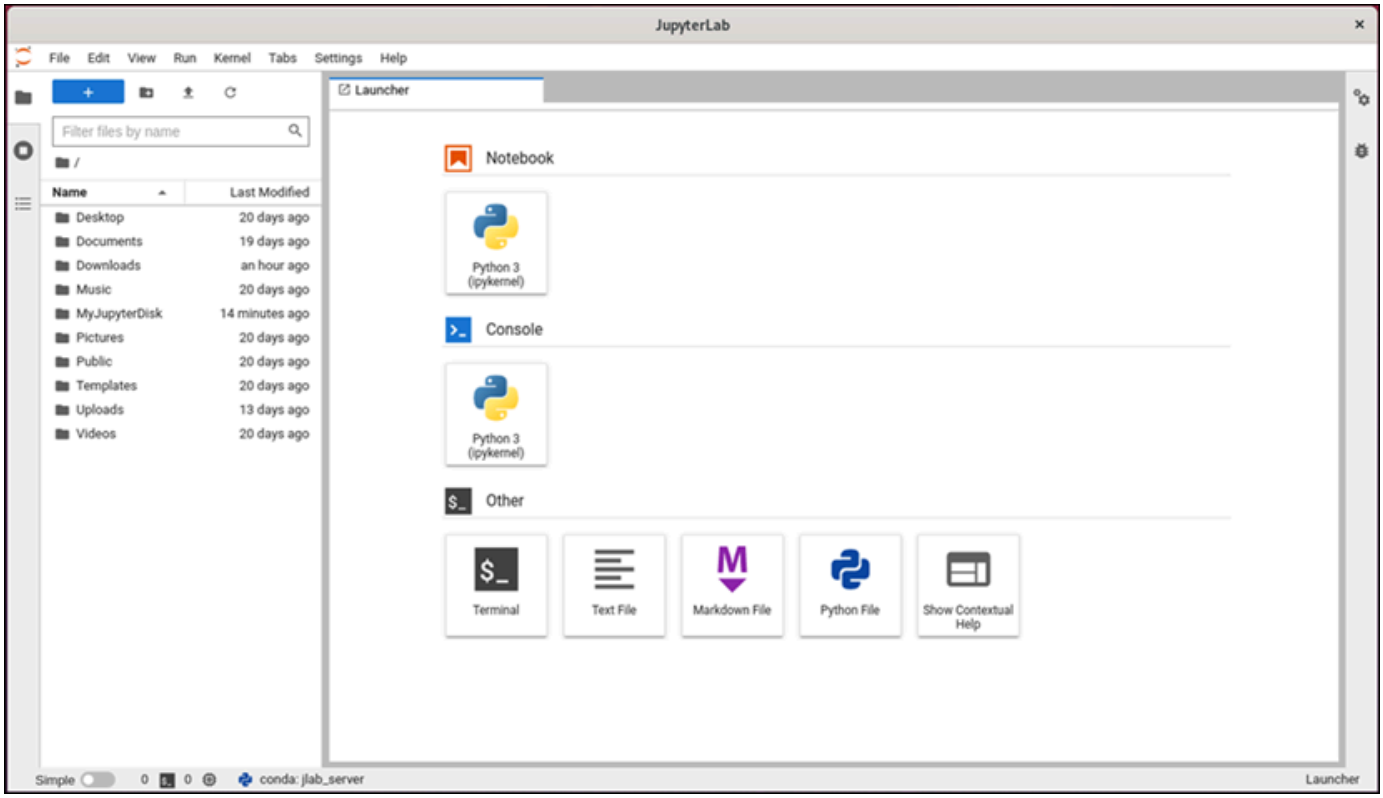


Lightsail for Research は、いくつかのコマンドを実行してリモートディスプレイプロトコル接続を開始します。しばらくすると、新しいブラウザタブウィンドウが開き、仮想コンピュータとの仮想デスクトップ接続が確立されます。アプリケーションの起動オプションを選択した場合は、この手順の次のステップに進み、 JupyterLab アプリケーションでファイルを開きます。[オペレーティングシステムにアクセス] オプションを選択した場合は、Ubuntu デスクトップから他のアプリケーションを開くことができます。

> **Note**
>
> ブラウザによっては、クリップボードの共有を許可するよう求められる場合があります。これを許可すると、ローカルコンピュータと仮想コンピュータの間でコピーアンドペーストができるようになります。

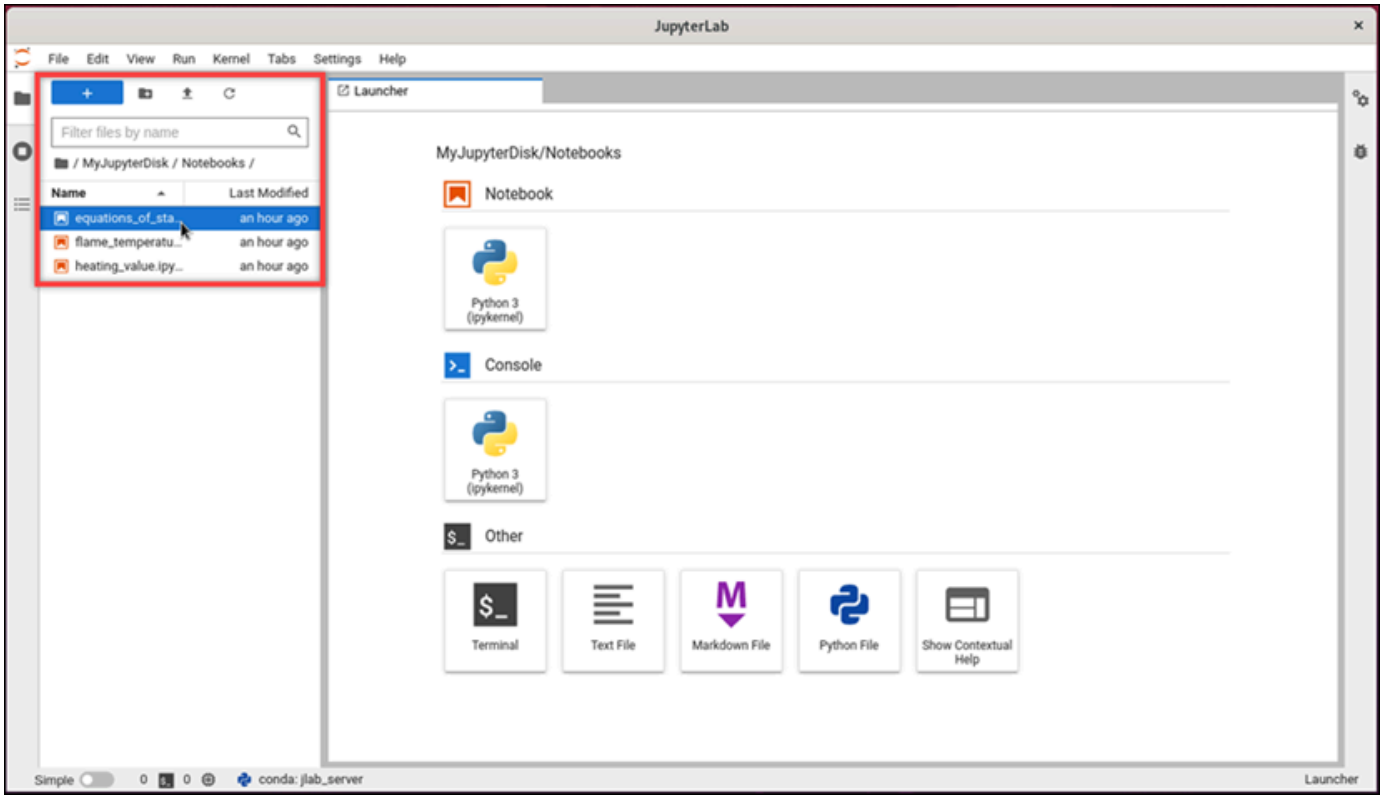
Ubuntu から初期設定を求めるメッセージが表示されることもあります。セットアップが完了し、オペレーティングシステムを使用できるようになるまで、プロンプトに従います。

4. JupyterLab アプリケーションが開きます。ランチャーメニューでは、新しいノートブックの作成、コンソールの起動、ターミナルの起動、さまざまなファイルの作成を行うことができます。

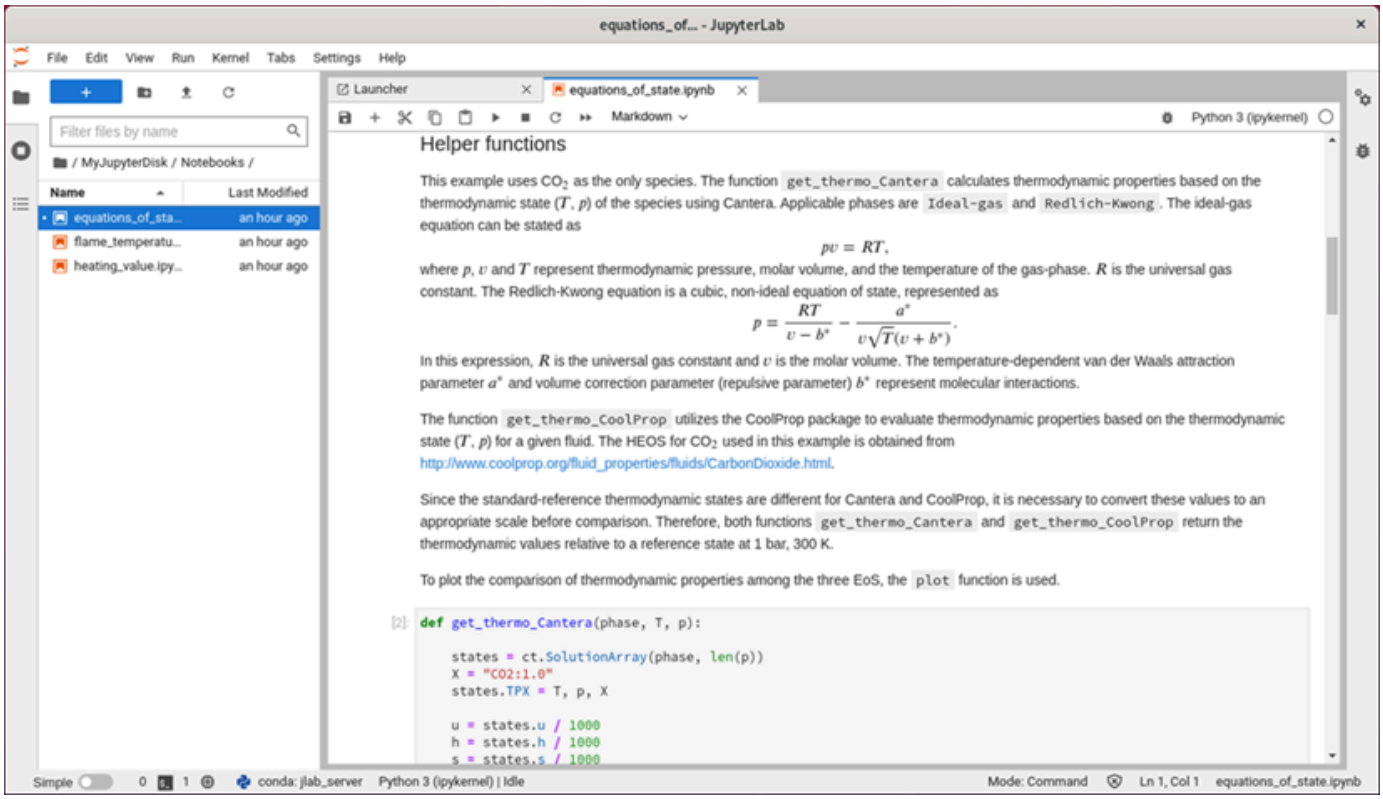


5. でファイルを開くには JupyterLab、ファイルブラウザペインで、プロジェクトファイルが保存されているディレクトリまたはフォルダを選択します。次に、ファイルを選択して開きます。

   アタッチされているディスクにプロジェクトファイルをアップロードした場合は、ディスクがマウントされているディレクトリを探します。デフォルトでは、Lightsail for Research はディスクを `/home/lightsail-user/<disk-name>` ディレクトリにマウントします。 *<disk-name>*はディスクに付けた名前です。次の例では、`MyJupyterDisk` ディレクトリはマウントされたディスクを表し、`Notebooks` サブディレクトリには Jupyter Notebook ファイルが格納されています。



次の例では、`equations_of_state.ipynb` Jupyter Notebook ファイルを開いています。



使用開始方法については、このチュートリアルの [ステップ 5: ドキュメントを読み取る JupyterLab] セクションに進みます。

ステップ 5: ドキュメントを読み取る JupyterLab

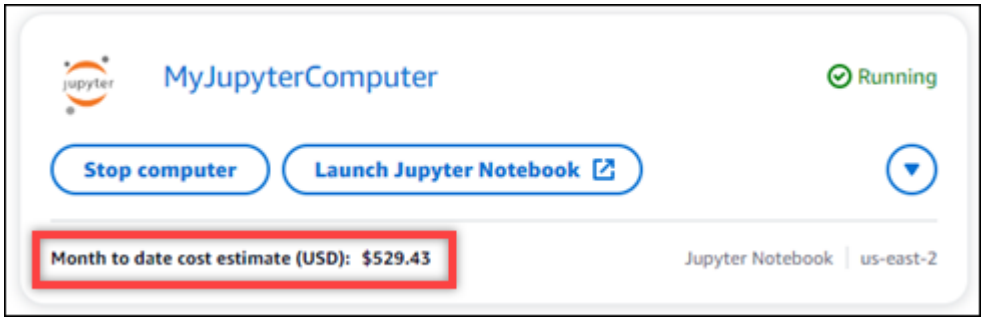
に慣れていない場合は JupyterLab、公式ドキュメントを読むことをお勧めします。次の JupyterLab オンラインリソースを使用できます。

- JupyterLab ドキュメント
- Jupyter Discourse Forum
- JupyterLab での StackOverflow
- JupyterLab での GitHub

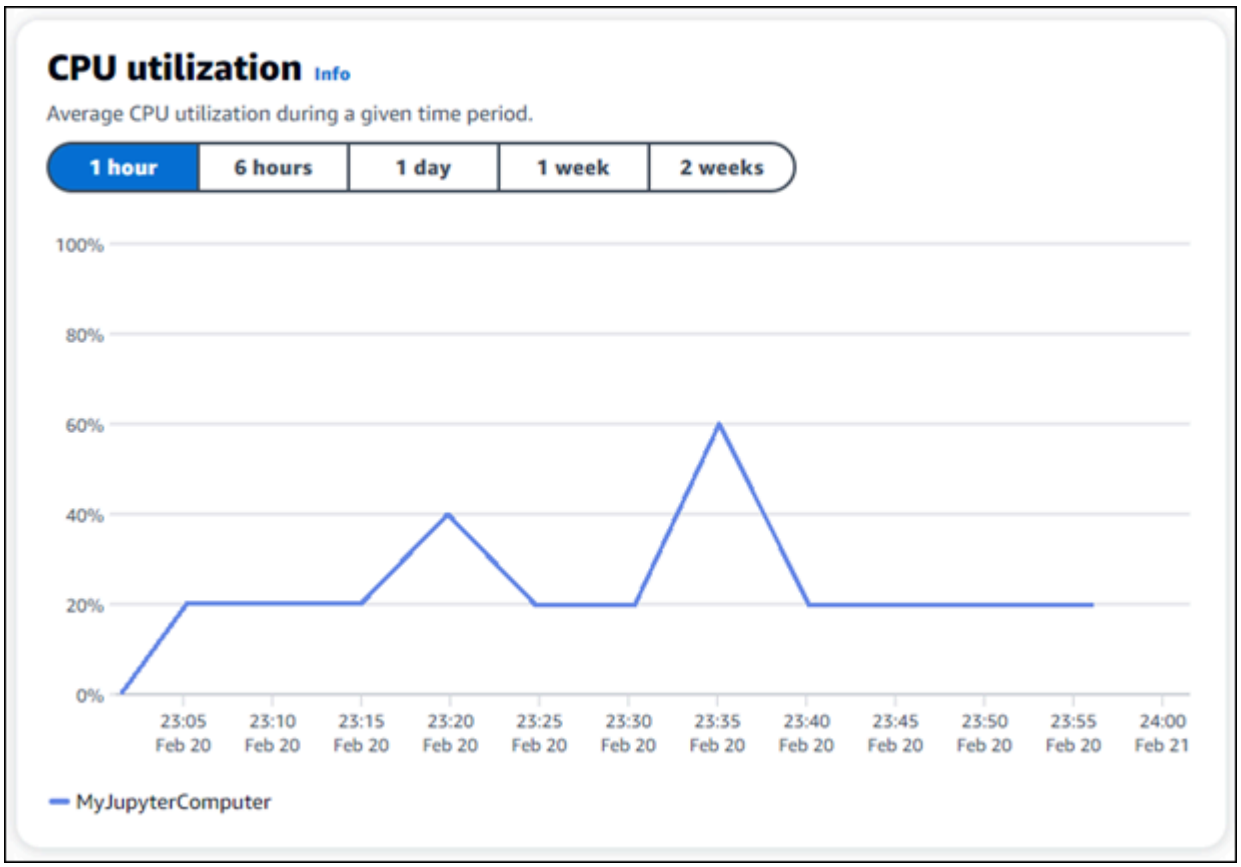
ステップ 6: (オプション) 使用量とコストをモニタリングする

Lightsail for Research リソースの過去 1 か月のコストと使用状況の見積もりは、Lightsail for Research コンソールの次の領域に表示されます。

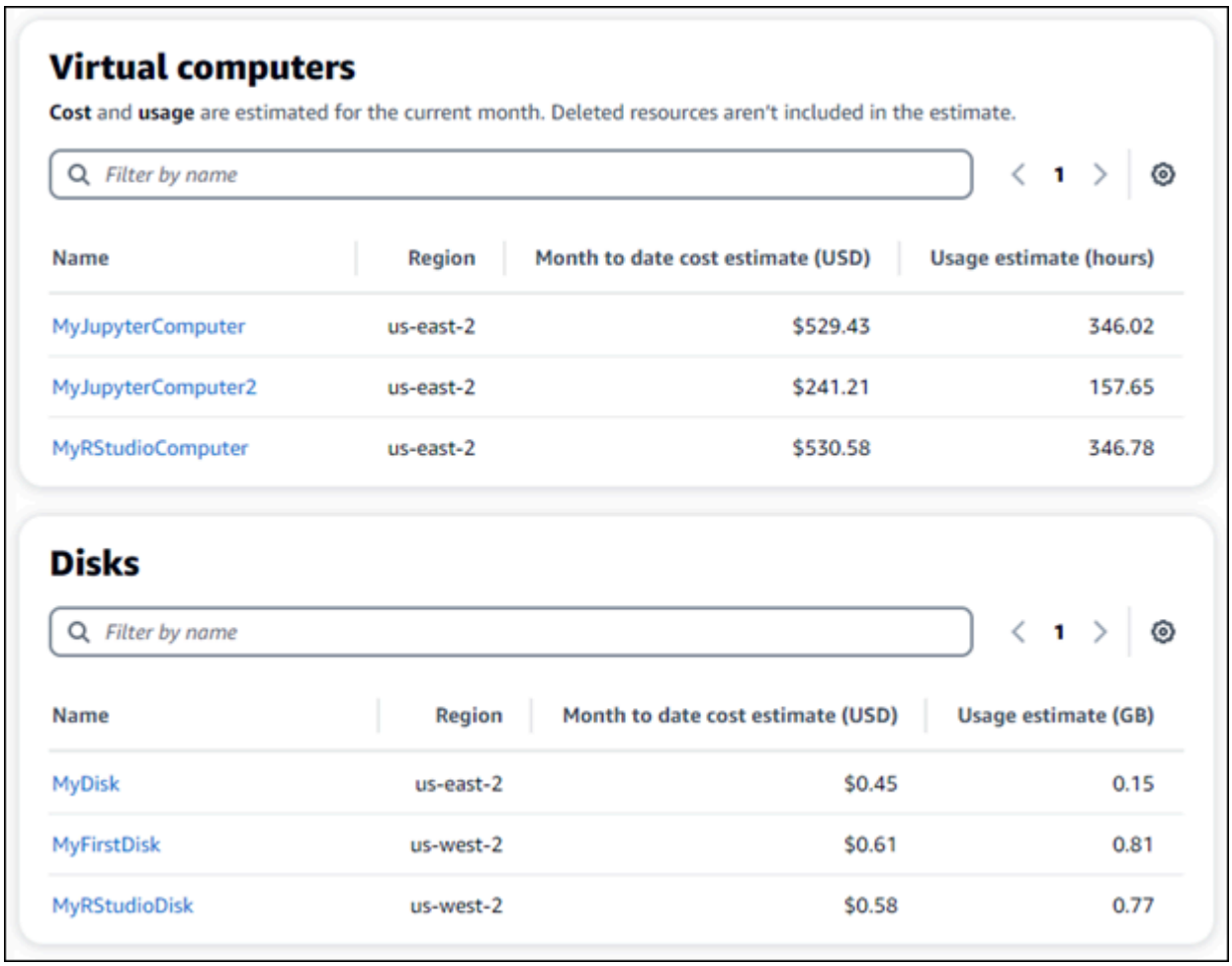
1. Lightsail for Research コンソールのナビゲーションペインで仮想コンピュータを選択します。仮想コンピュータの月初来のコスト見積もりは、実行中の各仮想コンピュータの下に表示されます。



2. 仮想コンピュータの CPU 使用率を表示するには、仮想コンピュータの名前を選択し、[ダッシュボード] タブを選択します。



3. すべての Lightsail for Research リソースの過去 1 か月のコストと使用状況の見積もりを表示するには、ナビゲーションペインで Usage を選択します。



ステップ 7: (オプション) コスト管理ルールを作成する

コスト管理ルールを作成して、仮想コンピュータの使用量とコストを管理します。一定期間に CPU 使用率が指定した割合に達すると実行中のコンピュータを停止する「アイドル状態の仮想コンピュータを停止」ルールを作成できます。例えば、30 分間の CPU 使用率が 5% 以下になると特定のコンピュータを自動的に停止するルールを作成できます。これは、コンピュータがアイドル状態であり、Lightsail for Research がコンピュータを停止して、アイドル状態のリソースに対して料金が発生しないようにすることを意味します。

> **Important**
>
> アイドル状態の仮想コンピュータを停止するルールを作成する前に、その CPU 使用率を数日間モニタリングすることをおすすめします。仮想コンピュータがさまざまな負荷を受けている間の CPU 使用率を記録しておきましょう。例えば、コードのコンパイル時、操作の処理中、アイドリング時などです。これは、ルールの正確なしきい値を決定するのに役立ちま

す。詳細については、このチュートリアルの「ステップ 6: (オプション) 使用量とコストをモニタリングする」セクションを参照してください。
CPU 使用率のしきい値がワークロードよりも高いルールを作成すると、そのルールによって仮想コンピュータが連続して停止する可能性があります。例えば、ルールによって停止した直後に仮想コンピュータを起動すると、ルールが再びアクティブになり、コンピュータは再び停止します。

コスト管理ルールの作成と管理の詳細な手順は、以下のガイドに記載されています。

- コスト管理
- ルールの作成
- ルールの削除

ステップ 8: (オプション) スナップショットを作成する

スナップショットはデータ point-in-time のコピーです。仮想コンピュータのスナップショットを作成し、それをベースラインとして使用して、新しいコンピュータを作成したり、データをバックアップしたりできます。スナップショットには、コンピュータの復元に必要なすべてのデータ (スナップショットが作成された時点のデータ) が含まれます。

スナップショットの作成と管理の詳細な手順は、以下のガイドに記載されています。

- スナップショットを作成する
- スナップショットを表示する
- スナップショットから仮想コンピュータまたはディスクを作成する
- スナップショットの削除

ステップ 9: (オプション) 仮想コンピュータを停止または削除する

このチュートリアルで作成した仮想コンピュータは、作業完了後に削除することができます。これにより、必要のない仮想コンピュータの料金が発生しなくなります。

仮想コンピュータを削除しても、関連するスナップショットやアタッチされたディスクは削除されません。スナップショットとディスクを作成した場合、料金の発生を停止するには手動で削除する必要があります。

仮想コンピュータを後で使用できるように保存しつつ、標準の時間料金で課金されないために、仮想コンピュータを削除するのではなく停止することができます。これは後で再起動できます。詳細については、「仮想コンピュータの詳細を表示する」を参照してください。料金の詳細については、「Lightsail for Research の料金」を参照してください。

> **Important**
>
> Lightsail for Research リソースの削除は永続的なアクションです。削除されたデータは復元できません。後でデータが必要になる可能性がある場合は、削除する前に仮想コンピュータのスナップショットを作成します。詳細については、「スナップショットを作成する」を参照してください。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[仮想コンピュータ] を選択します。
3. 削除する仮想コンピュータを選択します。
4. [アクション]、[仮想コンピュータを削除] の順に選択します。
5. テキストブロックに「confirm」と入力します。次に、[仮想コンピュータを削除] を選択します。

RStudio の使用を開始する

このチュートリアルでは、Amazon Lightsail for Research で RStudio 仮想コンピュータの管理と使用を開始する方法について説明します。

> **Note**
>
> Lightsail for Research と RStudio の使用を開始するための詳細なチュートリアルは、 AWS Public Sector Blog に公開されています。詳細については、「Getting started with Amazon Lightsail for Research: A tutorial using RStudio」を参照してください。

トピック

- ステップ 1: 前提条件を満たす
- ステップ 2: (オプション) ストレージ領域を追加する
- ステップ 3: ファイルをアップロードおよびダウンロードする

ステップ 1: 前提条件を満たす

仮想コンピュータをまだ作成していない場合は、RStudio アプリケーションを使用して作成します。詳細については、「仮想コンピュータを作成する」を参照してください。

新しい仮想コンピュータが稼働したら、このチュートリアルのステップ 4 に進みます。

ステップ 2: (オプション) ストレージ領域を追加する

仮想コンピュータにはシステムディスクが付属しています。ただし、ストレージのニーズが変化したら、仮想コンピュータに追加のディスクをアタッチしてストレージ領域を増やすことができます。

作業ファイルをアタッチされたディスクに保存することもできます。その後、ディスクをデタッチして別の仮想コンピュータにアタッチすると、ファイルをあるコンピュータから別のコンピュータにすばやく移動できます。

または、作業ファイルのあるアタッチされたディスクのスナップショットを作成し、そのスナップショットから複製ディスクを作成することもできます。その後、新しい複製ディスクを別のコンピュータにアタッチして、作業を別の仮想コンピュータに複製できます。詳細については、ディスクの作成およびディスクを仮想コンピュータに接続するを参照してください。

> **Note**
>
> コンソールを使用してディスクを仮想コンピュータに接続すると、Lightsail for Research は自動的にディスクをフォーマットしてマウントします。この処理には数分かかるため、使用を開始する前に、ディスクのマウント状態が [マウント済み] になっていることを確認する必要があります。デフォルトでは、Lightsail for Research はディスクを `/home/lightsail-user/<disk-name>` ディレクトリにマウントします。これはディスクに付けた名前*<disk-name>*です。

ステップ 3: ファイルをアップロードおよびダウンロードする

ファイルを RStudio 仮想コンピュータにアップロードし、そこからファイルをダウンロードすることができます。そのためには、以下の手順を実行します。

1. Amazon Lightsail からキーペアを取得します。詳細については、「仮想コンピュータのキーペアを取得する」を参照してください。
2. キーペアを入手したら、それを使用して Secure Copy (SCP) ユーティリティを使用して接続を確立できます。SCP では、コマンドプロンプトまたはターミナルを使用してファイルをアップロードおよびダウンロードできます。詳細については、「Secure Copy を使用してファイルを仮想コンピュータに転送する」を参照してください。
3. (オプション) キーペアを使用して、SSH で仮想コンピュータに接続することもできます。詳細については、「Secure Shell を使用して仮想コンピュータに接続する」を参照してください。

> **Note**
>
> また、ブラウザベースの NICE DCV クライアントを使用すれば、仮想コンピュータのコマンドラインインターフェイスにアクセスしてファイルを転送することもできます。NICE DCV は Lightsail for Research コンソールで使用できます。詳細については、仮想コンピュータのアプリケーションを起動するおよび仮想コンピュータのオペレーティングシステムにアクセスするを参照してください。

ステップ 4: RStudio アプリケーションを起動する

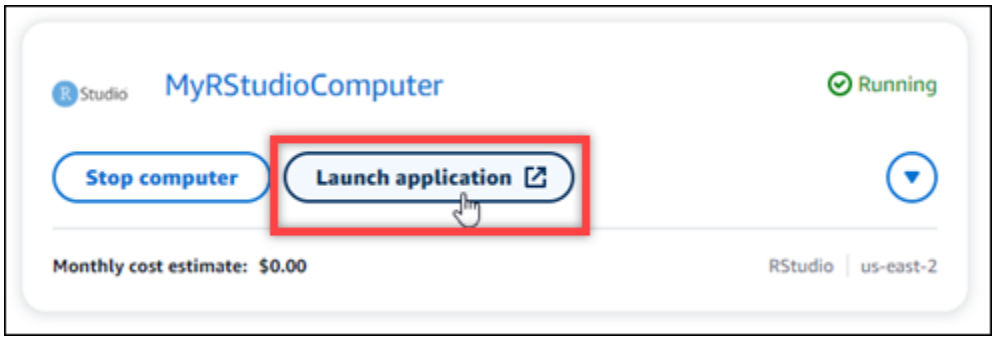
新しい仮想コンピュータで RStudio アプリケーションを起動するには、次のステップを実行します。

> **Important**
>
> オペレーティングシステムや RStudio アプリケーションを更新するようなプロンプトが表示されても、更新はしないでください。更新せず、これらのプロンプトを閉じるか無視するよう選択してください。さらに、/home/lightsail-admin/ ディレクトリにあるファイルは変更しないでください。これらの操作により、仮想コンピュータが使用できなくなる可能性があります。

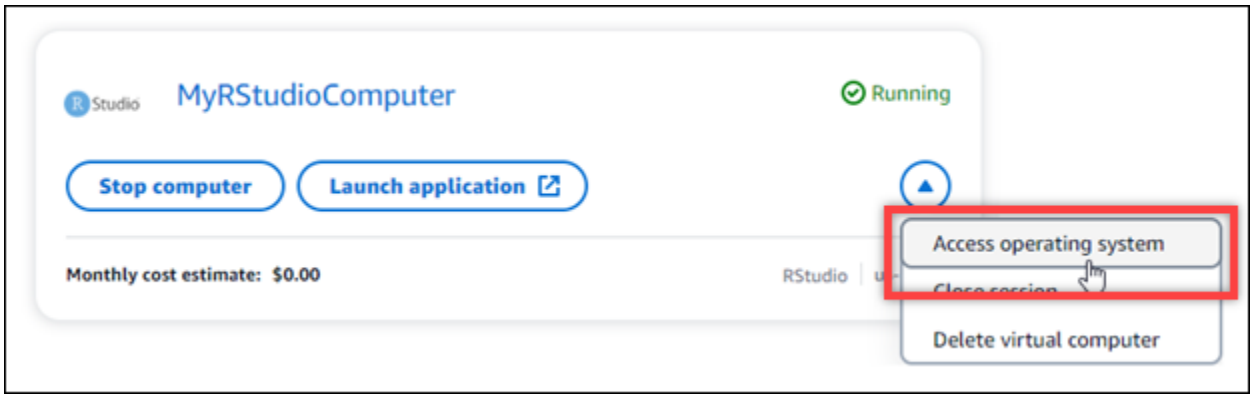
1. Lightsail for Research コンソールにサインインします。

2. ナビゲーションペインで [仮想コンピュータ] を選択すると、アカウントで使用可能な仮想コンピュータが表示されます。
3. [仮想コンピュータ] ページで仮想コンピュータを探し、以下のいずれかのオプションを選択して接続します。

   a. (推奨) [アプリケーションの起動] を選択し、RStudio アプリケーションをフォーカスモードで起動します。仮想コンピュータに最近接続していない場合は、Lightsail for Research がセッションを準備するまで数分かかることがあります。



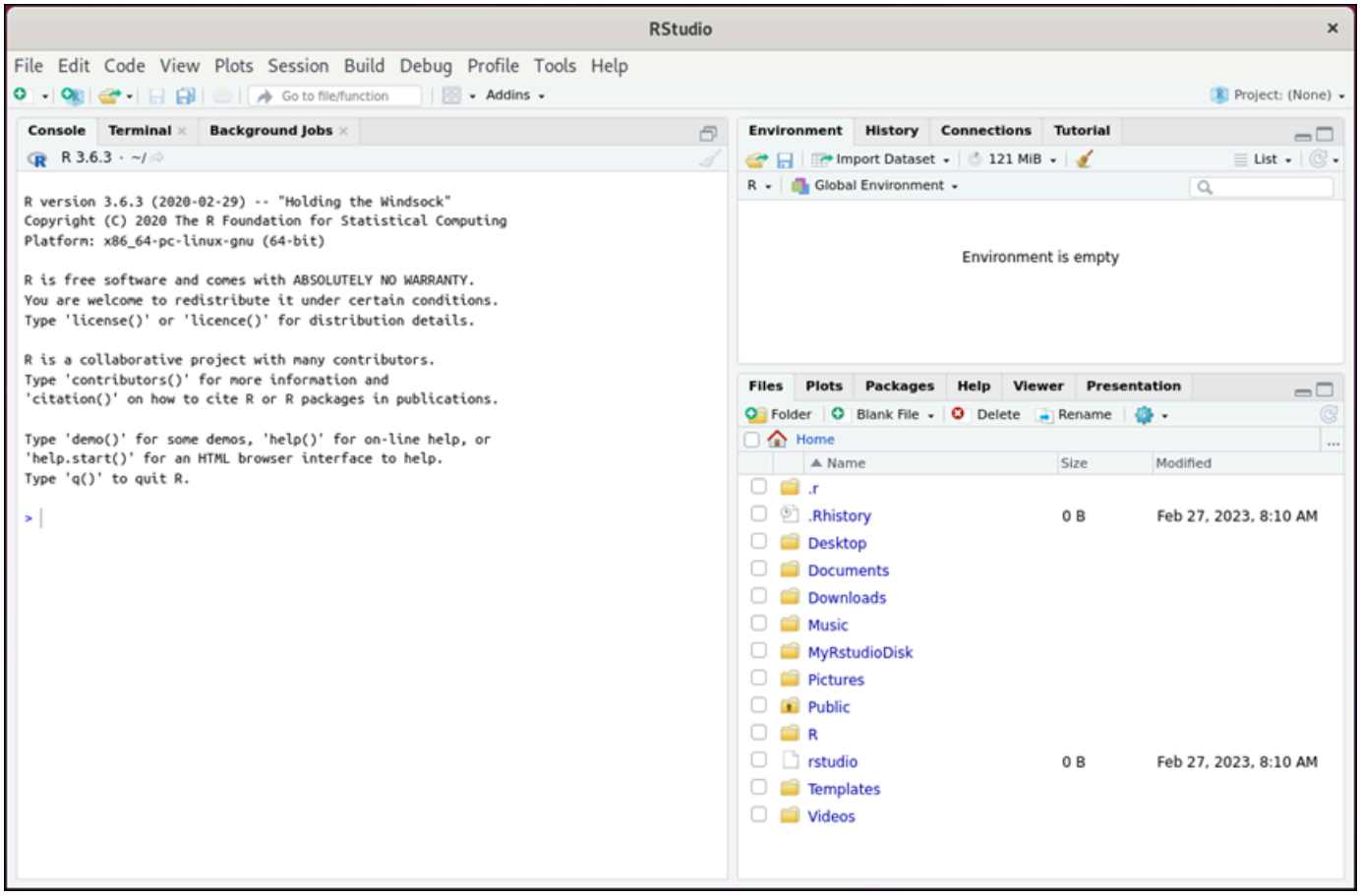
   b. コンピュータのドロップダウンメニューを選選択し、[オペレーティングシステムにアクセス] を選択して仮想コンピュータのデスクトップにアクセスします。オペレーティングシステムに別のアプリケーションをインストールする場合は、これを実行してください。



Lightsail for Research は、いくつかのコマンドを実行してリモートディスプレイプロトコル接続を開始します。しばらくすると、新しいブラウザタブウィンドウが開き、仮想コンピュータとの仮想デスクトップ接続が確立されます。[アプリケーションの起動] オプションを選択した場合は、次の手順に進んで RStudio アプリケーションでファイルを開きます。[オペレーティングシステムにアクセス] オプションを選択した場合は、Ubuntu デスクトップから他のアプリケーションを開くことができます。

> **Note**
>
> ブラウザによっては、クリップボードの共有を許可するよう求められる場合があります。これを許可すると、ローカルコンピュータと仮想コンピュータの間でコピーアンドペーストができるようになります。
>
> Ubuntu から初期設定を求めるメッセージが表示されることもあります。セットアップが完了し、オペレーティングシステムを使用できるようになるまで、プロンプトに従います。

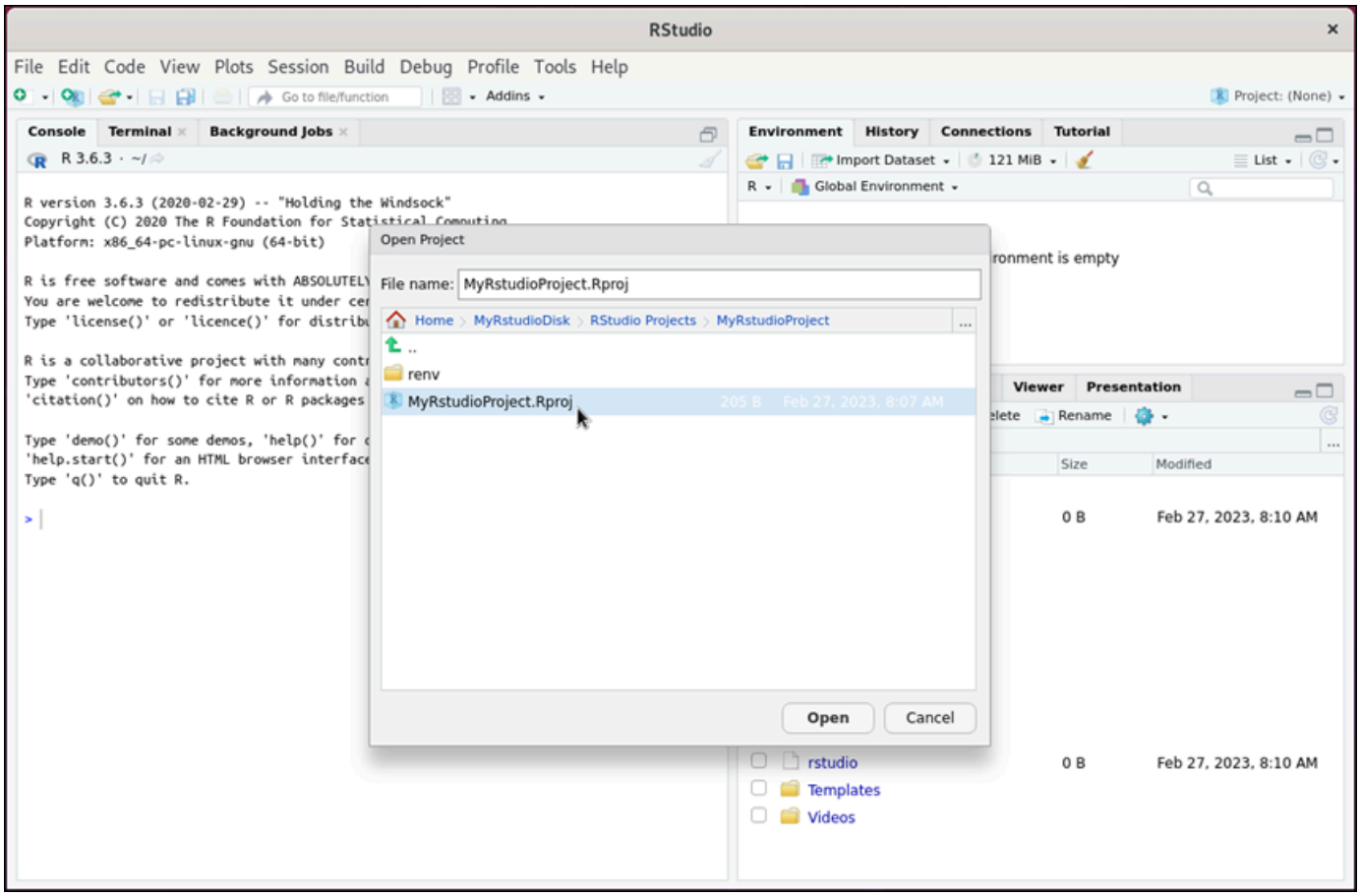
4. RStudio アプリケーションが開きます。



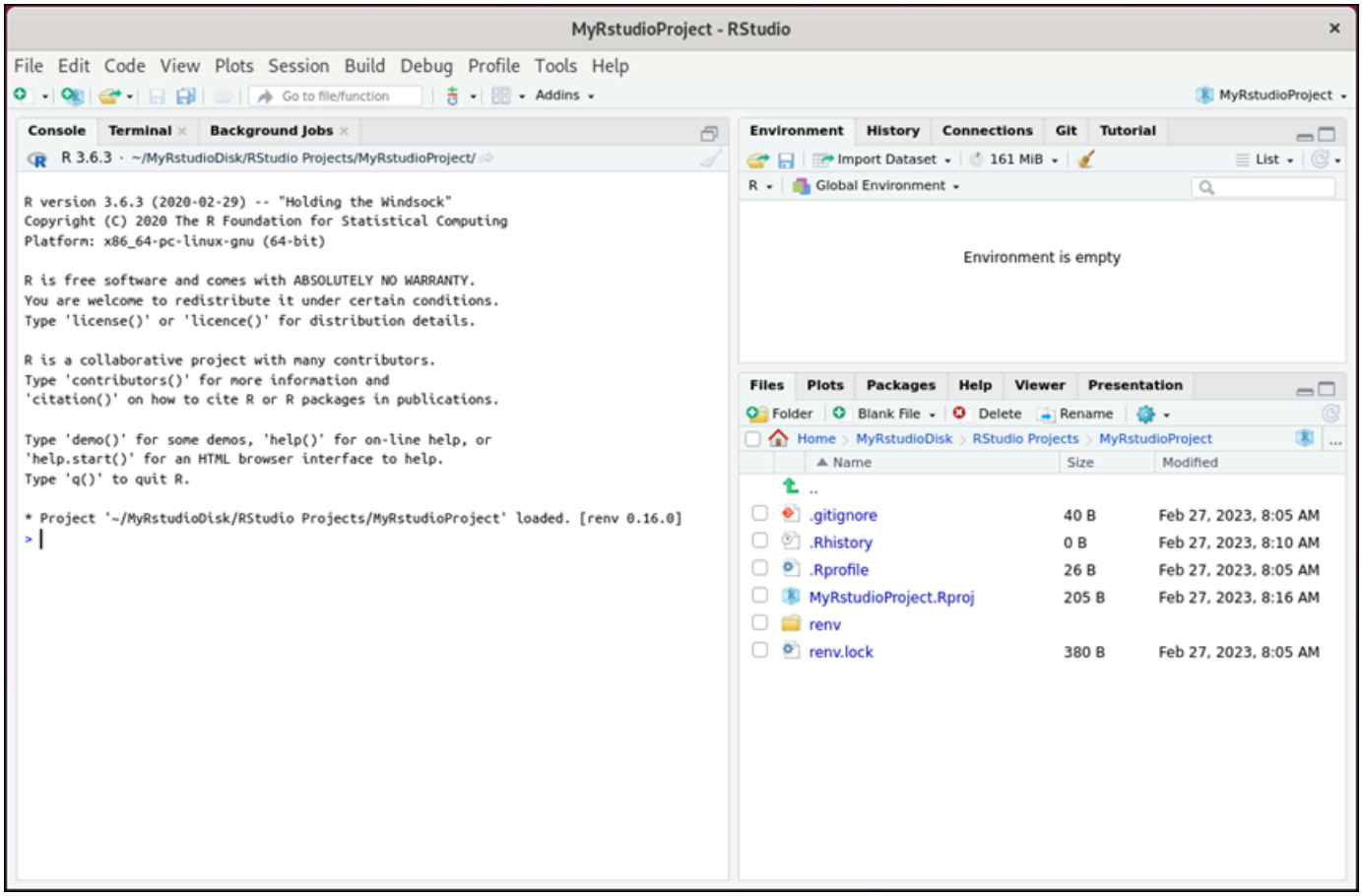
5. RStudio でプロジェクトを開くには、[ファイル] メニューを選択し、[プロジェクトを開く] を選択します。プロジェクトファイルが保存されているディレクトリまたはフォルダに移動します。次に、ファイルを選択して開きます。

   アタッチされているディスクにプロジェクトファイルをアップロードした場合は、ディスクがマウントされているディレクトリを探します。デフォルトでは、Lightsail for Research はディスクを `/home/lightsail-user/<disk-name>` ディレクトリにマウントします。 *<disk-*

name>はディスクに付けた名前です。次の例では、MyRstudioDisk ディレクトリはマウントされたディスクを表し、Projects サブディレクトリには RStudio プロジェクトファイルが含まれています。



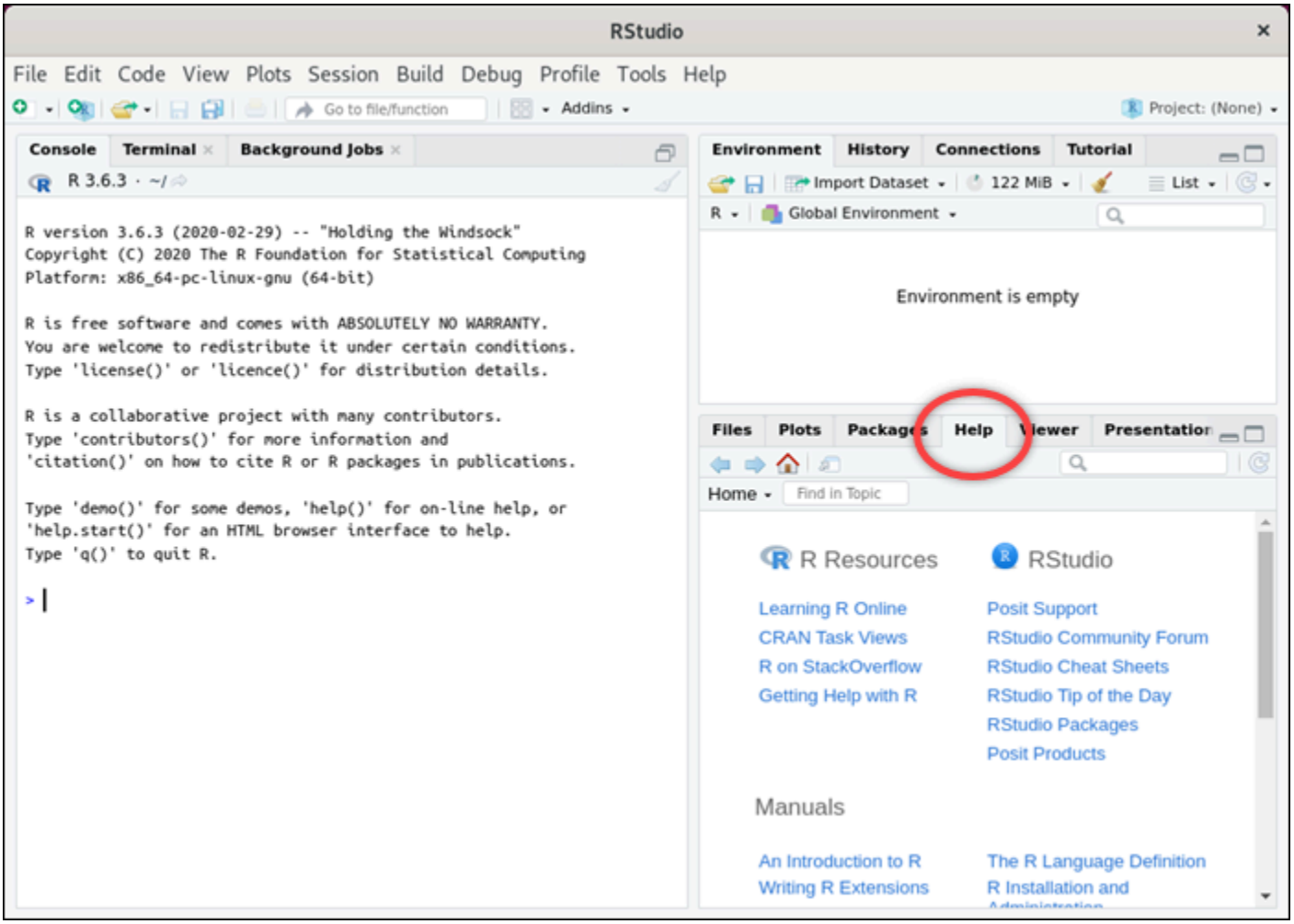
次の例では、MyRstudioProject.Rproj プロジェクトファイルを開きました。



RStudio の使用開始方法については、このチュートリアルの「ステップ 5: RStudio のドキュメントを確認する」セクションに進みます。

ステップ 5: RStudio のドキュメントを確認する

RStudio アプリケーションには、包括的なドキュメントパッケージがバンドルされています。RStudio の学習を始めるには、次の例のように RStudio の [ヘルプ] タブにアクセスすることをおすすめします。



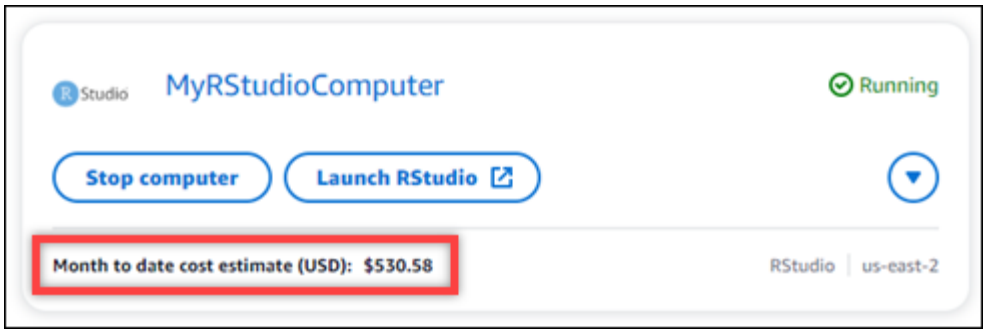
また、以下の RStudio のオンラインリソースも用意されています。

- Learning R Online
- の R StackOverflow
- Getting Help with R
- Posit Support
- RStudio Community Forum
- RStudio Cheat Sheets
- RStudio Tip of the Day (Twitter)
- RStudio Packages

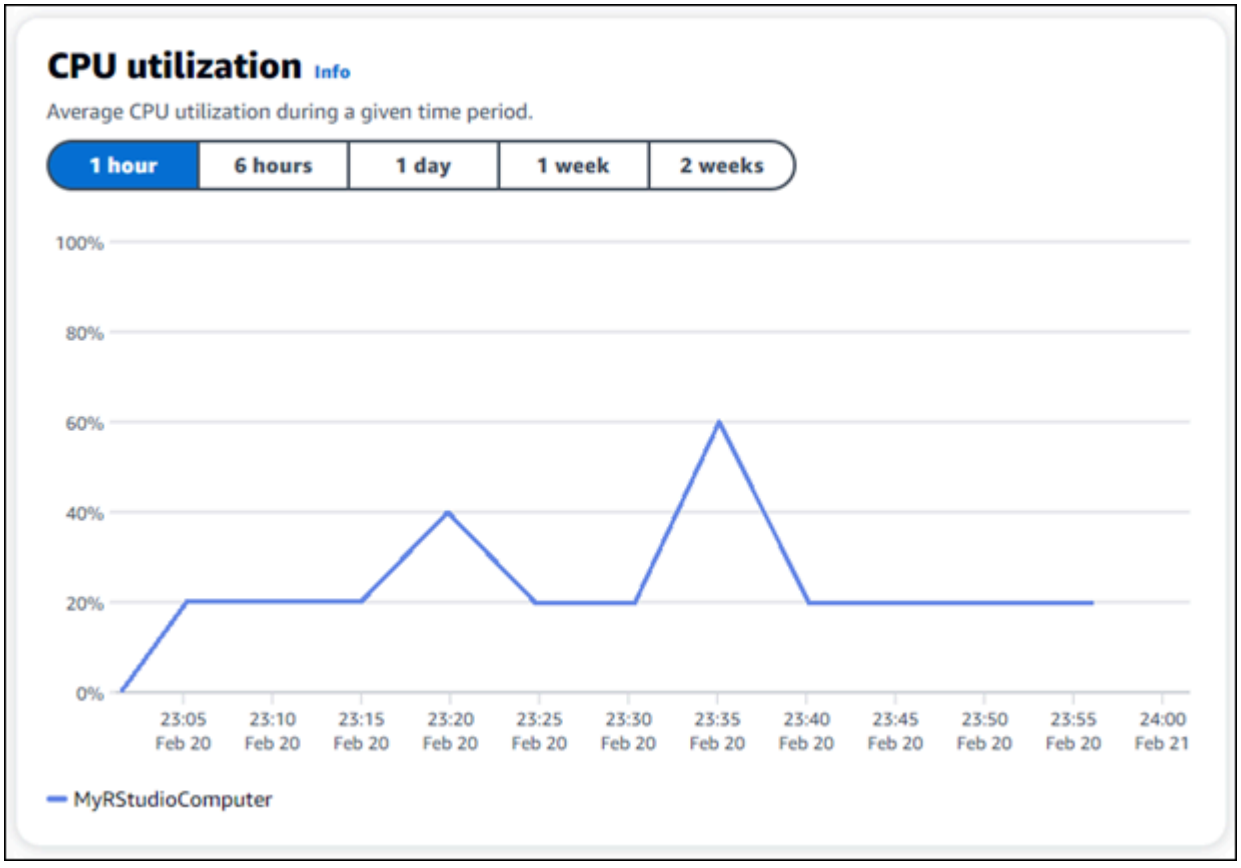
ステップ 6: (オプション) 使用量とコストをモニタリングする

Lightsail for Research リソースの過去 1 か月のコストと使用状況の見積もりは、Lightsail for Research コンソールの次の領域に表示されます。

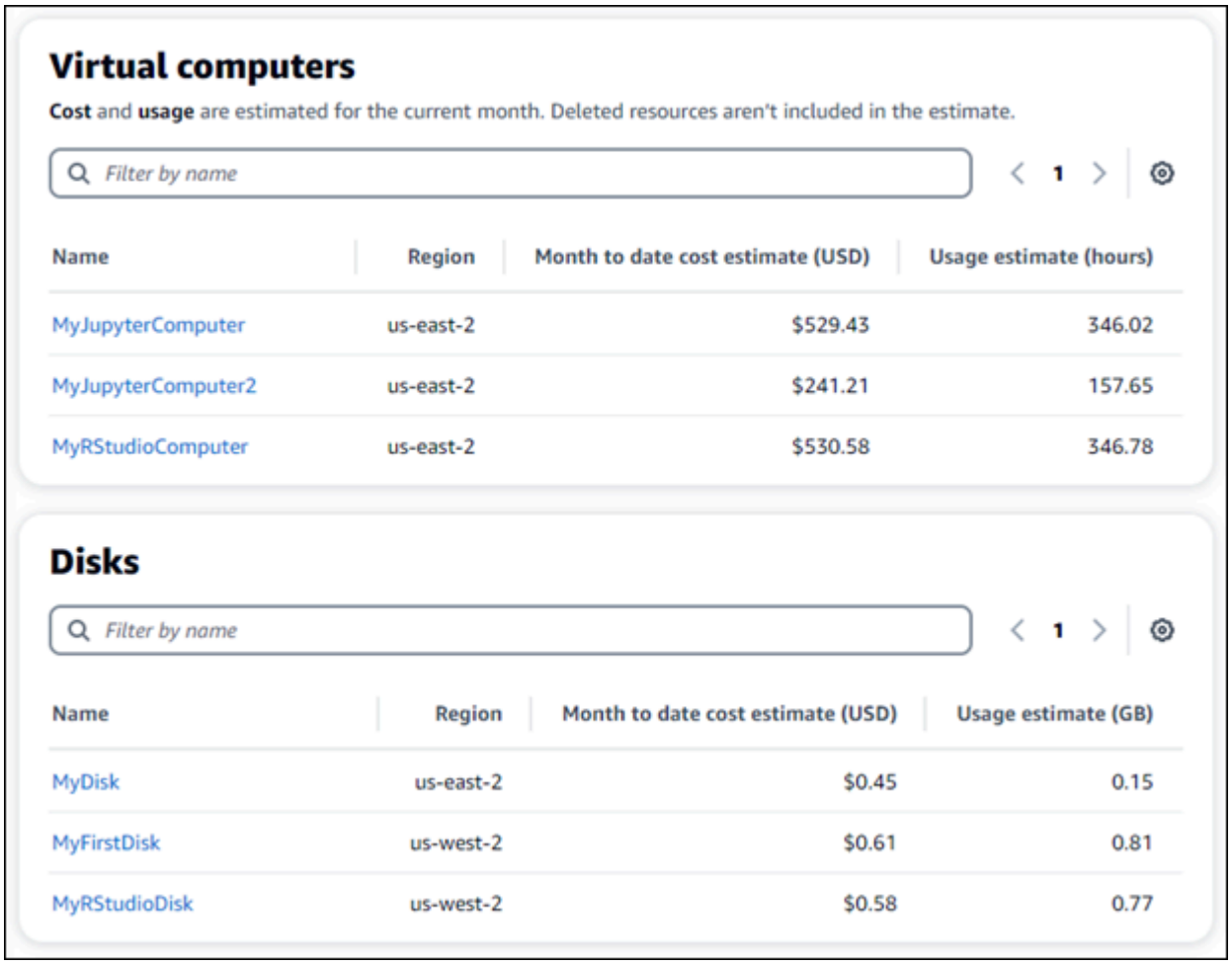
1. Lightsail for Research コンソールのナビゲーションペインで仮想コンピュータを選択します。仮想コンピュータの月初来のコスト見積もりは、実行中の各仮想コンピュータの下に表示されます。



2. 仮想コンピュータの CPU 使用率を表示するには、仮想コンピュータの名前を選択し、[ダッシュボード] タブを選択します。



3. すべての Lightsail for Research リソースの過去 1 か月のコストと使用状況の見積もりを表示するには、ナビゲーションペインで Usage を選択します。



ステップ 7: (オプション) コスト管理ルールを作成する

コスト管理ルールを作成して、仮想コンピュータの使用量とコストを管理します。一定期間に CPU 使用率が指定した割合に達すると実行中のコンピュータを停止する「アイドル状態の仮想コンピュータを停止」ルールを作成できます。例えば、30 分間の CPU 使用率が 5% 以下になると特定のコンピュータを自動的に停止するルールを作成できます。これは、コンピュータがアイドル状態であり、Lightsail for Research がコンピュータを停止して、アイドル状態のリソースに対して料金が発生しないようにすることを意味します。

> **Important**
>
> アイドル状態の仮想コンピュータを停止するルールを作成する前に、その CPU 使用率を数日間モニタリングすることをおすすめします。仮想コンピュータがさまざまな負荷を受けて

いる間の CPU 使用率を記録しておきましょう。例えば、コードのコンパイル時、操作の処理中、アイドリング時などです。これは、ルールの正確なしきい値を決定するのに役立ちます。詳細については、このチュートリアルの「ステップ 6: (オプション) 使用量とコストをモニタリングする」セクションを参照してください。
CPU 使用率のしきい値がワークロードよりも高いルールを作成すると、そのルールによって仮想コンピュータが連続して停止する可能性があります。例えば、ルールによって停止した直後に仮想コンピュータを起動すると、ルールが再びアクティブになり、コンピュータは再び停止します。

コスト管理ルールの作成と管理の詳細な手順は、以下のガイドに記載されています。

- コスト管理
- ルールの作成
- ルールの削除

ステップ 8: (オプション) スナップショットを作成する

スナップショットはデータ point-in-time のコピーです。仮想コンピュータのスナップショットを作成し、それをベースラインとして使用して、新しいコンピュータを作成したり、データをバックアップしたりできます。スナップショットには、コンピュータの復元に必要なすべてのデータ (スナップショットが作成された時点のデータ) が含まれます。

スナップショットの作成と管理の詳細な手順は、以下のガイドに記載されています。

- スナップショットを作成する
- スナップショットを表示する
- スナップショットから仮想コンピュータまたはディスクを作成する
- スナップショットの削除

ステップ 9: (オプション) 仮想コンピュータを停止または削除する

このチュートリアルで作成した仮想コンピュータは、作業完了後に削除することができます。これにより、必要のない仮想コンピュータの料金が発生しなくなります。

仮想コンピュータを削除しても、関連するスナップショットやアタッチされたディスクは削除されません。スナップショットとディスクを作成した場合、料金の発生を停止するには手動で削除する必要があります。

仮想コンピュータを後で使用できるように保存しつつ、標準の時間料金で課金されないために、仮想コンピュータを削除するのではなく停止することができます。これは後で再起動できます。詳細については、「仮想コンピュータの詳細を表示する」を参照してください。料金の詳細については、「Lightsail for Research の料金」を参照してください。

> **Important**
>
> Lightsail for Research リソースの削除は永続的なアクションです。削除されたデータは復元できません。後でデータが必要になる可能性がある場合は、削除する前に仮想コンピュータのスナップショットを作成します。詳細については、「スナップショットを作成する」を参照してください。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[仮想コンピュータ] を選択します。
3. 削除する仮想コンピュータを選択します。
4. [アクション]、[仮想コンピュータを削除] の順に選択します。
5. テキストブロックに「confirm」と入力します。次に、[仮想コンピュータを削除] を選択します。

仮想コンピュータ

Amazon Lightsail for Research では、 で仮想コンピュータを作成できます AWS クラウド。

仮想コンピュータを作成する場合、使用するアプリケーションとハードウェアプランを選択します。仮想コンピュータの使用制限を設定し、仮想コンピュータがその上限に達したときに何が起こるかを選択できます。例えば、設定した予算を超えて請求されることを回避するため、仮想コンピュータを自動的に停止するように選択できます。

> **Important**
>
> 2024 年 3 月 22 日以降、Lightsail for Research 仮想コンピュータにはデフォルトで IMDSv2 が適用されます。

トピック

アプリケーションとハードウェアプラン

Amazon Lightsail for Research 仮想コンピュータを作成するときは、アプリケーションとそのハードウェアプラン (プラン) を選択します。

アプリケーションはソフトウェア構成 (アプリケーションやオペレーティングシステムなど) を提供します。プランは、vCPU の数、メモリ、ストレージ領域、毎月のデータ転送許容量など、仮想コン

ピュータのハードウェアを提供します。アプリケーションとプランが合わさって、仮想コンピュータが構成されます。

> **Note**
>
> 仮想コンピュータを作成した後に、仮想コンピュータのアプリケーションまたはプランを変更することはできません。ただし、仮想コンピュータのスナップショットを作成し、そのスナップショットから新しい仮想コンピュータを作成するときに、新しいプランを選択することはできます。スナップショットの詳細については、「スナップショット」を参照してください。

トピック

アプリケーション

Amazon Lightsail for Research は、仮想コンピュータの起動に必要なアプリケーションとオペレーティングシステムを含むマシンイメージを提供および管理します。Lightsail for Research で仮想コンピュータを作成するときに、アプリケーションのリストからアプリケーションを選択します。Lightsail for Research アプリケーションイメージはすべて Ubuntu (Linux) オペレーティングシステムを使用します。

Lightsail for Research では、以下のアプリケーションを使用できます。

- JupyterLab — JupyterLab は、ノートブック、コード、データ用のウェブベースの統合開発環境 (IDE) です。柔軟なインターフェイスにより、データサイエンス、科学計算、計算ジャーナリズム、機械学習のワークフローの設定や調整ができます。詳細については、「Project Jupyter Documentation」を参照してください。
- RStudio — RStudio は、統計計算やグラフィックス用のプログラミング言語である R、および Python に使用できるオープンソースの統合開発環境 (IDE) です。ソースコードエディタ、ビルド自動化ツール、デバッガーのほか、プロットやワークスペース管理用のツールも統合されています。詳細については、「RStudio IDE」を参照してください。
- VSCodium — VSCodium は、Microsoft 製エディタである VS Code の、コミュニティ主導のバイナリディストリビューションです。詳細については、「VSCodium」を参照してください。

- Scilab — Scilab はオープンソースの数値計算パッケージであり、高レベルの数値指向プログラミング言語です。詳細については、「Scilab」を参照してください。
- Ubuntu 20.04 LTS — Ubuntu は Debian をベースにしたオープンソースの Linux ディストリビューションです。無駄がなく高速でパワフルな Ubuntu Server は、信頼性が高く、予想に沿った経済的なサービスを提供します。これは仮想コンピュータを構築するための基盤として最適です。詳細については、「Ubuntu releases」を参照してください。

プラン

プランはハードウェア仕様を提供し、Lightsail for Research 仮想コンピュータの料金を決定します。プランには、固定量のメモリ (RAM)、コンピューティング (vCPU)、SSD ベースのストレージボリューム (ディスク) 領域、毎月のデータ転送許容量が含まれます。プランは時間単位のオンデマンドで課金されるため、お支払いは仮想コンピュータが実行されている時間に対してのみとなります。

選択するプランは、ワークロードが必要とするリソースに応じて異なる場合があります。Lightsail for Research には、次のプランタイプがあります。

- スタンダード — スタンダードプランはコンピューティングに最適化されており、高パフォーマンスプロセッサから恩恵を受けるコンピューティングバウンドな用途に最適です。
- GPU — GPU プランは、汎用 GPU コンピューティング向けに費用対効果の高パフォーマンスのプラットフォームを提供します。これらのプランを使用すると、サイエンス、エンジニアリング、レンダリング用アプリケーションとワークロードを高速化できます。

スタンダードプラン

Lightsail for Research で利用できる標準プランのハードウェア仕様を次に示します。

プラン名	vCPUs	「メモリ」	ストレージ領域	毎月のデータ転送許容量
スタンダード XL	4	8 GB	50 GB	512 GB
スタンダード 2XL	8	16 GB	50 GB	512 GB
スタンダード 4XL	16	32 GB	50 GB	512 GB

GPU プラン

Lightsail for Research で利用できる GPU プランのハードウェア仕様を次に示します。

プラン名	vCPUs	「メモリ」	ストレージ領域	毎月のデータ転送許容量
GPU XL	4	16 GB	50 GB	1 TB
GPU 2XL	8	32 GB	50 GB	1 TB
GPU 4XL	16	64 GB	50 GB	1 TB

仮想コンピュータを作成する

アプリケーションを実行する Lightsail for Research 仮想コンピュータを作成するには、以下の手順を実行します。

1. Lightsail for Research コンソールにサインインします。
2. ホームページで [仮想コンピュータを作成] を選択します。
3. 物理的な場所に近い仮想コンピュータ AWS リージョン の を選択します。
4. アプリケーションとハードウェアプランを選択します。詳細については、「アプリケーションとハードウェアプラン」を参照してください。
5. 仮想コンピュータの名前を入力します。有効な文字として英数字、数字、ピリオド、ダッシュ、ハイフン、アンダースコアを使用できます。

   仮想コンピュータ名は、次の要件も満たしている必要があります。

   - Lightsail for Research アカウントの各 AWS リージョン 内で一意である必要があります。
   - 2～255 文字であること。
   - 先頭と末尾は英数字または数字を使用すること。
6. [概要] パネルで [仮想コンピュータを作成] を選択します。

数分以内に Lightsail for Research 仮想コンピュータの準備が完了し、グラフィカルユーザーインターフェイス (GUI) セッションを介して接続できます。Lightsail for Research 仮想コンピュータへの接続の詳細については、「」を参照してください仮想コンピュータのアプリケーションを起動する。

> **Important**
>
> 新しく作成された仮想コンピュータは、デフォルトでファイアウォールポートセットが開いています。これらのポートの詳細については、仮想コンピュータのファイアウォールポートを管理する を参照してください。

仮想コンピュータの詳細を表示する

Lightsail for Research アカウントで仮想コンピュータとその詳細のリストを表示するには、次のステップを実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで [仮想コンピュータ] を選択すると、アカウント内の仮想コンピュータのリストが表示されます。

仮想コンピュータの名前を選択すると、その管理ページに移動します。管理ページに表示される情報は次のとおりです。

- 仮想コンピュータ名 — 仮想コンピュータの名前。
- ステータス — 仮想コンピュータには、次のステータスコードのいずれかが表示されます。
  - [作成中]
  - 実行中
  - 停止中
  - 停止
  - 不明
- AWS リージョン – AWS リージョン 仮想コンピュータが作成された場所。
- アプリケーションとハードウェア — 仮想コンピュータのアプリケーションとハードウェアプラン。
- 1 か月あたりの使用量の見積もり — 現在の請求サイクルにおける、この仮想コンピュータの 1 時間あたりの推定使用量。
- 現在までの月の見積もり費用 — この請求サイクルにおける仮想コンピュータの推定コスト (USD)。
- ダッシュボード — [ダッシュボード] タブから、仮想コンピュータのアプリケーションにアクセスするためのセッションを起動できます。CPU 使用率も表示できます。CPU 使用率は、仮想コン

ピュータのアプリケーションが使用する処理能力を特定します。グラフに表示される各データポイントは、一定期間の平均 CPU 使用率を表します。

- コスト管理ルール — 仮想コンピュータの使用状況とコストの管理に役立つように定義するルール。
- 仮想コンピュータの使用状況 — 特定の請求サイクルにおけるコストと使用量の見積もり。これは日付と時刻でフィルタリングできます。
- ストレージ — [ストレージ] タブから仮想コンピュータのディスクを作成、アタッチ、デタッチします。ディスクは、仮想コンピュータにアタッチしてハードドライブとしてマウントできるストレージボリュームです。
- タグ — [タグ] タブから仮想コンピュータのタグを管理します。タグは、 AWS リソースに割り当てるラベルです。各タグは、キー、および値 (オプション) で構成されます。タグを使用して、リソースの検索とフィルタリング、または AWS コストの追跡を行うことができます。

仮想コンピュータのアプリケーションを起動する

Lightsail for Research 仮想コンピュータで実行されているアプリケーションを起動するには、以下の手順を実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[仮想コンピュータ] を選択します。
3. アプリケーションを起動する仮想コンピュータの名前を探します。

> **Note**
>
> 仮想コンピュータが停止している場合は、まず [コンピュータを起動] ボタンを選択して起動します。

4. [アプリケーションを起動] を選択します。例えば、 を起動します JupyterLab。アプリケーションセッションが新しいウェブブラウザウィンドウで開きます。

> **Important**
>
> ウェブブラウザにポップアップブロッカーがインストールされている場合は、セッションを開く前に aws.amazon.com ドメインのポップアップを許可する必要がある場合があります。

仮想コンピュータのオペレーティングシステムにアクセスする

Lightsail for Research 仮想コンピュータのオペレーティングシステムにアクセスするには、以下の手順を実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[仮想コンピュータ] を選択します。
3. 仮想コンピュータの名前を探し、コンピュータのステータスの下にあるアクションボタンのドロップダウンを選択します。

> **Note**
>
> 仮想コンピュータが停止している場合は、まず [スタート] ボタンを選択して仮想コンピュータを起動します。

4. [オペレーティングシステムにアクセス] を選択します。オペレーティングシステムセッションが新しいブラウザウィンドウで開きます。

> **Important**
>
> ウェブブラウザにポップアップブロッカーがインストールされている場合は、セッションを開く前に aws.amazon.com ドメインのポップアップを許可する必要がある場合があります。

仮想コンピュータのファイアウォールポートを管理する

Amazon Lightsail for Research のファイアウォールは、仮想コンピュータへの接続を許可するトラフィックを制御します。仮想コンピュータのファイアウォールに、接続を許可するプロトコル、ポート、送信元 IPv4 または IPv6 アドレスを指定するルールを追加します。ファイアウォールルール

は常にアクセスを許可します。アクセスを拒否するルールを作成することはできません。仮想コンピュータのファイアウォールにルールを追加して、トラフィックが仮想コンピュータに到達できるようにします。各仮想コンピュータにはファイアウォールが 2 つあります。1 つは IPv4 アドレス用、もう 1 つは IPv6 アドレス用です。どちらのファイアウォールも互いに独立しており、インスタンスに入ってくるトラフィックをフィルタリングするルールが事前に設定されています。

プロトコル

プロトコルは、2 台のコンピュータ間でデータを送信する形式です。ファイアウォールルールには次のプロトコルを指定できます。

- Transmission Control Protocol (TCP) は主に、仮想コンピュータで実行されているアプリケーション間の接続を確立して、データの交換が完了するまで接続を維持するために使用されます。これは広く使用されており、ファイアウォールルールで指定することが多いプロトコルです。
- UDP (User Datagram Protocol) は、仮想コンピュータで実行されているアプリケーションとクライアントとの間で低レイテンシーの損失許容接続を確立するために主に使用します。ゲーム、音声、ビデオ通信など、体感レイテンシーの重要度が高いネットワークアプリケーションに最適です。
- ICMP (Internet Control Message Protocol) は、ネットワーク通信の問題を診断するために主に使用します。たとえば、データが送信先にタイムリーに到着しているかどうかを確認します。このプロトコルは Ping ユーティリティに最適です。このユーティリティでは、ローカルコンピュータと仮想コンピュータ間の接続速度をテストできます。データが仮想コンピュータに到着してローカルコンピュータに戻ってくるまでの所要時間をレポートします。
- [すべて] では、仮想コンピュータへのすべてのプロトコルトラフィックの流入を許可します。どのプロトコルを指定すればよいかわからない場合は、このプロトコルを指定します。これには、ここで示したプロトコルだけではなく、すべてのインターネットプロトコルが含まれます。詳細については、「Protocol Numbers」(Internet Assigned Numbers Authority ウェブサイト) を参照してください。

ポート

コンピュータがキーボードやポインタなどの周辺機器と通信するためのコンピュータの物理ポートと同様に、ファイアウォールポートは仮想コンピュータのインターネット通信エンドポイントとして機能します。クライアントは、仮想コンピュータとの接続時に、通信を確立するためのポートを公開します。

ファイアウォールルールで指定できるポートの範囲は 0～65535 です。クライアントが仮想コンピュータとの接続を確立できるようにするファイアウォールルールを作成する場合は、使用するプロトコルを指定します。また、接続を確立できるポート番号と、接続の確立が許可された IP アドレスも指定します。

新しく作成された仮想コンピュータでは、以下のポートがデフォルトで開いています。

- TCP
  - 22 - Secure Shell (SSH) に使用されます。
  - 80 - Hypertext Transfer Protocol (HTTP) に使用されます。
  - 443 - Hypertext Transfer Protocol Secure (HTTPS) に使用されます。
  - 8443 - Hypertext Transfer Protocol Secure (HTTPS) に使用されます。

ポートを開閉する理由

ポートを開くと、クライアントが仮想コンピュータとの接続を確立できるようになります。ポートを閉じると、仮想コンピュータへの接続がブロックされます。たとえば、SSH クライアントが仮想コンピュータに接続できるようにするには、接続を確立する必要があるコンピュータの IP アドレスからのみポート 22 経由の TCP を許可するファイアウォールルールを構成します。この場合は、任意の IP アドレスからの仮想コンピュータへの SSH 接続を確立を許可しないようにする必要があります。これを許可すると、セキュリティ上のリスクが生じる可能性があります。このルールがインスタンスのファイアウォールですでに設定されている場合は、このルールを削除して、SSH クライアントが仮想コンピュータに接続できないように設定できます。

以下の手順は、仮想コンピュータ上で現在開いているポートを取得する方法、新しいポートを開く方法、ポートを閉じる方法を示しています。

トピック

前提条件を満たす

開始する前に、前提条件として次の作業を完了します。

- Lightsail for Research で仮想コンピュータを作成します。詳細については、「仮想コンピュータを作成する」を参照してください。
- AWS Command Line Interface () をダウンロードしてインストールしますAWS CLI。詳細については、「AWS Command Line Interface バージョン 2 用ユーザーガイド」の「AWS CLIの最新バージョンを使用してインストールまたは更新を行う」を参照してください。
- にアクセスする AWS CLI ように を設定します AWS アカウント。詳細については、「AWS Command Line Interface バージョン 2 用ユーザーガイド」の「Configuration basics」を参照してください。

仮想コンピュータのポート状態を取得する

仮想コンピュータのポート状態を取得するには、以下の手順を実行します。この手順では、 `get-instance-port-states` AWS CLI コマンドを使用して、特定の Lightsail for Research 仮想コンピュータのファイアウォールポート状態、ポートを介して仮想コンピュータに接続できる IP アドレス、および プロトコルを取得します。詳細については、AWS CLI コマンドリファレンスの get-instance-port-states を参照してください。

1. この手順はローカルコンピュータのオペレーティングシステムによって決まります。

   - ローカルコンピュータで Windows オペレーティングシステムを使用している場合は、コマンドプロンプトウィンドウを開きます。
   - ローカルコンピュータが Linux または Unix ベースのオペレーティングシステム (macOS を含む) を使用している場合は、ターミナルウィンドウを開きます。

2. 次のコマンドを入力して、ファイアウォールのポート状態、許可されている IP アドレス、プロトコルを取得します。コマンドでは、*`REGION`* を、仮想コンピュータが作成された AWS リージョンのコード (`us-east-2` など) に置き換えます。*`NAME`* の部分はお客様の仮想コンピュータ名に置き換えます。

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

   例

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

応答には、開いているポートおよびプロトコル、仮想コンピュータへの接続が許可されている IP CIDR 範囲が表示されます。

```
[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
```

ポートを開く方法については、次のセクションに進んでください。

仮想コンピュータのポートを開く

仮想コンピュータのポートを開くには、以下の手順を実行します。この手順では、 `open-instance-public-ports` AWS CLI コマンドを使用します。ファイアウォールポートを開いて、信頼できる IP アドレスまたは IP アドレス範囲からの接続確立を許可します。例えば、IP アドレス `192.0.2.44` を許可するには、`192.0.2.44` または `192.0.2.44/32` を指定します。IP アドレス `192.0.2.0`～`192.0.2.255` を許可するには、`192.0.2.0/24` を指定します。詳細については、AWS CLI コマンドリファレンスの open-instance-public-ports を参照してください。

1. この手順はローカルコンピュータのオペレーティングシステムによって決まります。

   - ローカルコンピュータで Windows オペレーティングシステムを使用している場合は、コマンドプロンプトウィンドウを開きます。
   - ローカルコンピュータが Linux または Unix ベースのオペレーティングシステム (macOS を含む) を使用している場合は、ターミナルウィンドウを開きます。

2. 以下のコマンドを入力してポートを開きます。

   コマンドでは、次の項目を置き換えます。

   - を、 などの仮想コンピュータが作成された AWS リージョンのコード*REGION*に置き換えますus-east-2。

- *NAME* の部分はお客様の仮想コンピュータ名に置き換えます。
- *FROM-PORT* を、開くポートの範囲で最初のポートに置き換えます。
- *PROTOCOL* を IP プロトコル名に置き換えます。(例: TCP)。
- *TO-PORT* を、開くポートの範囲で最後のポートに置き換えます。
- *IP* を、仮想コンピュータへの接続を許可する IP アドレスまたは IP アドレスの範囲に置き換えます。

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

例

```
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
```

応答には、新しく追加されたポート、プロトコル、仮想コンピュータへの接続が許可されている IP CIDR 範囲が表示されます。

```
[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"
    }
}
```

ポートを閉じる方法については、次のセクションに進んでください。

仮想コンピュータのポートを閉じる

仮想コンピュータのポートを閉じるには、以下の手順を実行します。この手順では、 `close-instance-public-ports` AWS CLI コマンドを使用します。詳細については、AWS CLI コマンドリファレンスの close-instance-public-ports を参照してください。

1. この手順はローカルコンピュータのオペレーティングシステムによって決まります。

   - ローカルコンピュータで Windows オペレーティングシステムを使用している場合は、コマンドプロンプトウィンドウを開きます。
   - ローカルコンピュータが Linux または Unix ベースのオペレーティングシステム (macOS を含む) を使用している場合は、ターミナルウィンドウを開きます。

2. 次のコマンドを入力してポートを閉じます。

   コマンドでは、次の項目を置き換えます。

   - を、 などの仮想コンピュータが作成された AWS リージョンのコード*REGION*に置き換えますus-east-2。
   - *NAME* の部分はお客様の仮想コンピュータ名に置き換えます。
   - *FROM-PORT* を、閉じるポートの範囲で最初のポートに置き換えます。
   - *PROTOCOL* を IP プロトコル名に置き換えます。(例: TCP)。
   - *TO-PORT* を、閉じるポートの範囲で最後のポートに置き換えます。
   - *IP* を、削除する IP アドレスまたは IP アドレスの範囲に置き換えます。

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

   例

   ```
   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
   ```

   応答には、閉じたポートおよびプロトコル、仮想コンピュータへの接続が許可されなくなった IP CIDR 範囲が表示されます。

```
[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"
    }
}
```

次のステップに進みます

仮想コンピュータのファイアウォールポートを正常に設定したら、次の追加手順を実行できます。

- 仮想コンピュータのキーペアを取得します。キーペアを使用すると、OpenSSH、PuTTY、Linux 用 Windows サブシステムなど、多数の SSH クライアントを使用して接続を確立できます。詳細については、「仮想コンピュータのキーペアを取得する」を参照してください。
- SSH を使用して仮想コンピュータに接続し、コマンドラインを使用して管理します。詳細については、「Secure Copy を使用してファイルを仮想コンピュータに転送する」を参照してください。
- SCP を使用して仮想コンピュータに接続し、ファイルを安全に転送します。詳細については、「Secure Copy を使用してファイルを仮想コンピュータに転送する」を参照してください。

仮想コンピュータのキーペアを取得する

キーペアは、パブリックキーとプライベートキーで構成され、Amazon Lightsail for Research 仮想コンピュータに接続するときにアイデンティティを証明するために使用する一連のセキュリティ認証情報です。パブリックキーは Lightsail for Research の各仮想コンピュータに保存され、プライベートキーはローカルコンピュータに保持されます。プライベートキーにより、仮想コンピュータとの Secure Shell Protocol (SSH) を安全に確立できます。プライベートキーを使用すれば、誰でも仮想コンピュータに接続できてしまうため、プライベートキーは安全な場所に保存することが重要です。

Lightsail インスタンスまたは Lightsail for Research 仮想コンピュータを初めて作成すると、Amazon Lightsail のデフォルトキーペア (DKP) が自動的に作成されます。DKP は、インスタンスまたは仮想コンピュータを作成する各 AWS リージョンに固有です。例えば、米国東部 (オハイオ) リージョン (米国東部-2) の Lightsail DKP は、作成時に DKP を使用するように設定された Lightsail お

よび Lightsail for Research で米国東部 (オハイオ) に作成するすべてのコンピュータに適用されます。Lightsail for Research は、作成した仮想コンピュータに DKP のパブリックキーを自動的に保存します。Lightsail サービスへの API コールを実行することで、DKP のプライベートキーをいつでもダウンロードできます。

このドキュメントでは、仮想コンピュータの DKP を取得する方法を説明します。DKP を取得すると、OpenSSH、PuTTY、Linux 用 Windows サブシステムなど、多数の SSH クライアントを使用して接続を確立できます。Secure Copy (SCP) を使用して、ローカルコンピュータから仮想コンピュータにファイルを安全に転送することもできます。

> **Note**
>
> ブラウザベースの NICE DCV クライアントを使用して、仮想コンピュータへのリモートディスプレイプロトコル接続を確立することもできます。NICE DCV は Lightsail for Research コンソールで使用できます。その RDP クライアントでは、コンピュータのキーペアを取得する必要はありません。詳細については、仮想コンピュータのアプリケーションを起動するおよび仮想コンピュータのオペレーティングシステムにアクセスするを参照してください。

トピック

前提条件を満たす

開始する前に、前提条件として次の作業を完了します。

- Lightsail for Research で仮想コンピュータを作成します。詳細については、「仮想コンピュータを作成する」を参照してください。
- AWS Command Line Interface () をダウンロードしてインストールしますAWS CLI。詳細については、「AWS Command Line Interface バージョン 2 用ユーザーガイド」の「AWS CLIの最新バージョンを使用してインストールまたは更新を行う」を参照してください。
- にアクセスする AWS CLI ように を設定します AWS アカウント。詳細については、「AWS Command Line Interface バージョン 2 用ユーザーガイド」の「Configuration basics」を参照してください。

- jq をダウンロードおよびインストールします。これは軽量で柔軟性の高いコマンドライン JSON プロセッサです。次の手順で使用して、 AWS CLIの JSON 出力からキーペアの詳細を抽出します。jq のダウンロードとインストールについて、詳しくは、jq ウェブサイトの「Download jq」を参照してください。

仮想コンピュータのキーペアを取得する

Lightsail for Research で仮想コンピュータの Lightsail DKP を取得するには、次のいずれかの手順を実行します。

Windows ローカルコンピュータを使用して仮想コンピュータのキーペアを取得する

この手順は、ローカルコンピュータが Windows オペレーティングシステムを使用している場合に適用されます。この手順では、 `download-default-key-pair` AWS CLI コマンドを使用して、AWS リージョンの Lightsail DKP を取得します。詳細については、AWS CLI コマンドリファレンスの download-default-key-pair を参照してください。

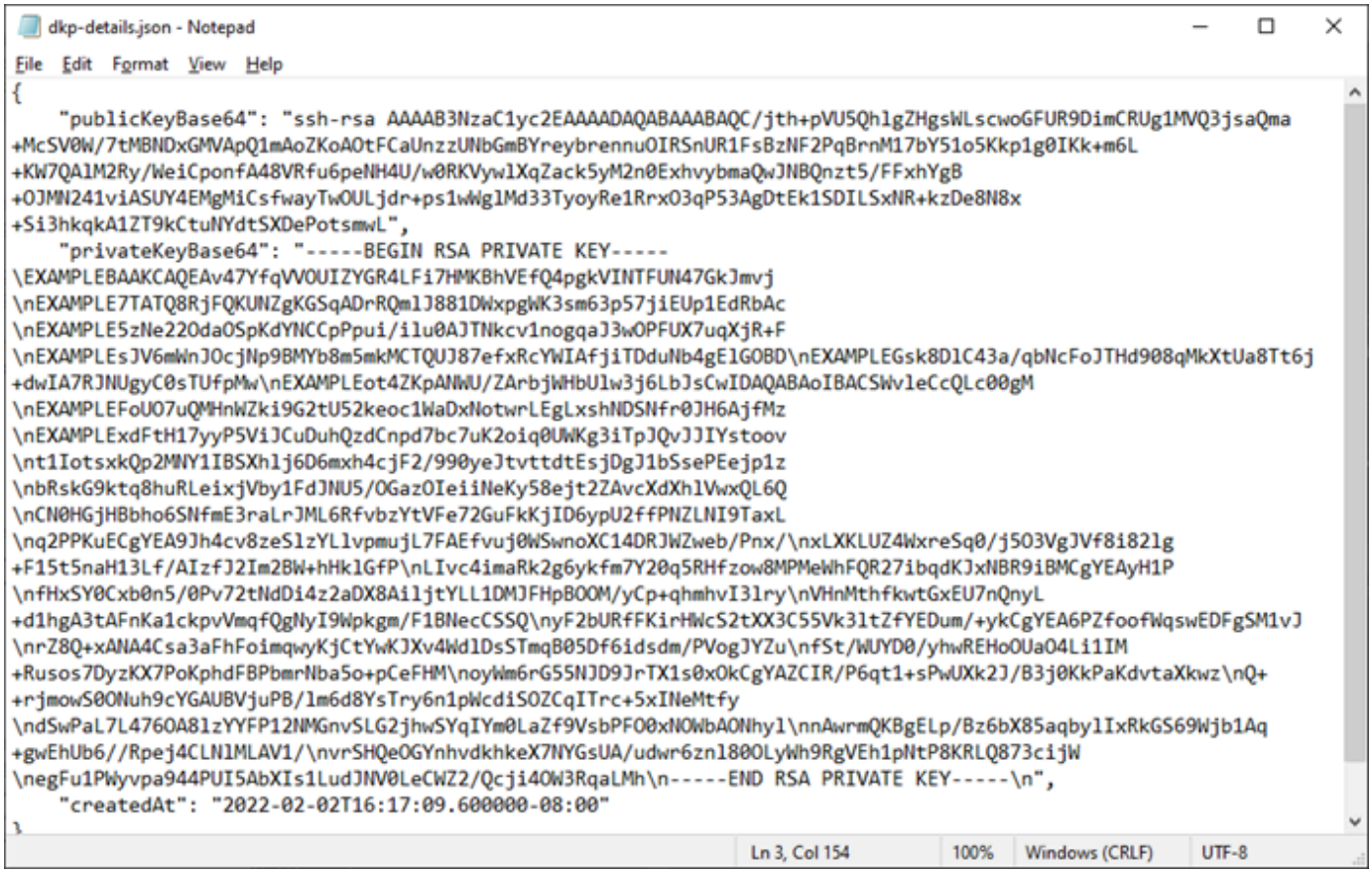
1. [コマンドプロント] ウィンドウを開きます。
2. 次のコマンドを入力して、特定の AWS リージョンの Lightsail DKP を取得します。このコマンドは、情報を `dkp-details.json` ファイルに保存します。コマンドで、 を などの仮想コンピュータが作成された AWS リージョンのコード*`region-code`*に置き換えます`us-east-2`。

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

   例

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

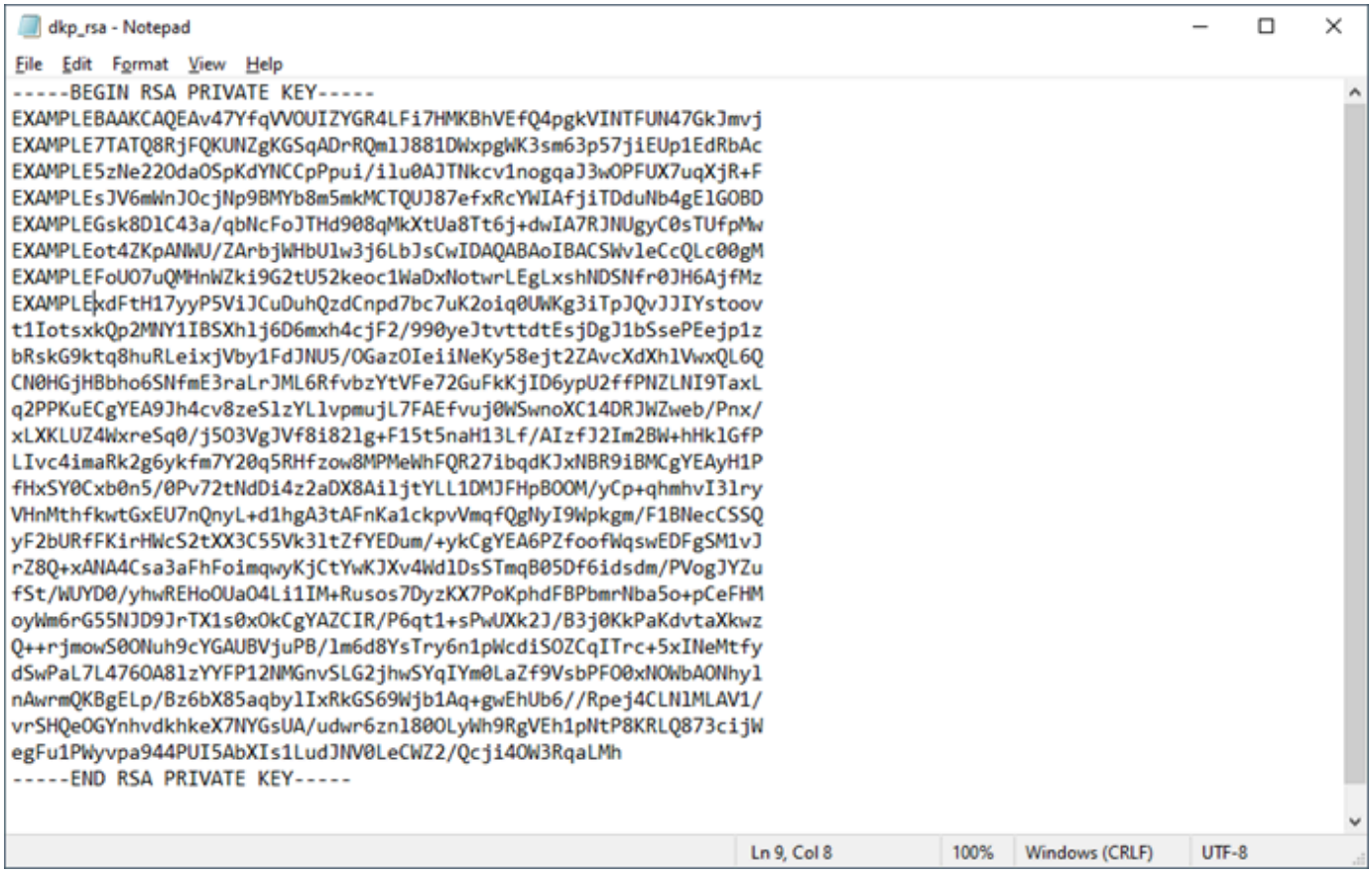
   コマンドには応答がありません。コマンドが成功したかどうかを確認するには、 `dkp-details.json` ファイルを開き、Lightsail DKP 情報が保存されたかどうかを確認します。`dkp-details.json` ファイルの内容は次の例のようになります。ファイルが空の場合、コマンドは失敗しています。



3. 次のコマンドを入力して、dkp-details.json ファイルからプライベートキー情報を抽出し、新しい dkp_rsa プライベートキーファイルに追加します。

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

コマンドには応答がありません。コマンドが成功したかどうかを知るには、dkp_rsa ファイルを開いて情報が含まれているかどうかを確認します。dkp_rsa ファイルの内容は次の例のようになります。ファイルが空の場合、コマンドは失敗しています。



これで、仮想コンピュータへの SSH または SCP 接続の確立に必要なプライベートキーを取得しました。次の追加ステップについては、次のセクションに進みます。

Linux、Unix、macOS ローカルコンピュータを使用して仮想コンピュータのキーペアを取得する

この手順は、ローカルコンピュータが Linux、Unix、macOS オペレーティングシステムを使用している場合に適用されます。この手順では、 `download-default-key-pair` AWS CLI コマンドを使用して、 AWS リージョンの Lightsail DKP を取得します。詳細については、AWS CLI コマンドリファレンスの download-default-key-pair を参照してください。

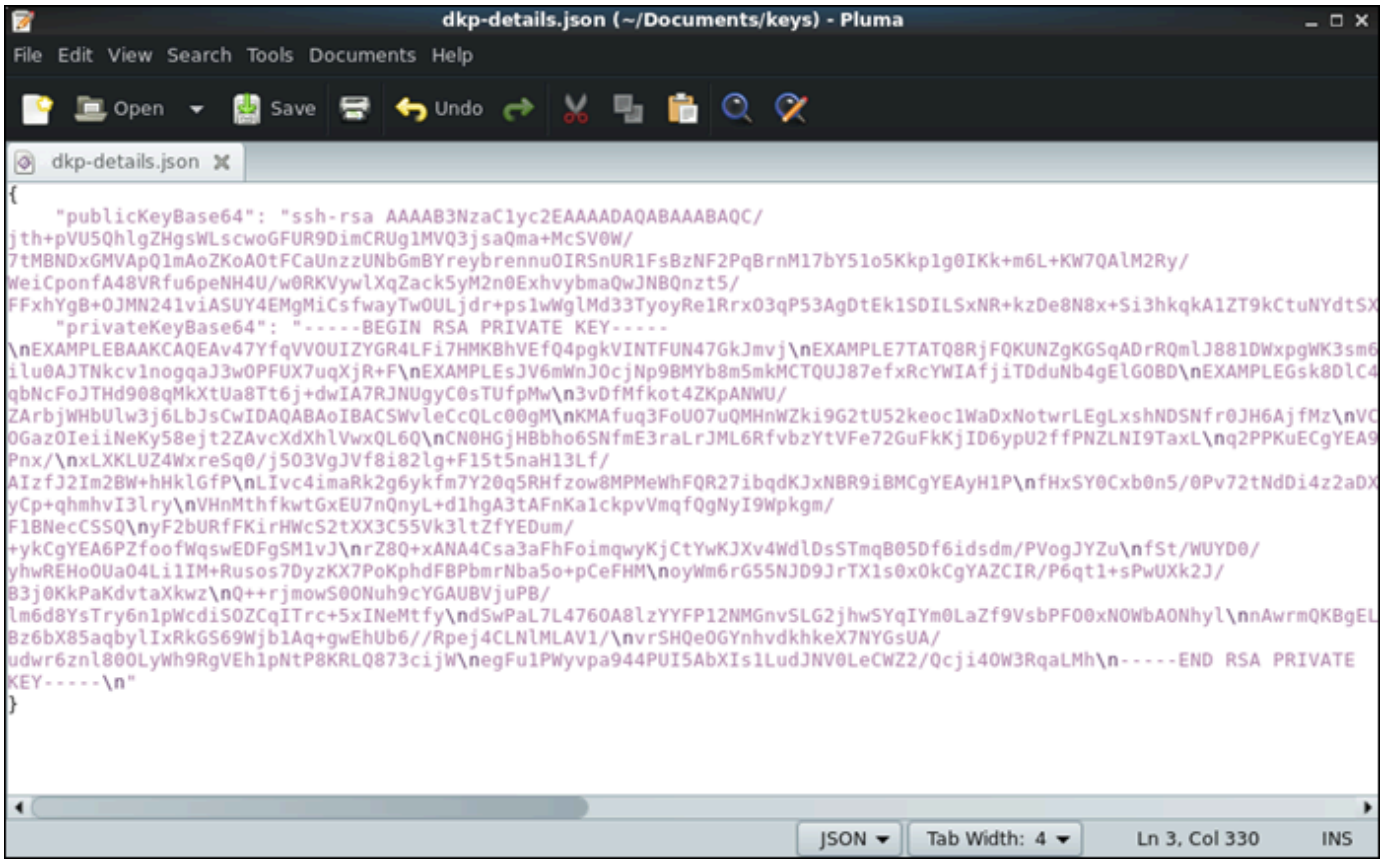
1. ターミナルウィンドウを開きます。
2. 次のコマンドを入力して、特定の AWS リージョンの Lightsail DKP を取得します。このコマンドは、情報を `dkp-details.json` ファイルに保存します。コマンドで、 を などの仮想コンピュータが作成された AWS リージョンのコード*`region-code`*に置き換えます`us-east-2`。

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

例

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

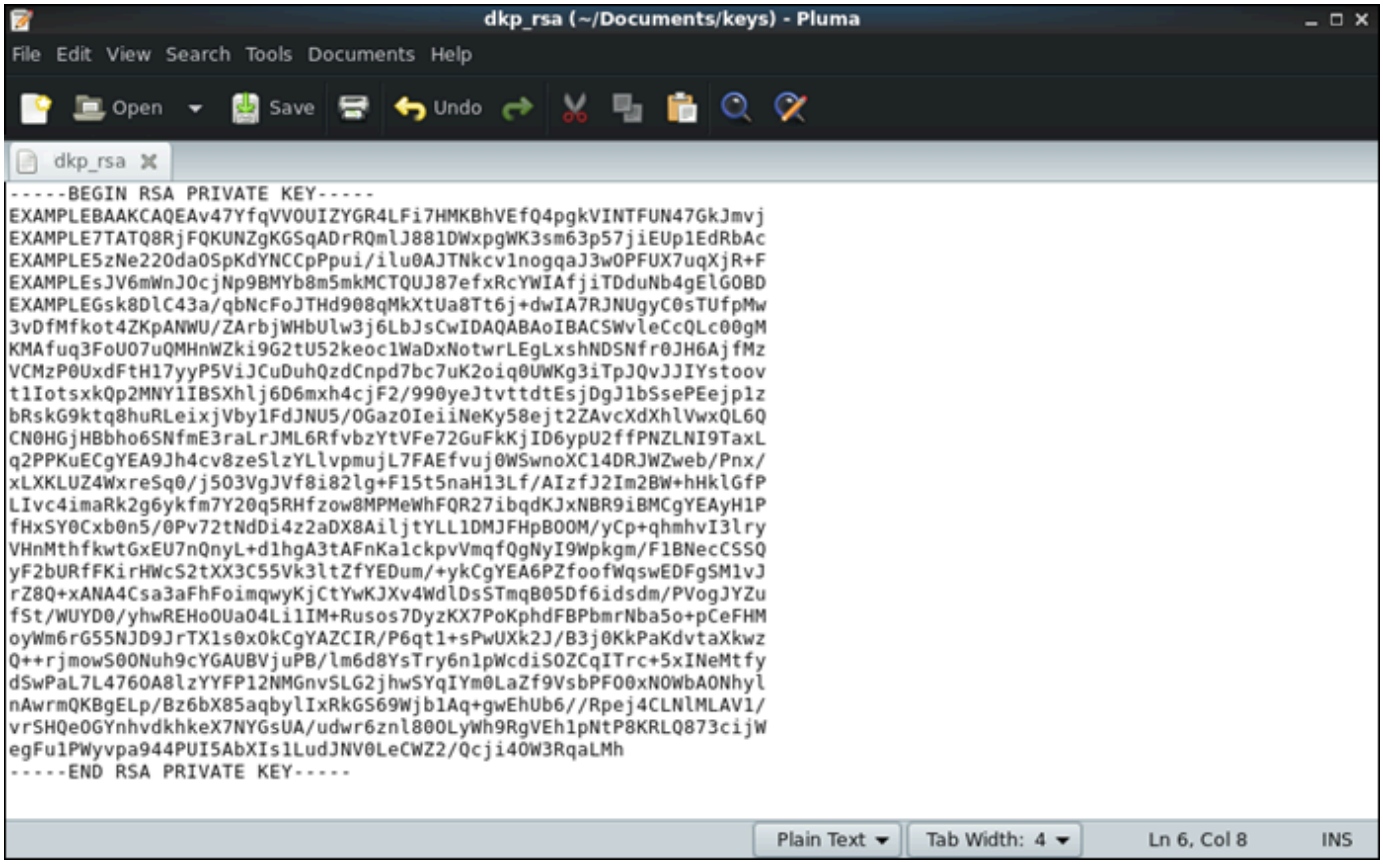
コマンドには応答がありません。コマンドが成功したかどうかを確認するには、 dkp-details.json ファイルを開き、Lightsail DKP 情報が保存されたかどうかを確認します。dkp-details.json ファイルの内容は次の例のようになります。ファイルが空の場合、コマンドは失敗しています。



3. 次のコマンドを入力して、dkp-details.json ファイルからプライベートキー情報を抽出し、新しい dkp_rsa プライベートキーファイルに追加します。

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

コマンドには応答がありません。コマンドが成功したかどうかを知るには、dkp_rsa ファイルを開いて情報が含まれているかどうかを確認します。dkp_rsa ファイルの内容は次の例のようになります。ファイルが空の場合、コマンドは失敗しています。



4. dkp_rsa ファイルのアクセス許可を設定するには、次のコマンドを入力します。

```
chmod 600 dkp_rsa
```

これで、仮想コンピュータへの SSH または SCP 接続の確立に必要なプライベートキーを取得しました。次の追加ステップについては、次のセクションに進みます。

次のステップに進みます

仮想コンピュータのキーペアを正常に取得したら、次の追加のステップを実行できます。

- SSH を使用して仮想コンピュータに接続し、コマンドラインを使用して管理します。詳細については、「Secure Shell を使用して仮想コンピュータに接続する」を参照してください。
- SCP を使用して仮想コンピュータに接続し、ファイルを安全に転送します。詳細については、「Secure Copy を使用してファイルを仮想コンピュータに転送する」を参照してください。

Secure Shell を使用して仮想コンピュータに接続する

Secure Shell Protocol (SSH) を使用して、Amazon Lightsail for Research の仮想コンピュータに接続できます。SSH を使用して仮想コンピュータをリモート管理できるため、インターネット経由でコンピュータにサインインしてコマンドを実行できます。

> **Note**
>
> ブラウザベースの NICE DCV クライアントを使用して、仮想コンピュータへのリモートディスプレイプロトコル接続を確立することもできます。NICE DCV は Lightsail for Research コンソールで使用できます。詳細については、「仮想コンピュータのオペレーティングシステムにアクセスする」を参照してください。

トピック

前提条件を満たす

開始する前に、前提条件として次の作業を完了します。

- Lightsail for Research で仮想コンピュータを作成します。詳細については、「仮想コンピュータを作成する」を参照してください。
- 接続する仮想コンピュータが動作状態であることを確認します。また、仮想コンピュータの名前と、仮想コンピュータが作成された AWS リージョンを書き留めます。この情報は、このプロセスの後半で必要になります。詳細については、「仮想コンピュータの詳細を表示する」を参照してください。
- 接続する仮想コンピュータのポート 22 が開いていることを確認します。これは SSH で使用されるデフォルトのポートです。デフォルトでは開いています。ただし、閉じている場合は、次に進む前に再度開く必要があります。詳細については、「仮想コンピュータのファイアウォールポートを管理する」を参照してください。
- 仮想コンピュータの Lightsail デフォルトキーペア (DKP) を取得します。詳細については、「仮想コンピュータのキーペアを取得する」を参照してください。

> **Tip**
>
> AWS CloudShell を使用して仮想コンピュータに接続する場合は、次のセクションを使用して仮想コンピュータに接続する AWS CloudShellの「」を参照してください。詳細については、「AWS とは CloudShell」を参照してください。それ以外の場合は、次の前提条件に進みます。

- AWS Command Line Interface () をダウンロードしてインストールしますAWS CLI。詳細については、「AWS Command Line Interface バージョン 2 用ユーザーガイド」の「AWS CLIの最新バージョンを使用してインストールまたは更新を行う」を参照してください。
- にアクセスする AWS CLI ように を設定します AWS アカウント。詳細については、「AWS Command Line Interface バージョン 2 用ユーザーガイド」の「Configuration basics」を参照してください。
- jq をダウンロードおよびインストールします。これは軽量で柔軟性の高いコマンドライン JSON プロセッサです。次の手順で使用して、キーペアの詳細を抽出します。jq のダウンロードとインストールについて、詳しくは、jq ウェブサイトの「Download jq」を参照してください。

SSH を使用して仮想コンピュータに接続する

Lightsail for Research で仮想コンピュータへの SSH 接続を確立するには、次のいずれかの手順を実行します。

を使用して仮想コンピュータに接続する AWS CloudShell

この手順は、仮想コンピュータへの接続に最小限のセットアップを希望する場合に適用されます。は、 から直接起動できるブラウザベースの事前認証済みシェル AWS CloudShell を使用します AWS Management Console。Bash、Z シェルなど PowerShell、任意のシェルを使用してコマンドを実行できます AWS CLI 。この手順は、コマンドラインツールのダウンロードもインストールも不要です。詳細については、「AWS CloudShell ユーザーガイド」の「AWS CloudShellの使用開始」を参照してください。

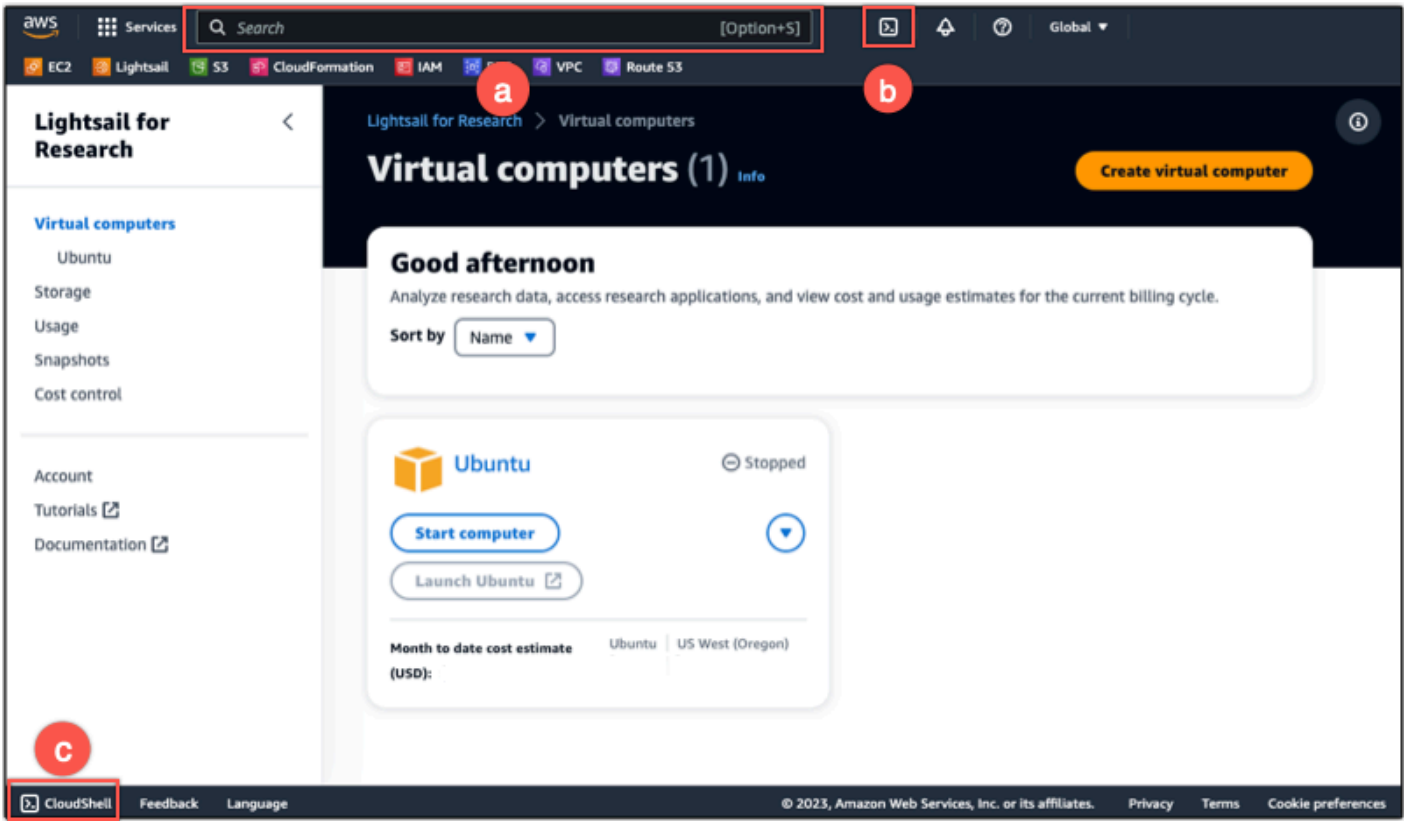
> **Important**
>
> 開始する前に、接続先の仮想コンピュータの Lightsail デフォルトキーペア (DKP) を取得してください。詳細については、「仮想コンピュータのキーペアを取得する」を参照してください。

1. Lightsail for Research コンソールから、次のいずれかのオプション CloudShell を選択して を起動します。

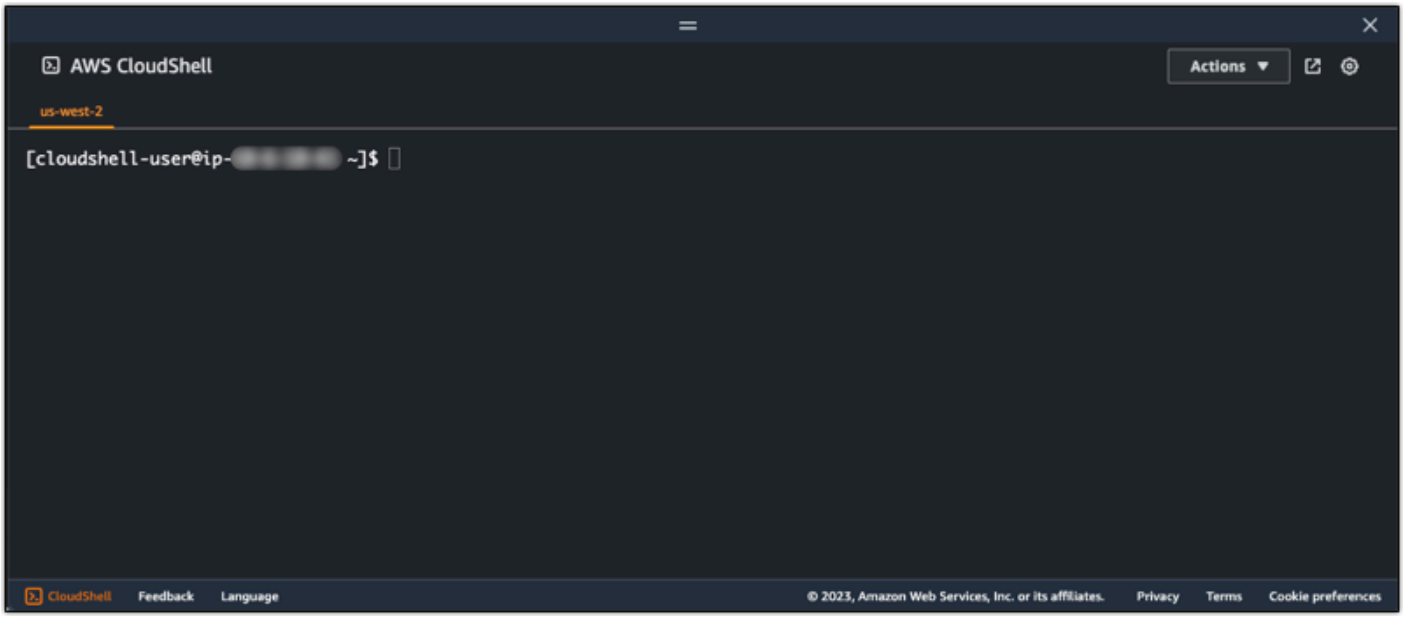
   a. 検索ボックスにCloudShell「」と入力し、 を選択しますCloudShell。

   b. ナビゲーションバーで、 CloudShell アイコンを選択します。

   c. コンソールの左下にあるコンソールツールバーCloudShellで を選択します。



コマンドプロンプトが表示されたら、シェルは対話的な操作の準備ができています。



2. 使用するプリインストールされたシェルを選択します。デフォルトのシェルを変更するには、コマンドラインプロンプトで次のいずれかのプログラム名を入力します。 Bashは、 の起動時に実行されるデフォルトのシェルです AWS CloudShell。

   Bash

   ```
   bash
   ```

   Bash に切り替えると、コマンドプロンプトの記号が $ に更新します。

   PowerShell

   ```
   pwsh
   ```

   に切り替えると PowerShell、コマンドプロンプトの記号が に更新されますPS>。

   Z shell

   ```
   zsh
   ```

   Z shell に切り替えると、コマンドプロンプトの記号が % に更新します。

3. CloudShell ターミナルウィンドウから仮想コンピュータに接続するには、「」を参照してくださいLinux、Unix、macOS ローカルコンピュータで SSH を使用して仮想コンピュータに接続する。

環境にプリインストールされているソフトウェア CloudShellの詳細については、AWS CloudShell「 ユーザーガイド」の「 AWS CloudShell コンピューティング環境」を参照してください。

Windows ローカルコンピュータで SSH を使用して仮想コンピュータに接続する

この手順は、ローカルコンピュータが Windows オペレーティングシステムを使用している場合に適用されます。この手順では、 `get-instance` AWS CLI コマンドを使用して、接続するインスタンスのユーザー名とパブリック IP アドレスを取得します。詳細については、「AWS CLI コマンドリファレンス」の「get-instance」を参照してください。

> **Important**
>
> この手順を開始する前に、接続しようとしている仮想コンピュータの Lightsail のデフォルトキーペア (DKP) を取得していることを確認してください。詳細については、「仮想コンピュータのキーペアを取得する」を参照してください。この手順では、Lightsail DKP のプライベートキーを、次のいずれかのコマンドで使用されるdkp_rsaファイルに出力します。

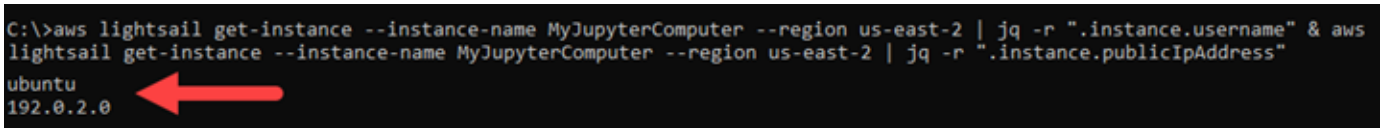
1. [コマンドプロント] ウィンドウを開きます。
2. 次のコマンドを入力すると、仮想コンピュータのパブリック IP アドレスとユーザー名が表示されます。コマンドで、 を などの仮想コンピュータ AWS リージョン が作成された のコードに置き換えますus-east-2。*computer-name* の部分は接続する仮想コンピュータの名前に置き換えます。*region-code*

```
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"
```

例

```
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"
```

以下の例に示すように、応答では、仮想コンピュータのユーザー名とパブリック IP アドレスを表示します。これらの値は、この手順の次のステップで必要になるため、記録しておいてください。



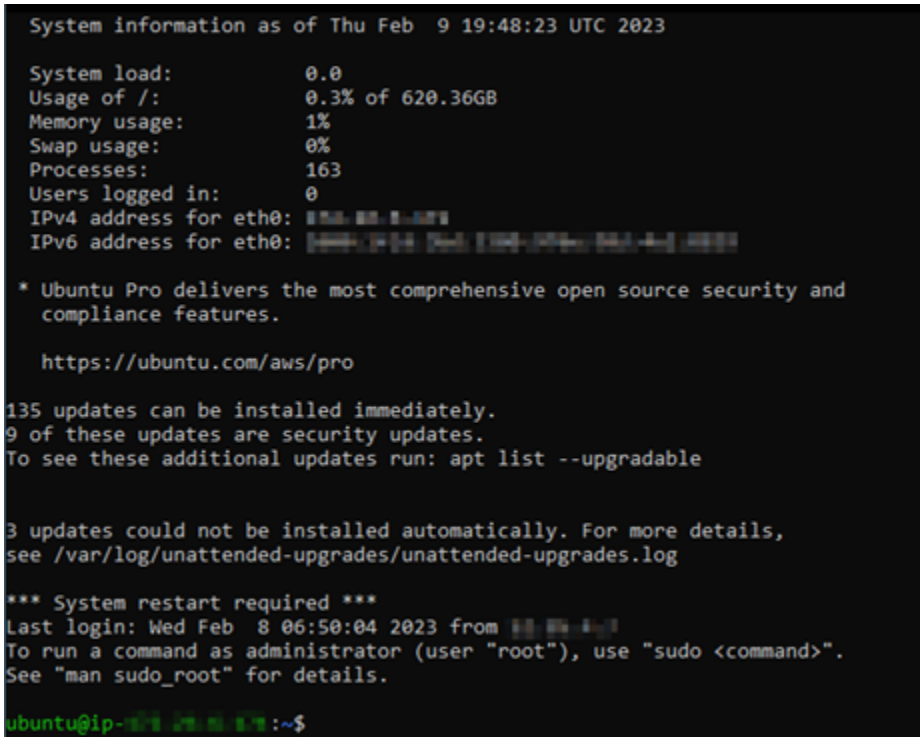
3. 次のコマンドを入力して、仮想コンピュータと SSH 接続を確立します。コマンドでは、*user-name* をサインイン時のユーザー名に、*public-ip-address* を仮想コンピュータのパブリック IP アドレスに置き換えます。

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

例

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

Lightsail for Research の Ubuntu 仮想コンピュータと SSH 接続が確立されていることを示す、次の例のようなレスポンスが表示されます。



仮想コンピュータへの SSH 接続が正常に確立されました。追加の次のステップについては、次のセクションに進みます。

Linux、Unix、macOS ローカルコンピュータで SSH を使用して仮想コンピュータに接続する

この手順は、ローカルコンピュータが Linux、Unix、または macOS オペレーティングシステムを使用している場合に適用されます。この手順では、 `get-instance` AWS CLI コマンドを使用し

て、接続するインスタンスのユーザー名とパブリック IP アドレスを取得します。詳細については、「AWS CLI コマンドリファレンス」の「get-instance」を参照してください。

> **Important**
>
> この手順を開始する前に、接続しようとしている仮想コンピュータの Lightsail デフォルトキーペア (DKP) を取得していることを確認してください。詳細については、「仮想コンピュータのキーペアを取得する」を参照してください。この手順では、Lightsail DKP のプライベートキーを、次のいずれかのコマンドで使用されるdkp_rsaファイルに出力します。

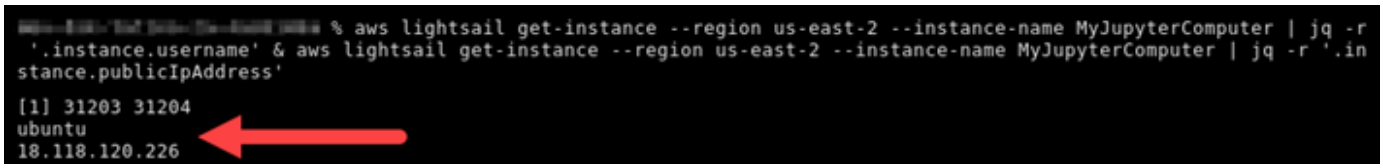
1. ターミナルウィンドウを開きます。
2. 次のコマンドを入力すると、仮想コンピュータのパブリック IP アドレスとユーザー名が表示されます。コマンドで、 を などの仮想コンピュータが作成された AWS リージョンのコードに置き換えますus-east-2。*region-code* に置き換えます。*computer-name* の部分は接続する仮想コンピュータの名前に置き換えます。

```
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'
```

例

```
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'
```

以下の例に示すように、応答では、仮想コンピュータのユーザー名とパブリック IP アドレスを表示します。これらの値は、この手順の次のステップで必要になるため、記録しておいてください。



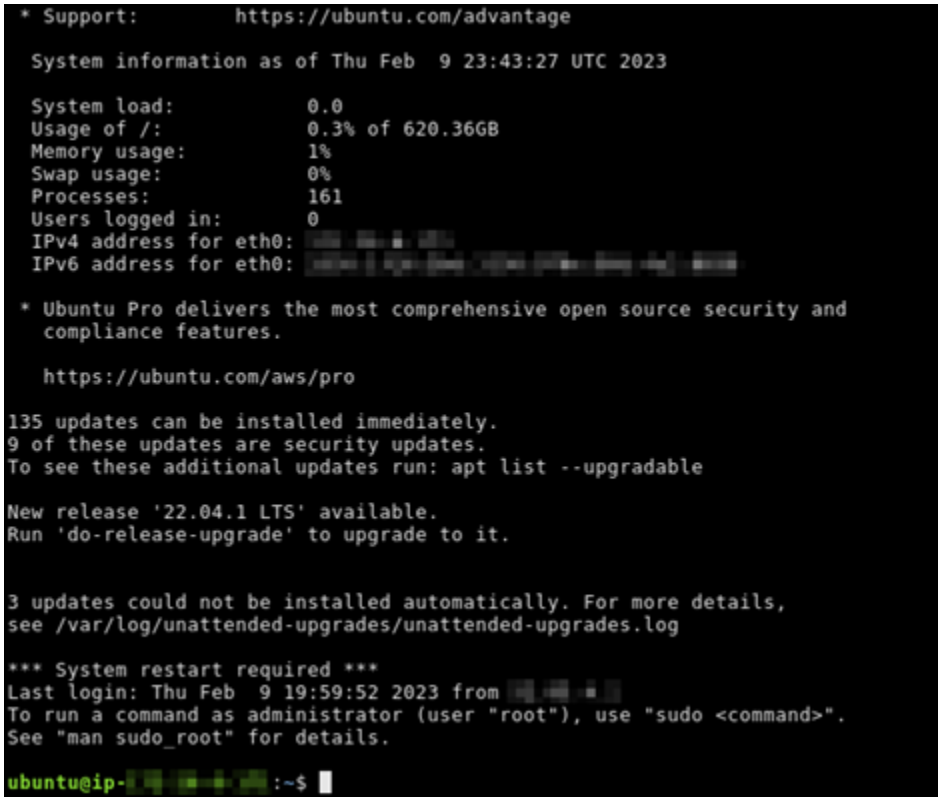
3. 次のコマンドを入力して、仮想コンピュータと SSH 接続を確立します。コマンドでは、*user-name* をサインイン時のユーザー名に、*public-ip-address* を仮想コンピュータのパブリック IP アドレスに置き換えます。

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

例

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

Lightsail for Research の Ubuntu 仮想コンピュータと SSH 接続が確立されていることを示す、次の例のようなレスポンスが表示されます。



仮想コンピュータへの SSH 接続が正常に確立されました。追加の次のステップについては、次のセクションに進みます。

次のステップに進みます

仮想コンピュータとの SSH 接続が正常に確立されたら、次の追加のステップを実行できます。

- SCP を使用して仮想コンピュータに接続し、ファイルを安全に転送します。詳細については、「Secure Copy を使用してファイルを仮想コンピュータに転送する」を参照してください。

Secure Copy を使用してファイルを仮想コンピュータに転送する

Secure Copy (SCP) を使用して、ローカルコンピュータから Amazon Lightsail for Research の仮想コンピュータにファイルを転送できます。この手順では、複数のファイルまたはディレクトリ全体を一度に転送できます。

> **Note**
>
> Lightsail for Research コンソールで利用できるブラウザベースの NICE DCV クライアントを使用して、仮想コンピュータへのリモートディスプレイプロトコル接続を確立することもできます。NICE DCV クライアントを使用すると、個別のファイルをすばやく転送できます。詳細については、「仮想コンピュータのオペレーティングシステムにアクセスする」を参照してください。

トピック

前提条件を満たす

開始する前に、前提条件として次の作業を完了します。

- Lightsail for Research で仮想コンピュータを作成します。詳細については、「仮想コンピュータを作成する」を参照してください。
- 接続する仮想コンピュータが動作状態であることを確認します。また、仮想コンピュータの名前と、その仮想コンピュータを作成した AWS リージョンを記録しておきます。この情報は、この手順で後ほど使用します。詳細については、「仮想コンピュータの詳細を表示する」を参照してください。
- AWS Command Line Interface () をダウンロードしてインストールしますAWS CLI。詳細については、「AWS Command Line Interface バージョン 2 用ユーザーガイド」の「AWS CLIの最新バージョンを使用してインストールまたは更新を行う」を参照してください。
- にアクセスする AWS CLI ように を設定します AWS アカウント。詳細については、「AWS Command Line Interface バージョン 2 用ユーザーガイド」の「Configuration basics」を参照してください。

- jq をダウンロードおよびインストールします。これは軽量で柔軟性の高いコマンドライン JSON プロセッサです。次の手順で使用して、キーペアの詳細を抽出します。jq のダウンロードとインストールについて、詳しくは、jq ウェブサイトの「Download jq」を参照してください。
- 接続する仮想コンピュータのポート 22 が開いていることを確認します。これは SSH で使用されるデフォルトのポートです。デフォルトでは開いています。ただし、閉じている場合は、次に進む前に再度開く必要があります。詳細については、「仮想コンピュータのファイアウォールポートを管理する」を参照してください。
- 仮想コンピュータの Lightsail デフォルトキーペア (DKP) を取得します。詳細については、「仮想コンピュータを作成する」を参照してください。

SCP を使用して仮想コンピュータに接続する

SCP を使用して Lightsail for Research の仮想コンピュータに接続するには、次のいずれかの手順を実行します。

Windows ローカルコンピュータで SCP を使用して仮想コンピュータに接続する

この手順は、ローカルコンピュータが Windows オペレーティングシステムを使用している場合に適用されます。この手順では、 `get-instance` AWS CLI コマンドを使用して、接続するインスタンスのユーザー名とパブリック IP アドレスを取得します。詳細については、「AWS CLI コマンドリファレンス」の「get-instance」を参照してください。

> **Important**
>
> この手順を開始する前に、接続しようとしている仮想コンピュータの Lightsail デフォルトキーペア (DKP) を取得していることを確認してください。詳細については、「仮想コンピュータのキーペアを取得する」を参照してください。この手順では、Lightsail DKP のプライベートキーを、次のいずれかのコマンドで使用されるdkp_rsaファイルに出力します。

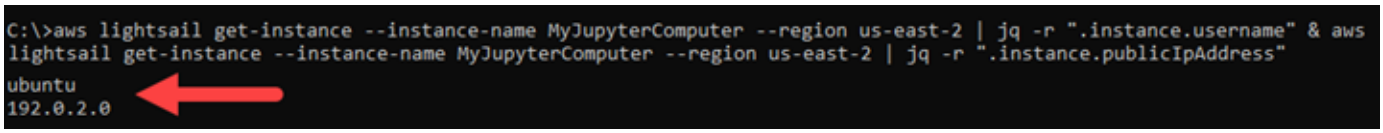
1. [コマンドプロント] ウィンドウを開きます。
2. 次のコマンドを入力すると、仮想コンピュータのパブリック IP アドレスとユーザー名が表示されます。コマンドで、 を などの仮想コンピュータが作成された AWS リージョンのコードに置き換えますus-east-2。*computer-name* の部分は接続する仮想コンピュータの名前に置き換えます。

```
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"
```

例

```
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"
```

以下の例に示すように、応答では、仮想コンピュータのユーザー名とパブリック IP アドレスを表示します。これらの値は、この手順の次のステップで必要になるため、記録しておいてください。



3. 次のコマンドを入力して、仮想コンピュータと SCP 接続を確立し、ファイルを転送します。

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

コマンドを、以下のように置き換えます。

- *source-folder* を、転送するファイルが保存されているローカルコンピュータ上のフォルダに置き換えます。
- *user-name* を、この手順の前のステップで使用したユーザー名 (ubuntu など) に置き換えます。
- *public-ip-address* を、この手順の前のステップで使用した仮想コンピュータのパブリック IP アドレスに置き換えます。
- *destination-directory* を、ファイルのコピー先となる仮想コンピュータ上のディレクトリへのパスに置き換えます。

次の例では、ローカルコンピュータ上の C:\Files フォルダにあるすべてのファイルをリモート仮想コンピュータ上の /home/lightsail-user/Uploads/ ディレクトリにコピーします。

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

次の例に示すようなレスポンスが表示されます。元のフォルダから転送先のディレクトリに転送された各ファイルが表示されます。これで、仮想コンピュータ上のファイルにアクセスできるようになりました。

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

Linux、Unix、macOS ローカルコンピュータで SCP を使用して仮想コンピュータに接続する

この手順は、ローカルコンピュータが Linux、Unix、macOS オペレーティングシステムを使用している場合に適用されます。この手順では、 `get-instance` AWS CLI コマンドを使用して、接続するインスタンスのユーザー名とパブリック IP アドレスを取得します。詳細については、「AWS CLI コマンドリファレンス」の「get-instance」を参照してください。

> **Important**
>
> この手順を開始する前に、接続しようとしている仮想コンピュータの Lightsail デフォルトキーペア (DKP) を取得していることを確認してください。詳細については、「仮想コンピュータのキーペアを取得する」を参照してください。この手順では、Lightsail DKP のプライベートキーを、次のいずれかのコマンドで使用されるdkp_rsaファイルに出力します。

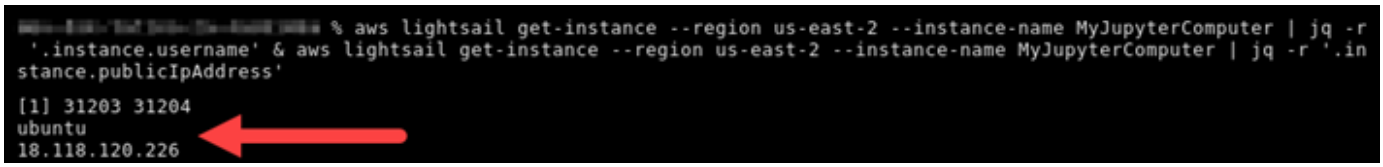
1. ターミナルウィンドウを開きます。
2. 次のコマンドを入力すると、仮想コンピュータのパブリック IP アドレスとユーザー名が表示されます。コマンドで、 を などの仮想コンピュータが作成された AWS リージョンのコードに置き換えますus-east-2。*computer-name* の部分は接続する仮想コンピュータの名前に置き換えます。

```
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'
```

例

```
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'
```

以下の例に示すように、応答では、仮想コンピュータのユーザー名とパブリック IP アドレスを表示します。これらの値は、この手順の次のステップで必要になるため、記録しておいてください。



3. 次のコマンドを入力して、仮想コンピュータと SCP 接続を確立し、ファイルを転送します。

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

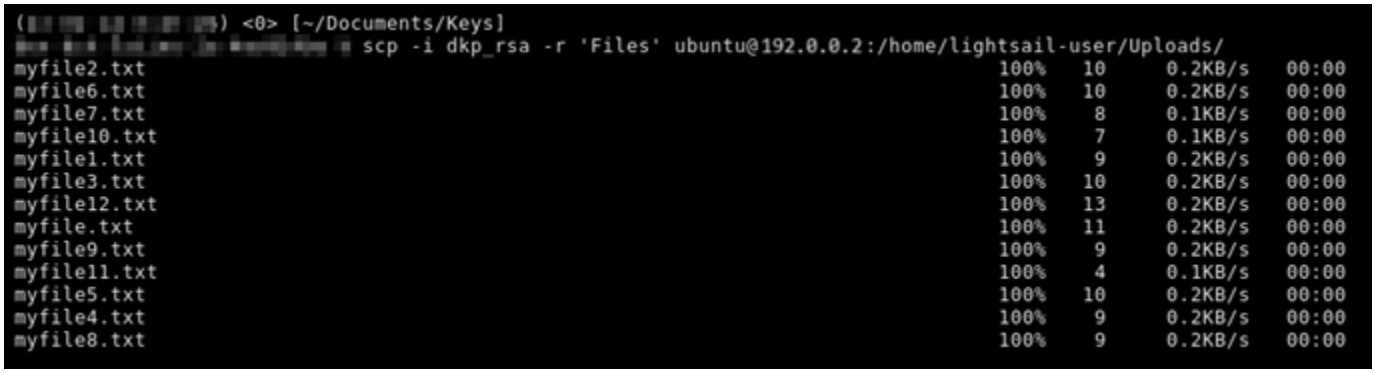
コマンドを、以下のように置き換えます。

- *source-folder* を、転送するファイルが保存されているローカルコンピュータ上のフォルダに置き換えます。
- *user-name* を、この手順の前のステップで使用したユーザー名 (ubuntu など) に置き換えます。
- *public-ip-address* を、この手順の前のステップで使用した仮想コンピュータのパブリック IP アドレスに置き換えます。
- *destination-directory* を、ファイルのコピー先となる仮想コンピュータ上のディレクトリへのパスに置き換えます。

次の例では、ローカルコンピュータ上の C:\Files フォルダにあるすべてのファイルをリモート仮想コンピュータ上の /home/lightsail-user/Uploads/ ディレクトリにコピーします。

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

次の例に示すようなレスポンスが表示されます。元のフォルダから転送先のディレクトリに転送された各ファイルが表示されます。これで、仮想コンピュータ上のファイルにアクセスできるようになりました。



仮想コンピュータを削除する

不要になった Lightsail for Research 仮想コンピュータを削除するには、次のステップを実行します。仮想コンピュータを削除すると、仮想コンピュータに対する課金も停止します。削除したコンピュータにアタッチされていたリソース (スナップショットなど) に対しては、削除するまで料金が発生します。

> **Important**
>
> 仮想コンピュータの削除は永続的な操作です。削除されたコンピュータを復元することはできません。後でデータが必要になる可能性がある場合は、削除する前に仮想コンピュータのスナップショットを作成してください。詳細については、「スナップショットを作成する」を参照してください。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[仮想コンピュータ] を選択します。
3. 削除する仮想コンピュータを選択します。
4. [アクション]、[仮想コンピュータを削除] の順に選択します。
5. テキストブロックに「confirm」と入力します。次に、[仮想コンピュータを削除] を選択します。

ストレージ

Amazon Lightsail for Research は、Lightsail for Research 仮想コンピュータに接続できるブロックレベルのストレージボリューム (ディスク) を提供します。このディスクは、細かい更新を頻繁に行う必要があるデータを対象とした主要ストレージデバイスとして使用できます。例えば、Lightsail for Research 仮想コンピュータでデータベースを実行する場合は、ディスクをストレージオプションとして使用することをお勧めします。

ディスクは、1 台の仮想コンピュータに接続できる、未フォーマットの外部ブロックデバイスのように動作します。これらのボリュームは、コンピュータの運用状況から独立した永続性を持ちます。ディスクは、コンピュータに接続後、他の物理ハードドライブと同じように使用できます。

1 台のコンピュータに複数のディスクを接続できます。また、コンピュータからディスクを切り離し、別のコンピュータに接続することもできます。

データのバックアップコピーを保持するには、ディスクのスナップショットを作成します。スナップショットから新しいディスクを作成して他のコンピュータに接続することもできます。

トピック

ディスクの作成

Lightsail for Research 仮想コンピュータのディスクを作成するには、以下のステップを実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[ストレージ] を選択します。
3. [ディスクの作成] を選択します。
4. ディスクの名前を入力します。有効な文字として英数字、数字、ピリオド、ダッシュ、ハイフン、アンダースコアを使用できます。

   ディスク名は、以下の要件を満たしている必要があります。

- Lightsail for Research アカウントの各 AWS リージョン で一意であること。
- 2～255 文字であること。
- 先頭と末尾は英数字または数字を使用すること。

5. ディスクの AWS リージョン を選択します。

   ディスクは、接続する仮想コンピュータと同じリージョンにある必要があります。
6. ディスクサイズを GB 単位で選択します。
7. ディスクを仮想コンピュータに接続する方法については、「ディスクを接続する」セクションに進んでください。

ディスクを表示する

Lightsail for Research アカウントにあるディスクとその詳細を表示するには、次の手順を実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[ストレージ] を選択します。

   [ストレージ] ページには、Lightsail for Research アカウント内のディスクの総合的に表示されます。

   ページには以下の情報が表示されます。

   - 名前 — ストレージディスクの名前。
   - サイズ — ディスクのサイズ (GB 単位)。
   - AWS リージョン— ディスクが作成された AWS リージョン。
   - アタッチ先 — ディスクが接続されている Lightsail コンピュータ。
   - 作成日 — ディスクが作成された日付。

ディスクを仮想コンピュータに接続する

Lightsail for Research の仮想コンピュータにディスクを接続するには、次の手順を実行します。1 台の仮想コンピュータに最大 15 台のディスクを接続できます。Lightsail for Research コンソールを使用してディスクを仮想コンピュータに接続すると、サービスがそのディスクを自動的にフォーマットおよびマウントします。この処理には数分かかるため、使用を開始する前に、ディスクのマウン

トステータスが [マウント済み] になっていることを確認する必要があります。Lightsail for Research は、デフォルトではディスクを /home/lightsail-user/*<disk-name>* ディレクトリにマウントします。この *<disk-name>* はディスクに付けた名前になります。

> **Important**
>
> ディスクを仮想コンピュータに接続するには、その仮想コンピュータが [実行中] の状態になっている必要があります。仮想コンピュータが [停止済み] の状態でディスクを接続すると、ディスクは接続されますがマウントはされません。ディスクの [マウントステータス] が [失敗] の場合、ディスクを切り離し、仮想コンピュータが [実行中] の状態になってから再接続する必要があります。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[仮想コンピュータ] を選択します。
3. ディスクを接続するコンピュータを選択します。
4. [ストレージ] タブを選択します。
5. [ディスクをアタッチする] を選択します。
6. コンピュータに接続するディスクの名前を選択します。
7. [アタッチ] を選択します。

仮想コンピュータからディスクを切り離す

コンピュータからディスクを切り離すには、以下の手順を実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[ストレージ] を選択します。
3. 切り離すディスクを見つけます。[アタッチ先] の列で、ディスクが接続されているコンピュータ名を選択します。
4. [停止] を選択してコンピュータを停止します。ディスクを切り離す前に、コンピュータを停止する必要があります。
5. コンピュータを停止することを確認し、[コンピュータの停止] を選択します。
6. [ストレージ] タブを選択します。
7. 切り離すディスクを選択し、[デタッチ] を選択します。

8. ディスクをコンピュータから切り離すことを確認し、[デタッチ] を選択します。

ディスクの削除

不要になったストレージディスクを削除するには、以下の手順を実行します。ディスクが削除されると、料金の発生も停止します。

ディスクがコンピュータに接続されている場合は、削除する前にまず切り離す必要があります。詳細については、「仮想コンピュータからディスクを切り離す」を参照してください。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[ストレージ] を選択します。
3. 削除するディスクを見つけて選択します。
4. [ディスクを削除] をクリックします。
5. ディスクを削除することを確定します。その後、[Delete] (削除) をクリックします。

スナップショット

スナップショットは、データのポイントインタイムコピーです。Amazon Lightsail for Research 仮想コンピュータとストレージディスクのスナップショットを作成し、それを基礎として新しいコンピュータを作成したり、データをバックアップしたりできます。

スナップショットには、コンピュータの復元に必要なすべてのデータ (スナップショットが作成された時点のデータ) が含まれます。スナップショットを元に新しい仮想コンピュータを作成すると、新しいコンピュータは、スナップショットの作成に使用された元のコンピュータのの完全なレプリカとして起動します。

リソースにはいつでも障害が発生する可能性があるため、データが永久に失われないように、頻繁にスナップショットを作成することをおすすめします。

トピック

スナップショットを作成する

Lightsail for Research 仮想コンピュータまたはディスクのスナップショットを作成するには、以下のステップを実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[スナップショット] を選択します。
3. 次のいずれかのステップを完了します。
   - [仮想コンピュータのスナップショット] で、スナップショットを作成するコンピュータの名前を見つけ、[スナップショットを作成] を選択します。
   - [ディスクのスナップショット] で、スナップショットを作成するディスクの名前を見つけ、[スナップショットを作成] を選択します。
4. スナップショットの名前を入力します。有効な文字として英数字、数字、ピリオド、ダッシュ、ハイフン、アンダースコアを使用できます。

スナップショット名は、以下の要件を満たしている必要があります。

- Lightsail for Research アカウントの各 AWS リージョン で一意であること。
- 2 ~ 255 文字であること。
- 先頭と末尾は英数字または数字を使用すること。

5. [Create snapshot] (スナップショットを作成) を選択します。

スナップショットを表示する

仮想コンピュータとディスクのスナップショットを表示するには、以下の手順を実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[スナップショット] を選択します。

   [スナップショット] ページに、作成した仮想コンピュータとディスクのスナップショットが表示されます。

   アーカイブされたスナップショットもこのページにあります。アーカイブされたスナップショットとは、アカウントから削除されたリソースのスナップショットです。

スナップショットから仮想コンピュータまたはディスクを作成する

スナップショットから新しい Lightsail for Research 仮想コンピュータまたはディスクを作成するには、以下の手順を実行します。

スナップショットから仮想コンピュータを作成する場合は、元のコンピュータと同じかそれ以上のサイズのプランを使用してください。元の仮想コンピュータよりサイズの小さいプランを使用することはできません。

スナップショットからディスクを作成する場合は、元のディスクよりも大きいディスクサイズを選択します。元のディスクよりも小さいディスクは使用できません。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[スナップショット] を選択します。

3. [スナップショット] ページで、新しいコンピュータまたはディスクの作成に使用するコンピュータまたはディスクスナップショットの名前を見つけます。[スナップショット] のドロップダウンメニューを選択すると、そのリソースで使用できるスナップショットのリストが表示されます。
4. 仮想コンピュータの作成に使用するスナップショットを選択します。
5. [アクション] ドロップダウンメニューを選択します。次に、[仮想コンピュータを作成] または [ディスクを作成] を選択します。

スナップショットの削除

スナップショットを削除するには、次のステップを実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[スナップショット] を選択します。
3. [スナップショット] ページで、削除するコンピュータまたはディスクのスナップショットの名前を見つけます。[スナップショット] のドロップダウンメニューを選択すると、そのリソースで使用できるスナップショットのリストが表示されます。
4. 削除するスナップショットを選択します。
5. [アクション] ドロップダウンメニューを選択します。その後、[スナップショットを削除] を選択します。
6. スナップショット名が正しいことを確認します。その後、[スナップショットを削除] を選択します。

Amazon Lightsail for Research のコストと使用状況の見積もり

Amazon Lightsail for Research は、 AWS リソースのコストと使用状況の見積りを提供します。これらの見積もりを使用して、Lightsail for Research を使用する際の支出の計画、コスト削減の機会の発見、情報に基づいた意思決定に役立てることができます。

仮想コンピュータまたはディスクを作成すると、そのリソースのコストと使用状況の見積りが表示されます。リソースが作成され、[使用可能] または [実行中] の状態になると、直ちにコストと使用状況の見積りが反映されます。見積りは、リソースが作成されてから 15 分以内に AWS マネジメントコンソールに表示されます。削除されたリソースは見積りには含まれません。

> **Important**
>
> 見積りは、リソースの使用状況に基づいた推定コストです。実際のコストは、Lightsail for Research コンソールに表示される見積もりではなく、リソースの実際の使用状況に基づいて決まります。実際のコストは、 AWS Billing アカウントステートメントに表示されます。にサインイン AWS Management Console し、https://console.aws.amazon.com/billing/ で AWS Billing コンソールを開きます。

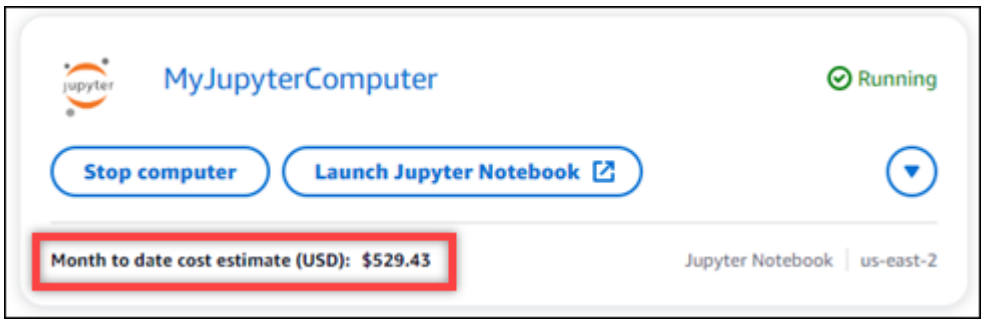
トピック

- コストと使用状況の見積りをモニタリングする

コストと使用状況の見積りをモニタリングする

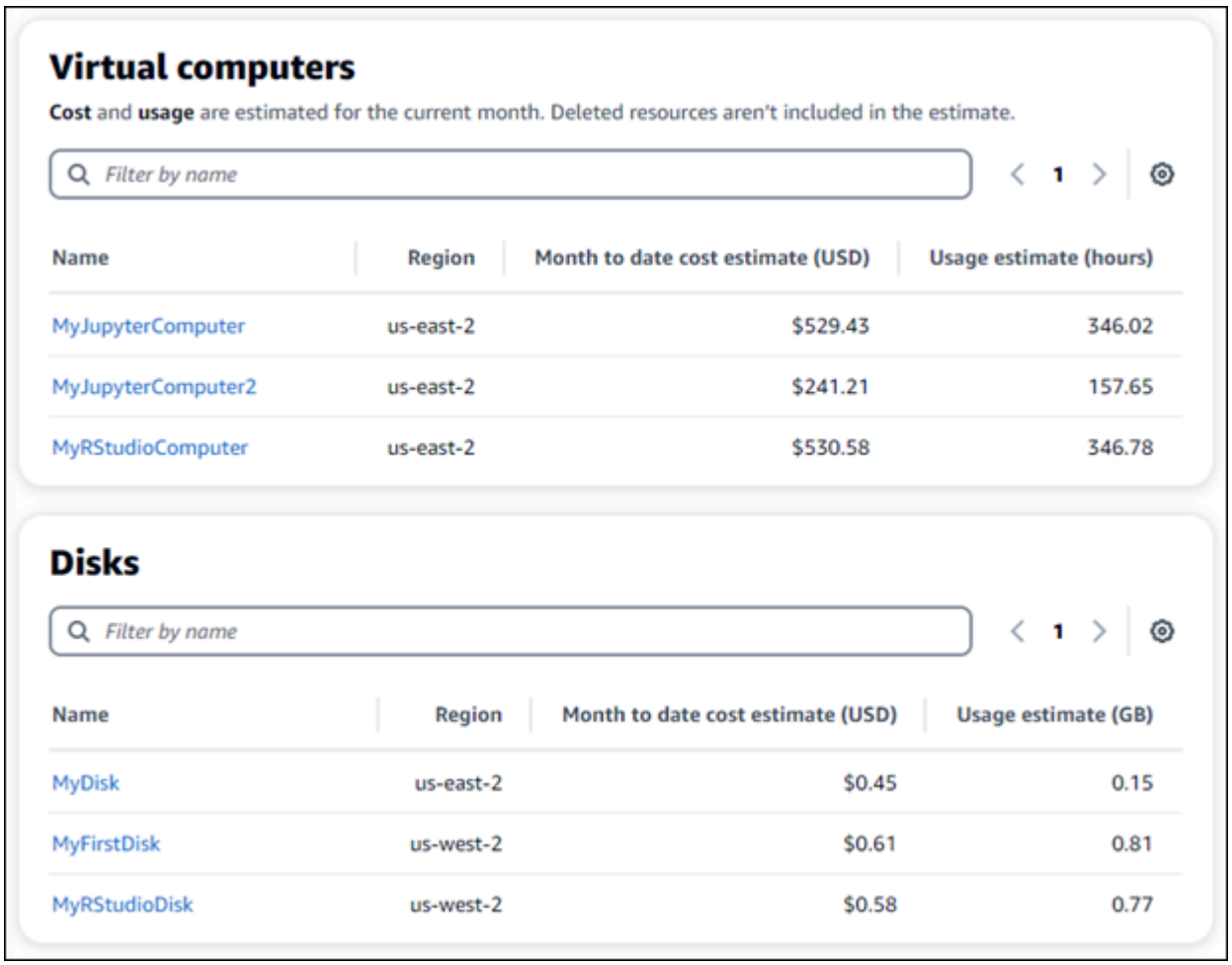
Lightsail for Research リソースの過去 1 か月のコストと使用状況の見積もりは、Lightsail for Research コンソールの次の領域に表示されます。

1. Lightsail for Research コンソールのナビゲーションペインで仮想コンピュータを選択します。仮想コンピュータの月初来のコスト見積もりは、実行中の各仮想コンピュータの下に表示されます。



2. 仮想コンピュータの CPU 使用率を表示するには、仮想コンピュータの名前を選択し、[ダッシュボード] タブを選択します。

3. すべての Lightsail for Research リソースの過去 1 か月のコストと使用状況の見積もりを表示するには、ナビゲーションペインで Usage を選択します。


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

コスト管理

コスト管理では、Lightsail for Research 仮想コンピュータの使用状況とコストの管理に役立つように定義するルールを使用します。

一定期間に CPU 使用率が指定した割合に達すると実行中のコンピュータを停止する「アイドル状態の仮想コンピュータを停止」ルールを作成できます。例えば、30 分間の CPU 使用率が 5% 以下になると特定のコンピュータを自動的に停止するルールを作成できます。これはコンピュータがアイドル状態であることを意味しているため、Lightsail for Research がコンピュータを停止します。仮想コンピュータの停止後は、標準の時間単位の料金は発生しなくなります。

トピック

ルールの作成

Lightsail for Research 仮想コンピュータ用のルールを作成するには、以下の手順を実行します。

> **Note**
>
> 現時点でサポートされているルールアクションは、仮想コンピュータを停止するアクションのみです。CPU 使用率は現在ルールがモニタリングする唯一のメトリクスです。また、「~以下」のオペレーションのみサポートされています。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで [コスト管理] を選択します。
3. [ルールの作成] を選択します。
4. ルールを適用するリソースを選択します。
5. CPU 使用率とルールを実行する期間を指定します。

   例えば、「5%」、「30 分」といった指定ができます。Lightsail for Research は、30 分間の CPU 使用率が 5% 以下になると、コンピュータを自動的に停止します。
6. [ルールの作成] を選択します。

7. 新しいルールの情報が正しいことを確認し、[確認] を選択します。

ルールの削除

Lightsail for Research 仮想コンピュータ用のルールを削除するには、以下の手順を実行します。

1. Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで [コスト管理] を選択します。
3. 削除するルールを選択します。
4. [Delete] (削除) をクリックします。
5. ルールを削除することを確認した上で、[削除] をクリックします。

タグ

Amazon Lightsail for Research では、タグをリソースに割り当てることができます。タグはそれぞれ、キーと任意の値で構成される 1 つのラベルです。タグを使うと、効率的にリソースを管理することができます。値のないキーはキーオンリータグと呼ばれ、値のあるキーはキー値タグと呼ばれます。タグには、固有なタイプはありませんが、リソースを用途、所有者、環境などの基準で分類できます。これは、同じ種類のリソースが多い場合に役立ちます。リソースに割り当てたタグに基づいて、特定のリソースをすばやく識別できます。例えば、各リソースのプロジェクトや優先度の追跡に役立つ一連のタグを定義できます。

以下のリソースには、Amazon Lightsail for Research コンソールでタグを付けることができます。

- 仮想コンピュータ
- ストレージディスク
- スナップショット

タグには以下の制限があります。

- リソースあたりのタグの最大数は 50 です。
- リソースごとに各タグキーを一意にする必要があります。各タグキーが保持できる値は 1 つのみです。
- キーの最大長は UTF-8 で 128 Unicode 文字です。
- 値の最大長は UTF-8 で 256 Unicode 文字です。
- 複数のサービス間およびリソース間でタグ付けスキーマを使用する場合、他のサービスでも許可される文字に制限が適用されることがあることに注意してください。通常、使用できる文字は、英字、数字、スペース、および次の文字です: `+ - = . _ : / @`
- タグのキーと値は大文字と小文字が区別されます。
- キーや値には `aws:` プレフィックスは使用しないでください。このプレフィックスは AWS 専用です。

トピック

タグの作成

Lightsail for Research の仮想コンピュータにタグを作成するには、次の手順を実行します。手順は、Lightsail for Research のディスクとスナップショットの場合と同様です。

1. Lightsail for Research コンソールから Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[仮想コンピュータ] を選択します。
3. タグを作成する仮想コンピュータを選択します。
4. [タグ] タブを選択します。
5. [Manage tags] (タグの管理) を選択します。
6. 新しいタグを追加を選択します。
7. [キー] フィールドにキー名を入力します。(例: Project)
8. (オプション) [値]フィールドに値名を入力します。(例: Blog)
9. [変更を保存] を選択して、キーを仮想コンピュータに保存します。

タグの削除

Lightsail for Research の仮想コンピュータからタグを削除するには、次の手順を実行します。手順は、Lightsail for Research のディスクとスナップショットの場合と同様です。

1. Lightsail for Research コンソールから Lightsail for Research コンソールにサインインします。
2. ナビゲーションペインで、[仮想コンピュータ] を選択します。
3. タグを削除する仮想コンピュータを選択します。
4. [タグ] タブを選択します。
5. [Manage tags] (タグの管理) を選択します。
6. [削除] を選択して、リソースからタグを削除します。

> **Note**
>
> タグの値だけを削除する場合は、削除する値を見つけて、その横にある X アイコンをクリックします。

7. [Save changes] (変更の保存) をクリックします。

Amazon Lightsail for Research のセキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。責任共有モデルではこれを、クラウドのセキュリティ、およびクラウド内でのセキュリティと説明しています:

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行するインフラストラクチャを保護する責任を担います AWS クラウド。また、 は、お客様が安全に使用できるサービス AWS も提供します。コンプライアンスAWS プログラムコンプライアンスプログラム の一環として、サードパーティーの監査者は定期的にセキュリティの有効性をテストおよび検証。Amazon Lightsail for Research に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウドのセキュリティ — お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Lightsail for Research を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Lightsail for Research を設定する方法を示します。また、Lightsail for Research リソースのモニタリングや保護に役立つ他の AWS のサービスの使用方法についても説明します。

トピック

Amazon Lightsail for Research でのデータ保護

責任 AWS 共有モデル、Amazon Lightsail for Research でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。お客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された記事「AWS 責任共有モデルおよび GDPR」を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 は必須であり TLS 1.3 がお勧めです。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。
- AWS 暗号化ソリューションと、 内のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報は、タグ、または名前フィールドなどの自由形式のテキストフィールドに配置しないことを強くお勧めします。これは、コンソール、API、または AWS CLI SDK を使用して Lightsail for Research または他の AWS のサービス を使用する場合も同様です。 AWS SDKs 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

Amazon Lightsail for Research の Identity and Access Management

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に Lightsail for Research リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

> **Note**
>
> Amazon Lightsail と Lightsail for Research は、同じ IAM ポリシーパラメータを共有します。Lightsail for Research ポリシーに加えられた変更は、Lightsail ポリシーにも影響します。例えば、ユーザーが Lightsail for Research でディスクを作成するアクセス許可を持っている場合、同じユーザーが Lightsail でディスクを作成することもできます。

トピック

対象者

AWS Identity and Access Management (IAM) の使用方法は、Lightsail for Research で行う作業によって異なります。

サービスユーザー – Lightsail for Research サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの Lightsail for Research 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Lightsail for Research の機能にアクセスできない場合は、「」を参照してくださいAmazon Lightsail for Research のアイデンティティとアクセスのトラブルシューティング。

サービス管理者 – 社内の Lightsail for Research リソースを担当している場合は、通常、Lightsail for Research へのフルアクセスがあります。サービスユーザーがどの Lightsail for Research 機能やリ

ソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。お客様の会社で Lightsail for Research で IAM を使用する方法の詳細については、「」を参照してくださいAmazon Lightsail for Research と IAM の連携方法。

IAM 管理者 – IAM 管理者は、Lightsail for Research へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Lightsail for Research アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon Lightsail for Research のアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証（ にサインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center（ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook の認証情報は、フェデレーション ID の例です。フェデレーティッドアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーション AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 ユーザーガイド」の「 へのサインイン AWS アカウント方法AWS サインイン 」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを向上させることをお勧めします。詳細については、『AWS IAM Identity Center ユーザーガイド』の「Multi-factor authentication」(多要素認証) および『IAM ユーザーガイド』の「AWSにおける多要素認証 (MFA) の使用」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、『IAM ユーザーガイド』の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、Identity Center ディレクトリのユーザー、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID がにアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期して、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、『AWS IAM Identity Center ユーザーガイド』の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに対して特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できま

す。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する権限を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、『IAM ユーザーガイド』の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッドアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーティッドアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、『IAM ユーザーガイド』の「サードパーティーアイデンティティプロバイダー向けロールの作成」 を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。権限セットの詳細については、『AWS IAM Identity Center ユーザーガイド』の「権限セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、 (ロールをプロキシとして使用する代わりに) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、

『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

- クロスサービスアクセス — 一部の は、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの権限、サービスロール、またはサービスにリンクされたロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して でアクションを実行する場合 AWS、ユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに権限を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。
- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、『IAM ユーザーガイド』の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して権限を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、『IAM ユーザーガイド』の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、 AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。プリンシパル (ユーザー、ルートユーザー、またはロールセッション) AWS がリクエストを行うと、 はこれらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、『IAM ユーザーガイド』の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、『Amazon Simple Storage Service デベロッパーガイド』の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートします。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティの許可の境界」を参照してください。
- サービスコントロールポリシー (SCPs) – SCPs は、 の組織または組織単位 (OU) に対する最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、 AWS

アカウント ビジネスが所有する複数の をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、『AWS Organizations ユーザーガイド』の「SCP の仕組み」を参照してください。

- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS を決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

Amazon Lightsail for Research と IAM の連携方法

IAM を使用して Lightsail for Research へのアクセスを管理する前に、Lightsail for Research で使用できる IAM 機能について学びます。

Amazon Lightsail for Research で使用できる IAM の機能

IAM 機能	Lightsail for Research のサポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	No
ポリシーアクション	Yes
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい

IAM 機能	Lightsail for Research のサポート
ACL	No
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	Yes
プリンシパル権限	いいえ
サービスロール	いいえ
サービスリンクロール	いいえ

Lightsail for Research およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

Lightsail for Research のアイデンティティベースのポリシー

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 権限ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素については、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Lightsail for Research のアイデンティティベースのポリシーの例

Lightsail for Research のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon Lightsail for Research のアイデンティティベースのポリシーの例。

Lightsail for Research 内のリソースベースのポリシー

リソースベースのポリシーのサポート	No

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Lightsail for Research のポリシーアクション

ポリシーアクションに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

JSON ポリシーの`Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連付けられた AWS API オペレー

ションと同じです。一致する API オペレーションのない権限のみのアクションなど、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

このアクションは、関連付けられたオペレーションを実行するための権限を付与するポリシーで使用されます。

Lightsail for Research アクションのリストを確認するには、「サービス認証リファレンス」のAmazon Lightsail for Research で定義されるアクション」を参照してください。

Lightsail for Research のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
lightsail
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

Lightsail for Research のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon Lightsail for Research のアイデンティティベースのポリシーの例。

Lightsail for Research のポリシーリソース

ポリシーリソースに対するサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースにどのような条件でアクションを実行できるかということです。

Resource JSON ポリシー要素は、アクションが適用されるオブジェクトを指定します。ステートメントには、Resource または NotResource要素を含める必要があります。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの権限と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

Lightsail for Research リソースタイプとその ARNs「サービス認証リファレンス」のAmazon Lightsail for Research で定義されるリソース」を参照してください。各リソースの ARN を指定できるアクションについては、Amazon Lightsail for Research で定義されるアクション」を参照してください。

Lightsail for Research のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon Lightsail for Research のアイデンティティベースのポリシーの例。

Lightsail for Research のポリシー条件キー

サービス固有のポリシー条件キーのサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS は AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、『IAM ユーザーガイド』の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートします。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

Lightsail for Research の条件キーのリストを確認するには、「サービス認証リファレンス」のAmazon Lightsail for Research の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、Amazon Lightsail for Research で定義されるアクション」を参照してください。

Lightsail for Research のアイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAmazon Lightsail for Research のアイデンティティベースのポリシーの例。

Lightsail for Research の ACLs

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Lightsail for Research での ABAC

ABAC (ポリシー内のタグ) のサポート	部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいて権限を定義する認可戦略です。ではAWS、これらの属性はタグ と呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール) および多くの AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合に操作を許可するように ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値ははいです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、『IAM ユーザーガイド』の「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性に基づくアクセスコントロール (ABAC) を使用する」を参照してください。

Lightsail for Research での一時的な認証情報の使用

一時的な認証情報のサポート	はい

一部の は、一時的な認証情報を使用してサインインすると機能 AWS のサービス しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「IAM と連携する 」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社の Single Sign-On (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ロールへの切り替え (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用して にアクセスします AWS。 AWS 長期的なアクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

Lightsail for Research のクロスサービスプリンシパル許可

転送アクセスセッション (FAS) をサポート	いいえ

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストと組み合わせ

て使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Lightsail for Research のサービスロール

サービスロールのサポート	いいえ

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに権限を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、Lightsail for Research の機能が破損する可能性があります。Lightsail for Research が指示する場合以外は、サービスロールを編集しないでください。

Lightsail for Research のサービスにリンクされたロール

サービスにリンクされたロールのサポート	いいえ

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールの権限を表示できますが、編集することはできません。

サービスにリンクされたロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の中から、[Service-linked role] (サービスにリンクされたロール) 列に Yes と記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[Yes] リンクを選択します。

Amazon Lightsail for Research のアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには Lightsail for Research リソースを作成または変更するアクセス許可はありません。また、、 AWS Command Line Interface （ AWS CLI ） AWS Management Console、または AWS API を使用してタスクを実行することはできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、『IAM ユーザーガイド』の「IAM ポリシーの作成」を参照してください。

各リソースタイプの ARNs「サービス認証リファレンス」のAmazon Lightsail for Research のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- Lightsail for Research コンソールの使用
- 自分の権限の表示をユーザーに許可する

ポリシーのベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが Lightsail for Research リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、『IAM ユーザーガイド』の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで権限を設定するときは、タスクの実行に必要な権限のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定

義します。これは、最小特権権限とも呼ばれています。IAM を使用して権限を適用する方法の詳細については、『IAM ユーザーガイド』の「IAM でのポリシーと権限」を参照してください。

- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、 などの特定の を介してサービスアクションが使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、『IAM ユーザーガイド』の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、『IAM ユーザーガイド』の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、『IAM ユーザーガイド』の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、『IAM ユーザーガイド』の「IAM でのセキュリティのベストプラクティス」を参照してください。

Lightsail for Research コンソールの使用

Amazon Lightsail for Research コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 の Lightsail for Research リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続き Lightsail for Research コンソールを使用できるようにするには、エンティティに Lightsail for Research *ConsoleAccess*または *ReadOnly* AWS 管理ポリシーもアタッチ

します。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

自分の権限の表示をユーザーに許可する

この例では、ユーザーアイデンティティにアタッチされたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーの作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "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": "*"
        }
    ]
}
```

Amazon Lightsail for Research のアイデンティティとアクセスのトラブルシューティング

以下の情報は、Lightsail for Research と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立ちます。

トピック

Lightsail for Research でアクションを実行する権限がない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なlightsail:*GetWidget* アクセス許可を持っていない場合に発生するものです。

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

この場合、lightsail:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン資格情報を提供した担当者が管理者です。

自分の 以外のユーザーに Lightsail for Research リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Lightsail for Research がこれらの機能をサポートしているかどうかを確認するには、「」を参照してくださいAmazon Lightsail for Research と IAM の連携方法。
- 所有 AWS アカウント している のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。
- リソースへのアクセスをサードパーティー に提供する方法については AWS アカウント、IAM ユーザーガイドの「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、『IAM ユーザーガイド』の「外部で認証されたユーザー (ID フェデレーション) へのアクセス権限」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、『IAM ユーザーガイド』の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Amazon Lightsail for Research のコンプライアンス検証

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、関心のあるコンプライアンスプログラムを選択します。一般的な情報については、AWS 「コンプライアンスプログラム」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「 でのレポートのダウンロード AWS Artifact」の」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

> **Note**
>
> すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、「HIPAA 対応サービスのリファレンス」を参照してください。

- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- AWS カスタマーコンプライアンスガイド — コンプライアンスの観点から責任共有モデルを理解します。このガイドでは、ガイダンスを保護し AWS のサービス 、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council (PCI)、国際標準化機構 (ISO) を含む) のセキュリティコントロールにマッピングするためのベストプラクティスをまとめています。
- 「 デベロッパーガイド」の「 ルールによるリソースの評価」 – この AWS Config サービスは、リソース設定が社内プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に確認できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールのリストについては、「Security Hub のコントロールリファレンス」を参照してください。
- AWS Audit Manager – これにより AWS のサービス 、 AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

Amazon Lightsail for Research の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、および高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

AWS グローバルインフラストラクチャに加えて、Lightsail for Research には、データの耐障害性とバックアップのニーズをサポートするのに役立つくつかの機能があります。詳細については、「スナップショット」および「スナップショットを作成する」を参照してください。

Amazon Lightsail for Research のインフラストラクチャセキュリティ

マネージドサービスである Amazon Lightsail for Research は、 AWS グローバルネットワークセキュリティで保護されています。 AWS セキュリティサービスと がインフラストラクチャ AWS を保護する方法については、AWS 「 クラウドセキュリティ」を参照してください。インフラストラクチャセキュリティのベストプラクティスを使用して AWS 環境を設計するには、「セキュリティの柱 AWS Well-Architected Framework」の「Infrastructure Protection」を参照してください。

AWS が公開した API コールを使用して、ネットワーク経由で Lightsail for Research にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2 は必須で TLS 1.3 がお勧めです。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token Service (AWS STS) を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

Amazon Lightsail for Research の設定と脆弱性の分析

設定と IT コントロールは、 AWS とお客様の間で共有される責任です。詳細については、 AWS 「 責任共有モデル」を参照してください。

Amazon Lightsail for Research のセキュリティのベストプラクティス

Lightsail for Research には、独自のセキュリティポリシーを開発および実装する際に考慮すべきいくつかのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドライン

であり、完全なセキュリティソリューションを説明するものではありません。これらのベストプラクティスはお客様の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な考慮事項とお考えください。

Lightsail for Research の使用に関連する潜在的なセキュリティイベントを防ぐには、以下のベストプラクティスに従ってください。

- Lightsail for Research コンソールにアクセスするには、 AWS Management Console 最初のコンソールを認証します。個人コンソールの認証情報は共有しないでください。インターネット上の誰でもコンソールを表示できますが、コンソールへの有効な認証情報がなければサインインやセッションの開始はできません。

Lightsail for Research ユーザーガイドのドキュメント履歴

次の表は、Lightsail for Research のドキュメントリリースの内容をまとめたものです。

変更	説明	日付
初回リリース	Lightsail for Research ユーザーガイドの初回リリース。	2023 年 2 月 28 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。