



ユーザーガイド

Amazon Lightsail for Research



Amazon Lightsail for Research: ユーザーガイド

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

Amazon の商標およびトレードドレスは、Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は、Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

Amazon Lightsail for Research とは	1
料金	1
可用性	1
設定	2
にサインアップする AWS アカウント	2
管理アクセスを持つユーザーを作成する	2
開始方法のチュートリアル	5
ステップ 1: 前提条件を満たす	5
ステップ 2: 仮想コンピュータを作成する	5
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	6
ステップ 4: 仮想コンピュータに接続する	7
ステップ 5: 仮想コンピュータにストレージを追加する	8
ステップ 6: スナップショットを作成する	8
ステップ 7: クリーンアップする	9
チュートリアル	11
の使用を開始する JupyterLab	11
ステップ 1: 前提条件を満たす	12
ステップ 2: (オプション) ストレージ領域を追加する	12
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	12
ステップ 4: アプリケーションを起動する JupyterLab	13
ステップ 5: ドキュメントを読む JupyterLab	17
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	17
ステップ 7: (オプション) コスト管理ルールを作成する	19
ステップ 8: (オプション) スナップショットを作成する	20
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	20
の使用を開始する RStudio	21
ステップ 1: 前提条件を満たす	22
ステップ 2: (オプション) ストレージ領域を追加する	22
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	23
ステップ 4: RStudioアプリケーションを起動する	23
ステップ 5: RStudioドキュメントを読む	27
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	29
ステップ 7: (オプション) コスト管理ルールを作成する	30
ステップ 8: (オプション) スナップショットを作成する	31

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	31
仮想コンピュータ	33
アプリケーションとハードウェアプラン	33
アプリケーション	34
プラン	35
仮想コンピュータを作成する	36
仮想コンピュータの詳細を表示する	37
仮想コンピュータのアプリケーションを起動する	38
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	39
ファイアウォールポート	40
プロトコル	40
ポート	41
ポートを開閉する理由	41
前提条件を満たす	42
仮想コンピュータのポート状態を取得する	42
仮想コンピュータのポートを開く	43
仮想コンピュータのポートを閉じる	45
次のステップに進みます	46
仮想コンピュータのキーペアを取得する	47
前提条件を満たす	48
仮想コンピュータのキーペアを取得する	48
次のステップに進みます	52
を使用して仮想コンピュータに接続する SSH	53
前提条件を満たす	53
を使用して仮想コンピュータに接続する SSH	54
次のステップに進みます	60
を使用して仮想コンピュータにファイルを転送する SCP	61
前提条件を満たす	61
を使用して仮想コンピュータに接続する SCP	62
仮想コンピュータを削除する	66
[Storage (ストレージ)]	67
ディスクの作成	67
ディスクを表示する	68
ディスクを仮想コンピュータに接続する	68
仮想コンピュータからディスクを切り離す	69
ディスクの削除	70

スナップショット	71
スナップショットの作成	71
スナップショットを表示する	72
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	72
スナップショットを削除する	73
コストと使用状況	74
コストと使用状況を表示する	74
コスト管理ルール	77
ルールの作成	77
ルールの削除	78
タグ	79
タグの作成	80
タグの削除	80
セキュリティ	81
データ保護	82
Identity and Access Management	82
対象者	83
アイデンティティを使用した認証	84
ポリシーを使用したアクセスの管理	88
Amazon Lightsail for Research と の連携方法 IAM	90
アイデンティティベースポリシーの例	97
トラブルシューティング	100
コンプライアンス検証	101
耐障害性	103
インフラストラクチャセキュリティ	103
設定と脆弱性の分析	104
セキュリティに関するベストプラクティス	104
ドキュメント履歴	105
.....	cvi

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 を使用すると、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機能を備えているため、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すべて、公開されている [API](#)、Amazon Lightsail [API](#) の [AWS CLI](#) および をインストールして使用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。

にサインアップする AWS アカウント

がない場合は AWS アカウント、次のステップ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/サインアップ> 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。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。 <https://aws.amazon.com/> に移動し、マイアカウント を選択すると、いつでも現在のアカウントアクティビティを表示し、アカウントを管理できます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 AWS アカウントのルートユーザー

1. ルートユーザーを選択し、AWS アカウント E メールアドレスを入力して、アカウント所有者 [AWS Management Console](#) として にサインインします。次のページでパスワードを入力します。

ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの[ルートユーザーとしてサインインする](#)を参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

手順については、「ユーザーガイド」の[AWS アカウント「ルートユーザーの仮想MFAデバイスを有効にする \(コンソール\) IAM」](#)を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM Identity Center を有効にします。

手順については、「AWS IAM Identity Center ユーザーガイド」の「[AWS IAM Identity Centerの有効化](#)」を参照してください。

2. IAM Identity Center で、ユーザーに管理アクセス権を付与します。

を ID ソース IAM アイデンティティセンターディレクトリとして使用する方法的チュートリアルについては、「ユーザーガイド」の「[デフォルトでユーザーアクセスを設定する IAM アイデンティティセンターディレクトリAWS IAM Identity Center](#)」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM Identity Center ユーザーでサインインするには、IAM Identity Center ユーザーの作成時に E メールアドレスに URL 送信されたサインインを使用します。

IAM Identity Center ユーザーを使用してサインインする方法については、「AWS サインイン ユーザーガイド」の[AWS「アクセスポータルにサインインする」](#)を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM Identity Center で、最小特権のアクセス許可を適用するベストプラクティスに従うアクセス許可セットを作成します。

手順については、「AWS IAM Identity Center ユーザーガイド」の「[権限設定を作成する](#)」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

手順については、「AWS IAM Identity Center ユーザーガイド」の「[グループの参加](#)」を参照してください。

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 では、仮想コンピュータは、で作成して管理する研究ワークステーションです AWS クラウド。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 Linux インスタンスに基づいています。仮想コンピュータでは、JupyterLab、Scilab RStudioなどの研究アプリケーションを事前設定できます。

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 for Research 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](#)
- [ステップ 2: 仮想コンピュータを作成する](#)
- [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](#)
- [ステップ 4: 仮想コンピュータに接続する](#)
- [ステップ 5: 仮想コンピュータにストレージを追加する](#)
- [ステップ 6: スナップショットを作成する](#)
- [ステップ 7: クリーンアップする](#)

ステップ 1: 前提条件を満たす

新規の AWS お客様は、Amazon Lightsail for Research の使用を開始する前に、セットアップの前提条件を完了してください。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

次の手順で説明するように、[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、「[Lightsail for Research のアプリケーションイメージとハードウェアプランを選択する](#)」および「[Lightsail for Research 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 AWS リージョン の を選択します。

レイテンシーを減らすには AWS リージョン 、物理的な場所に最も近い を選択します。

4. Lightsail のブループリントとも呼ばれるアプリケーションを選択しますAPI。

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. Lightsail のバンドルとも呼ばれるハードウェアプランを選択しますAPI。

ハードウェアプランは、vCPU コア、メモリ、ストレージ、毎月のデータ転送など、さまざまな処理能力を提供します。Lightsail for Research は、仮想コンピュータの標準プランと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。機械学習モデルやその他の計算負荷の高いタスクを実行する場合など、その要件が高い場合はGPU計画を選択します。

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、 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 コンソールで利用可能なブラウザベースのNICEDCVクライアントを使用します。ではNICEDCV、グラフィカルユーザーインターフェイス (GUI) を使用して、研究アプリケーションと仮想コンピュータのオペレーティングシステムとやり取りできます。

ブラウザベースのNICEDCV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し、ファイルを転送することもできます。

- Open 、 Pu SSH、 Windows Subsystem for Linux などのセキュアシェル (SSH) クライアントを使用してTTY、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ます。SSH クライアントを使用すると、スクリプトと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間でファイルを安全に転送します。を使用するとSCP、作業をローカルで開始し、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。

仮想コンピュータに接続するには、SSHまたは を使用してファイルを転送するには、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SCP。キーペアは、Lightsail for Research 仮想コンピュータに接続するときに ID 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:
 - [Lightsail for Research 仮想コンピュータアプリケーションにアクセスする](#)

- [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](#)
- を使用してSSH接続を確立するか、ファイルを転送しますSCP。
- [Lightsail for Research 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 Lightsail for Research 仮想コンピュータに接続する](#)
- [Secure Copy を使用して Lightsail for Research 仮想コンピュータにファイルを転送する](#)

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アタッチ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仮想コンピュータにディスクをアタッチすると、Lightsail for Research は自動的にディスクをフォーマットして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。

- [Lightsail for Research コンソールでストレージディスクを作成する](#)
- [Lightsail for Research コンソールでストレージディスクの詳細を表示する](#)
- [Lightsail for Research の仮想コンピュータにストレージを追加する](#)
- [Lightsail for Research の仮想コンピュータからディスクをデタッチする](#)
- [Lightsail for Research で未使用のストレージディスクを削除する](#)

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 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

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。

- [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](#)
- [Lightsail for Research での仮想コンピュータとディスクスナップショットの表示と管理](#)
- [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](#)
- [Lightsail for Research コンソールでスナップショットを削除する](#)

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、「[Lightsail for Research 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。

Lightsail for Research でデータサイエンスアプリケーションの使用を開始する

以下のチュートリアルでは、Lightsail for Research で利用可能な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

- [Lightsail for Research JupyterLab での起動と使用](#)
- [Lightsail for Research RStudioでの起動と使用](#)

Note

Lightsail for Research の使用を開始するための詳細なチュートリアルRStudioは、AWS 公共部門ブログに公開されています。詳細については、[Amazon Lightsail for Research の開始方法: を使用したチュートリアルRStudio](#)」を参照してください。

Lightsail for Research JupyterLab での起動と使用

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: ドキュメントを読む 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

まだ作成していない場合は、JupyterLab アプリケーションを使用して仮想コンピュータを作成します。詳細については、「[Lightsail for Research 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 of 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、ファイルの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、「[Lightsail for Research コンソールでストレージディスクを作成する](#)」および「[Lightsail for Research の仮想コンピュータにストレージを追加する](#)」を参照してください。

Note

コンソールを使用して仮想コンピュータにディスクをアタッチすると、Lightsail for Research はディスクを自動的に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、「[Lightsail for Research 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. キーペアを取得したら、Secure Copy (SCP) ユーティリティを使用して接続を確立できません。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せん。詳細については、「[Secure Copy を使用して Lightsail for Research 仮想コンピュータにファイルを転送する](#)」を参照してください。
3. (オプション) キーペアを使用して、で仮想コンピュータに接続することもできますSSH。詳細については、「[Secure Shell を使用して Lightsail for Research 仮想コンピュータに接続する](#)」を参照してください。

Note

ブラウザベースのNICE DCVクライアントを使用して、仮想コンピュータのコマンドラインインターフェイスにアクセスし、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、「[Lightsail for Research 仮想コンピュータアプリケーションにアクセスする](#)」および「[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](#)」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仮想コンピュータにディスクをアタッチすると、Lightsail for Research は自動的にディスクをフォーマットして `/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

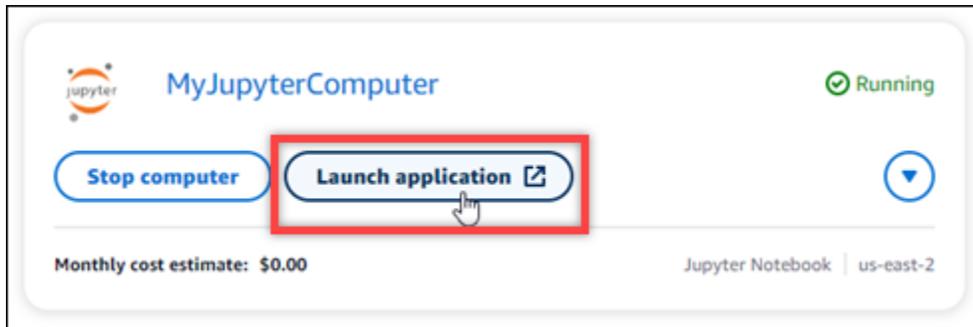
新しい仮想コンピュータで JupyterLab アプリケーションを起動するには、次の手順を実行します。

Important

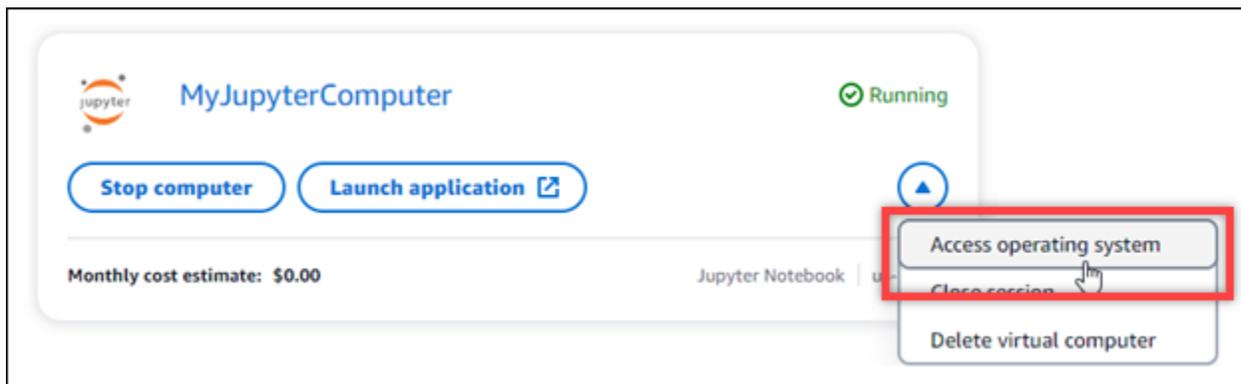
オペレーティングシステムや JupyterLab アプリケーションは、更新を求められた場合でも更新しないでください。更新せず、これらのプロンプトを閉じるか無視するよう選択してください。さらに、`/home/lightsail-admin/` ディレクトリにあるファイルは変更しないでください。これらの操作により、仮想コンピュータが使用できなくなる可能性があります。

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) アプリケーションを起動 を選択して、JupyterLab 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。



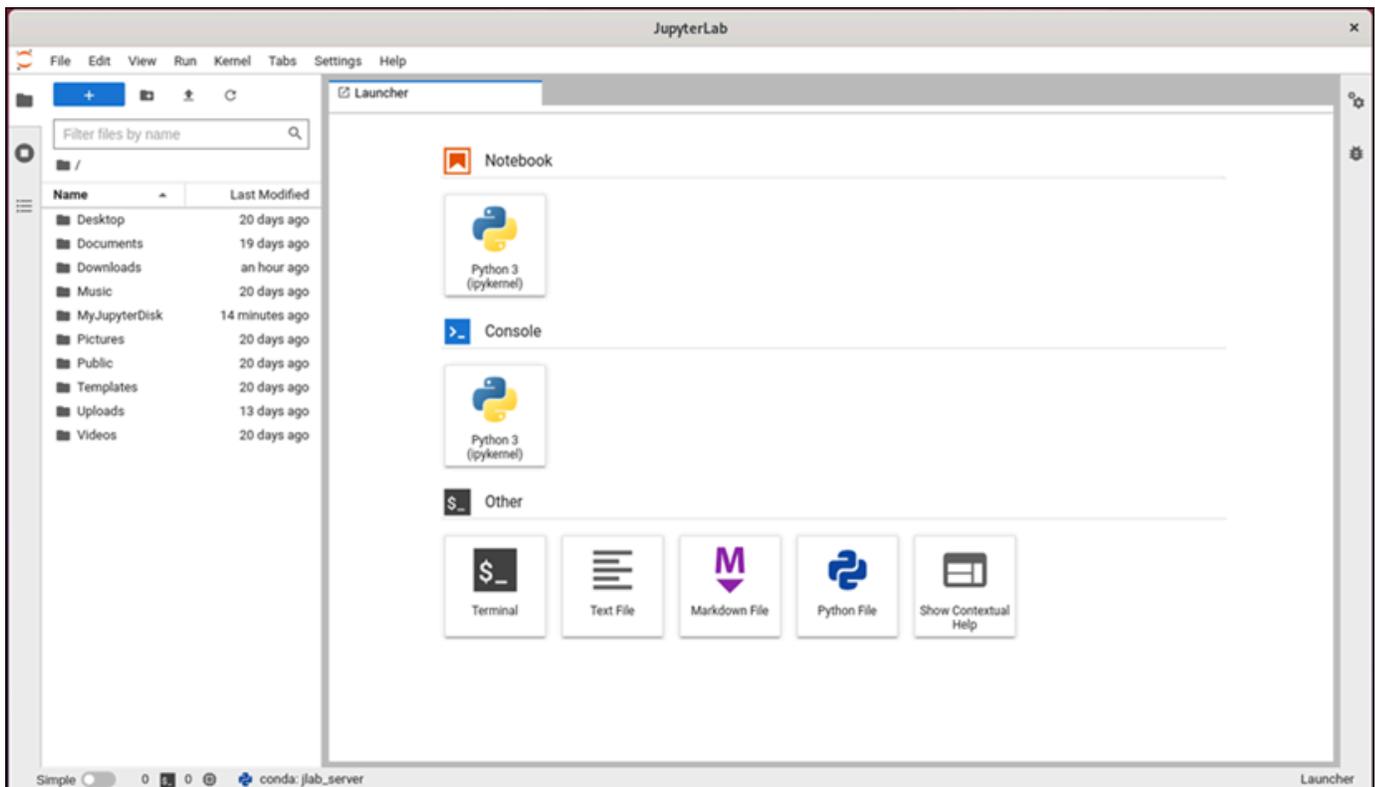
Lightsail for Research は、いくつかのコマンドを実行してリモートディスプレイプロトコル接続を開始します。しばらくすると、新しいブラウザタブウィンドウが開き、仮想コンピュータとの仮想デスクトップ接続が確立されます。アプリケーションの起動オプションを選択した場合は、この手順の次のステップに進み、JupyterLab アプリケーションでファイルを開きます。[オペレーティングシステムにアクセス] オプションを選択した場合は、Ubuntu デスクトップから他のアプリケーションを開くことができます。

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。

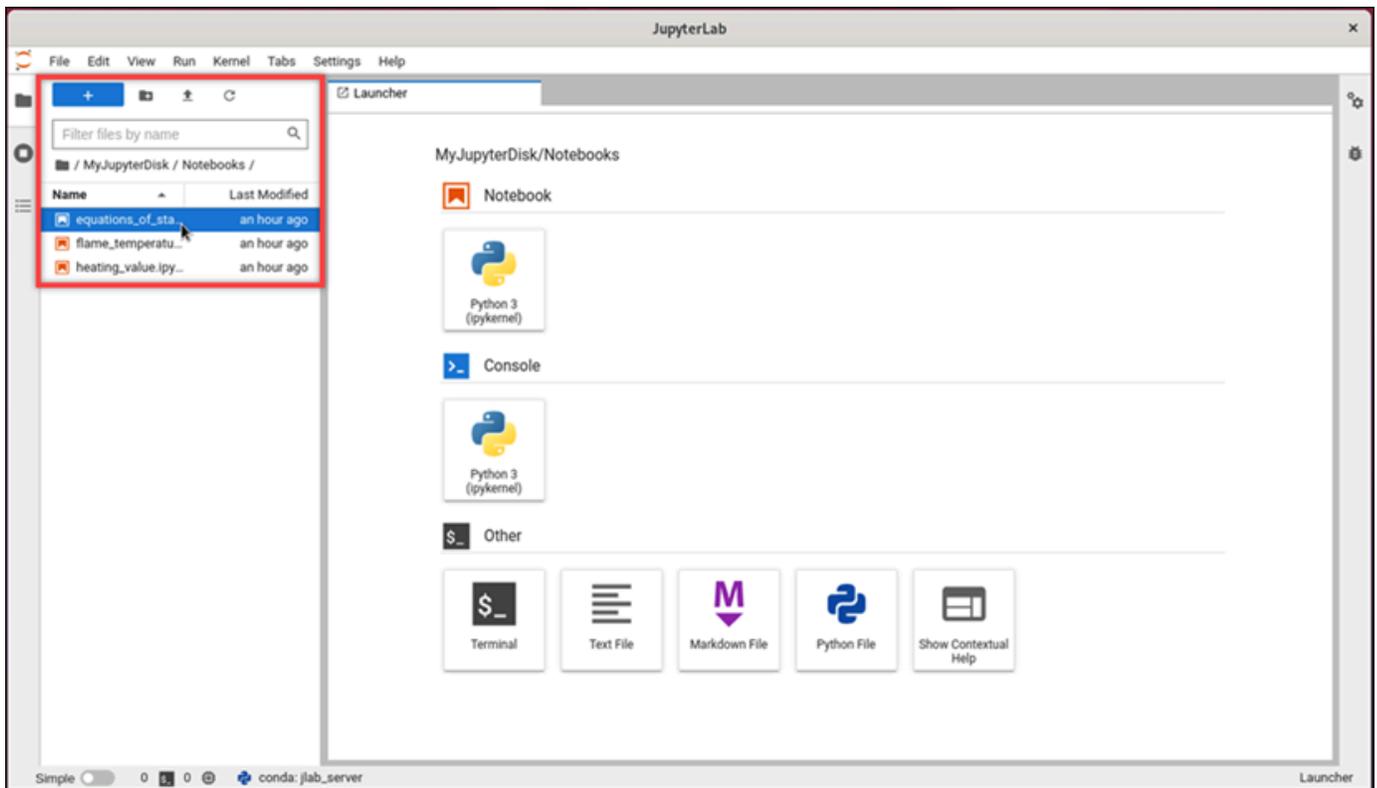
4. JupyterLab アプリケーションが開きます。ランチャーメニューでは、新しいノートブックの作成、コンソールの起動、ターミナルの起動、さまざまなファイルの作成を行うことができます。



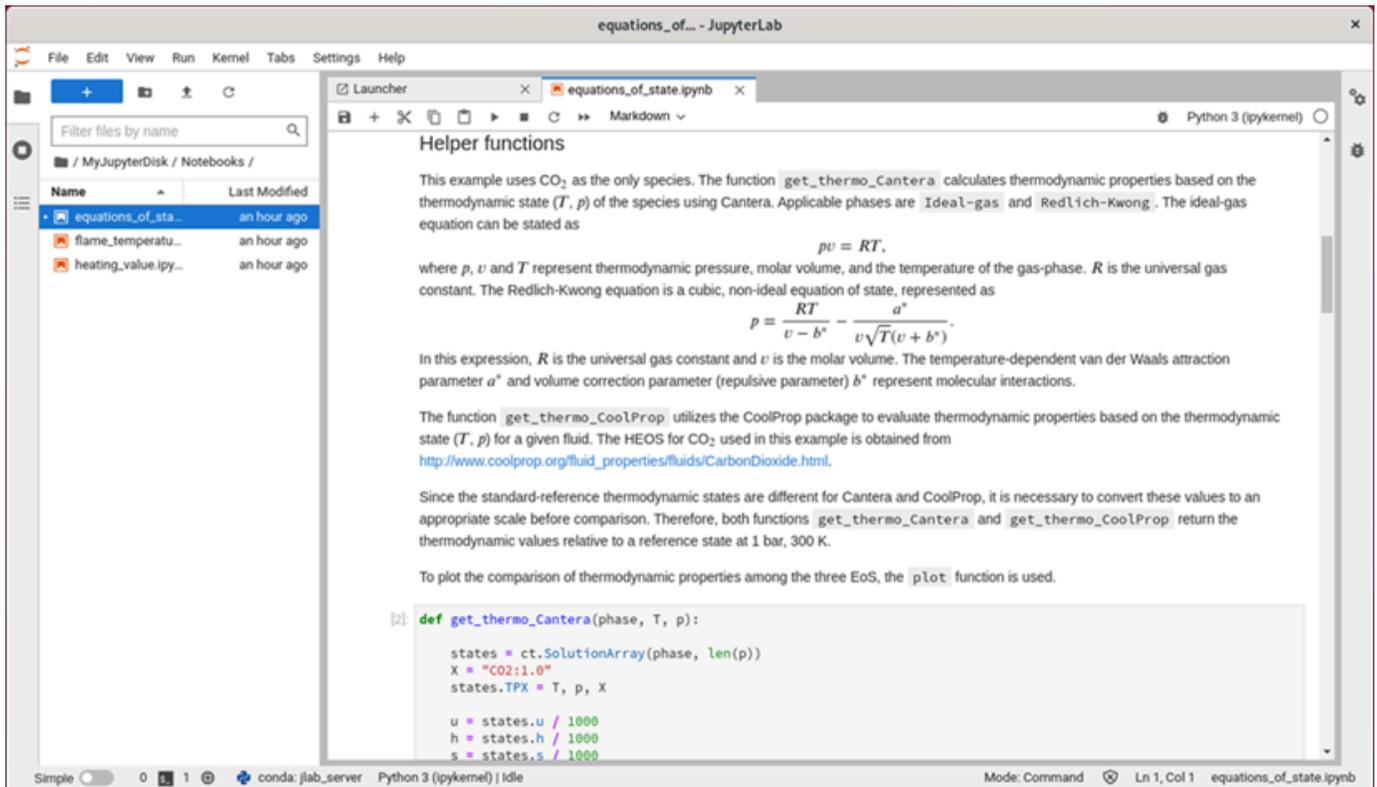
5. でファイルを開くには JupyterLab、ファイルブラウザペインで、プロジェクトファイルが保存されているディレクトリまたはフォルダを選択します。次に、ファイルを選択して開きます。

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: ドキュメントを読む JupyterLab](#) セクションに進みます。

ステップ 5: ドキュメントを読む JupyterLab

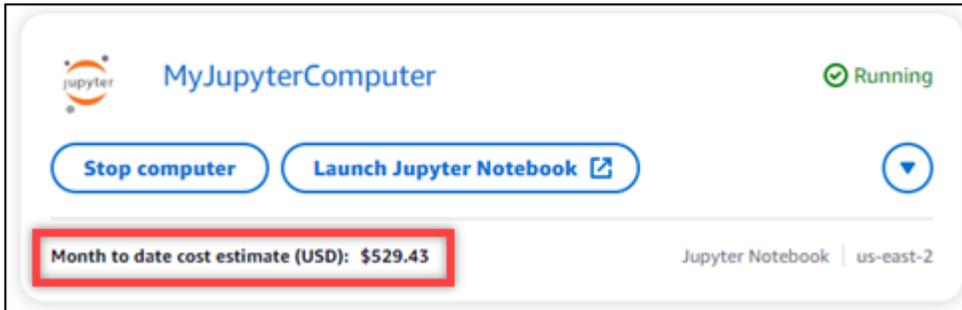
に慣れていない場合は JupyterLab、公式ドキュメントを読むことをお勧めします。以下の JupyterLab オンラインリソースを利用できます。

- [JupyterLab ドキュメント](#)
- [Jupyter Discourse Forum](#)
- [JupyterLab 上の StackOverflow](#)
- [JupyterLab 上の GitHub](#)

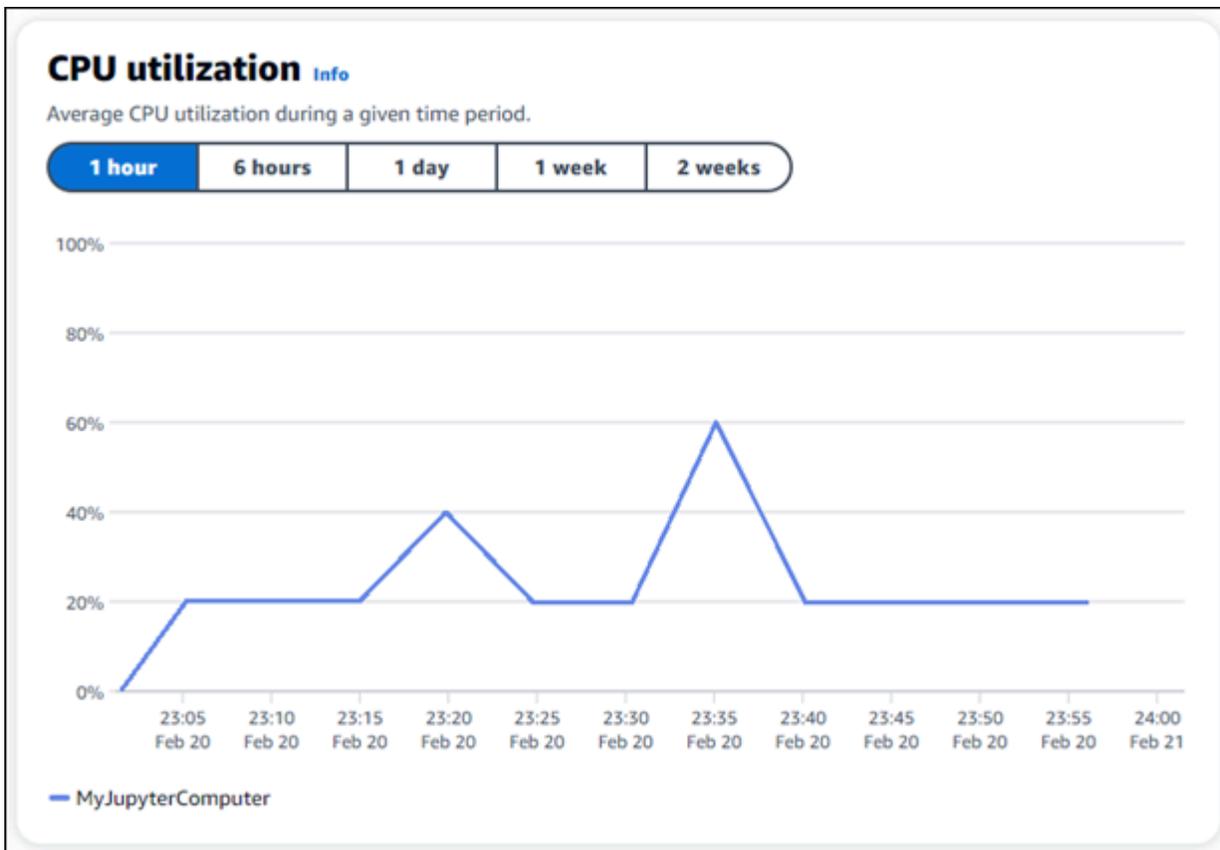
ステップ 6: (オプション) 使用量とコストをモニタリングする

Lightsail for Research リソースの月初来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 リソースの月初来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「使用状況」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.

Q Filter by name < 1 > ⚙

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

Disks

Q Filter by name < 1 > ⚙

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

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。アイドル状態のルールで Stop 仮想コンピュータを作成し、特定の期間中にCPU指定された使用率に達したときに実行中のコンピュータを停止できます。例えば、ルールは、30 分間のCPU使用率が 5% 以下の場合に、特定のコンピュータを自動的に停止できます。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

アイドル状態で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勧めします。仮想コンピュータの負荷が異なる間は、CPU使用率を書き留めておきます。例えば、コードのコンパイル時、操作の処理中、アイドルリング時などです。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内の「[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。

ワークロードよりも高いCPU使用率のしきい値を持つルールを作成すると、そのルールは仮想コンピュータを連続して停止できます。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。

- [Lightsail for Research でコスト管理ルールを管理する](#)
- [Lightsail for Research 仮想コンピュータのコスト管理ルールを作成する](#)
- [Lightsail for Research 仮想コンピュータのコスト管理ルールを削除する](#)

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。

- [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](#)
- [Lightsail for Research での仮想コンピュータとディスクスナップショットの表示と管理](#)
- [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](#)
- [Lightsail for Research コンソールでスナップショットを削除する](#)

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

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、「[Lightsail for Research 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。

Lightsail for Research RStudioでの起動と使用

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 の使用を開始するための詳細なチュートリアルRStudioは、AWS 公共部門ブログに公開されています。詳細については、「[Amazon Lightsail for Research の開始方法: を使用したチュートリアル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 4: RStudioアプリケーションを起動する](#)
- [ステップ 5: RStudioドキュメントを読む](#)
- [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

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仮想コンピュータを作成します。詳細については、「[Lightsail for Research 仮想コンピュータを作成する](#)」を参照してください。

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、ファイルの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、「[Lightsail for Research コンソールでストレージディスクを作成する](#)」および「[Lightsail for Research の仮想コンピュータにストレージを追加する](#)」を参照してください。

Note

コンソールを使用して仮想コンピュータにディスクをアタッチすると、Lightsail for Research はディスクを自動的に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 `<disk-name>` 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。

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

RStudio 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、「[Lightsail for Research 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. キーペアを取得したら、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 Lightsail for Research 仮想コンピュータにファイルを転送する](#)」を参照してください。
3. (オプション) キーペアを使用して、で仮想コンピュータに接続することもできますSSH。詳細については、「[Secure Shell を使用して Lightsail for Research 仮想コンピュータに接続する](#)」を参照してください。

Note

ブラウザベースのNICE DCVクライアントを使用して、仮想コンピュータのコマンドラインインターフェイスにアクセスし、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、「[Lightsail for Research 仮想コンピュータアプリケーションにアクセスする](#)」および「[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](#)」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

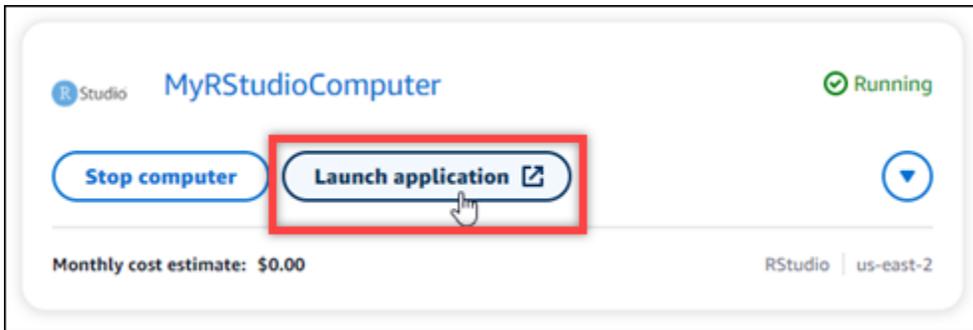
新しい仮想コンピュータでRStudioアプリケーションを起動するには、次の手順を実行します。

Important

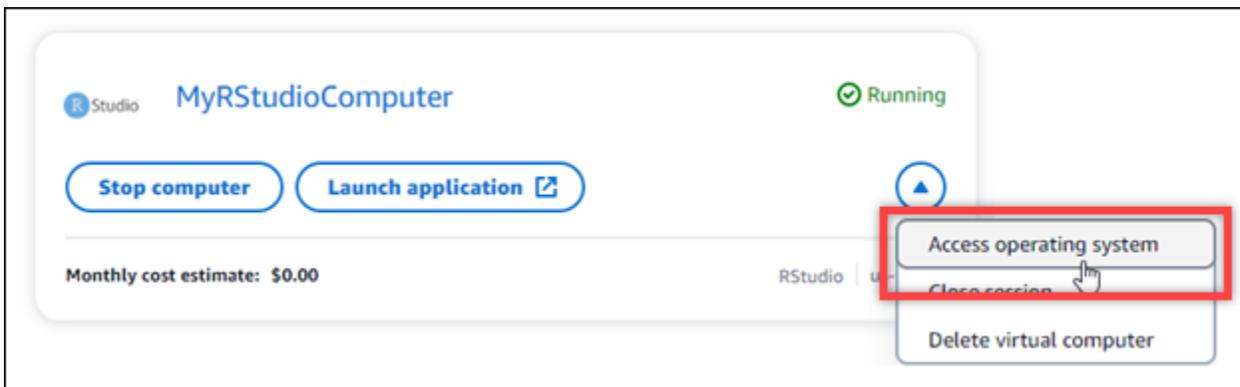
オペレーティングシステムやRStudioアプリケーションは、更新を求められた場合でも更新しないでください。更新せず、これらのプロンプトを閉じるか無視するよう選択してください。さらに、/home/lightsail-admin/ ディレクトリにあるファイルは変更しないでください。これらの操作により、仮想コンピュータが使用できなくなる可能性があります。

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) アプリケーションを起動 を選択して、アプリケーションをフォーカスRStudio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。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。

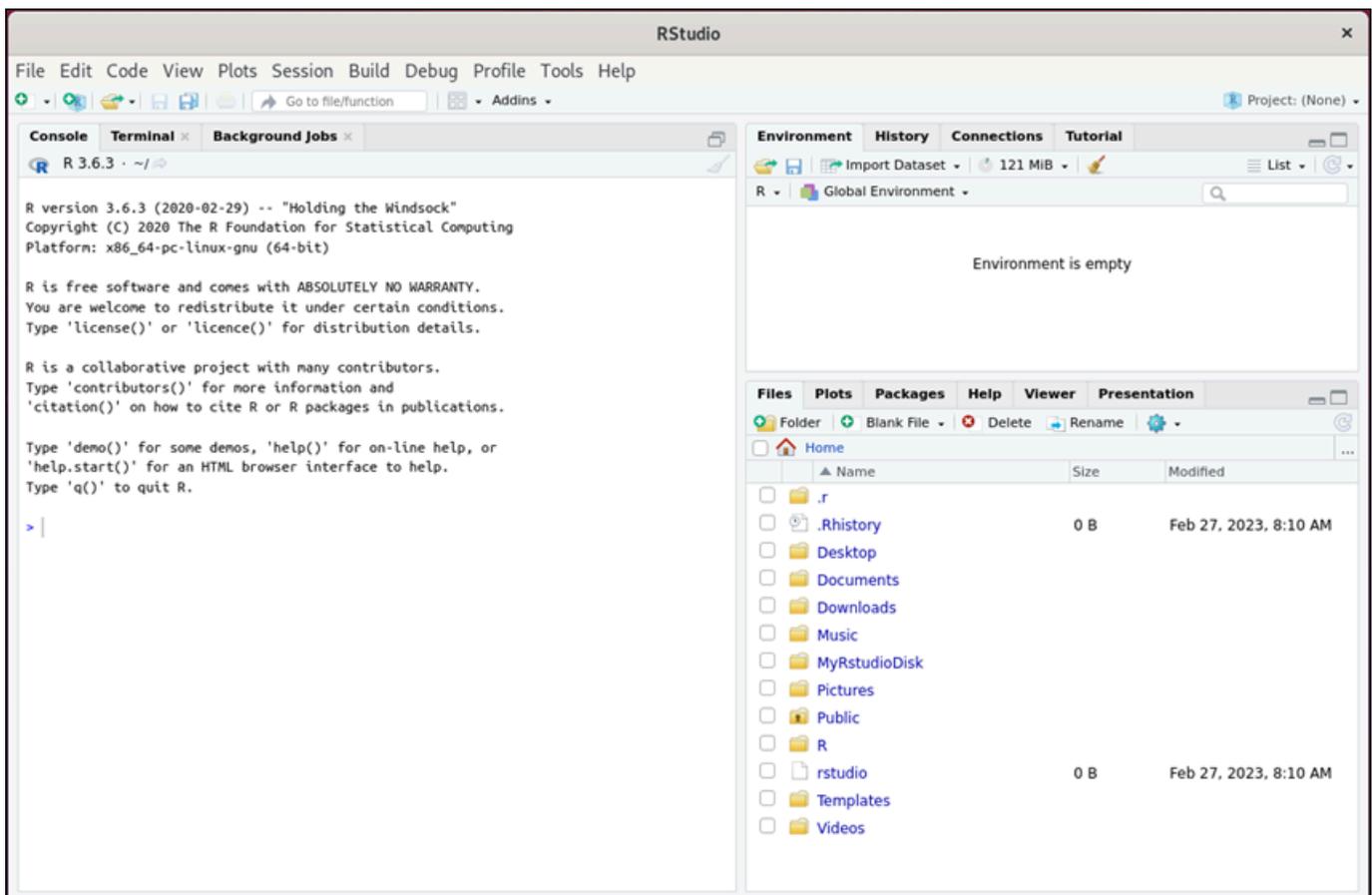


Lightsail for Research は、いくつかのコマンドを実行してリモートディスプレイプロトコル接続を開始します。しばらくすると、新しいブラウザタブウィンドウが開き、仮想コンピュータとの仮想デスクトップ接続が確立されます。アプリケーションの起動オプションを選択した場合は、この手順の次のステップに進み、RStudioアプリケーションでファイルを開きます。[オペレーティングシステムにアクセス] オプションを選択した場合は、Ubuntu デスクトップから他のアプリケーションを開くことができます。

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。

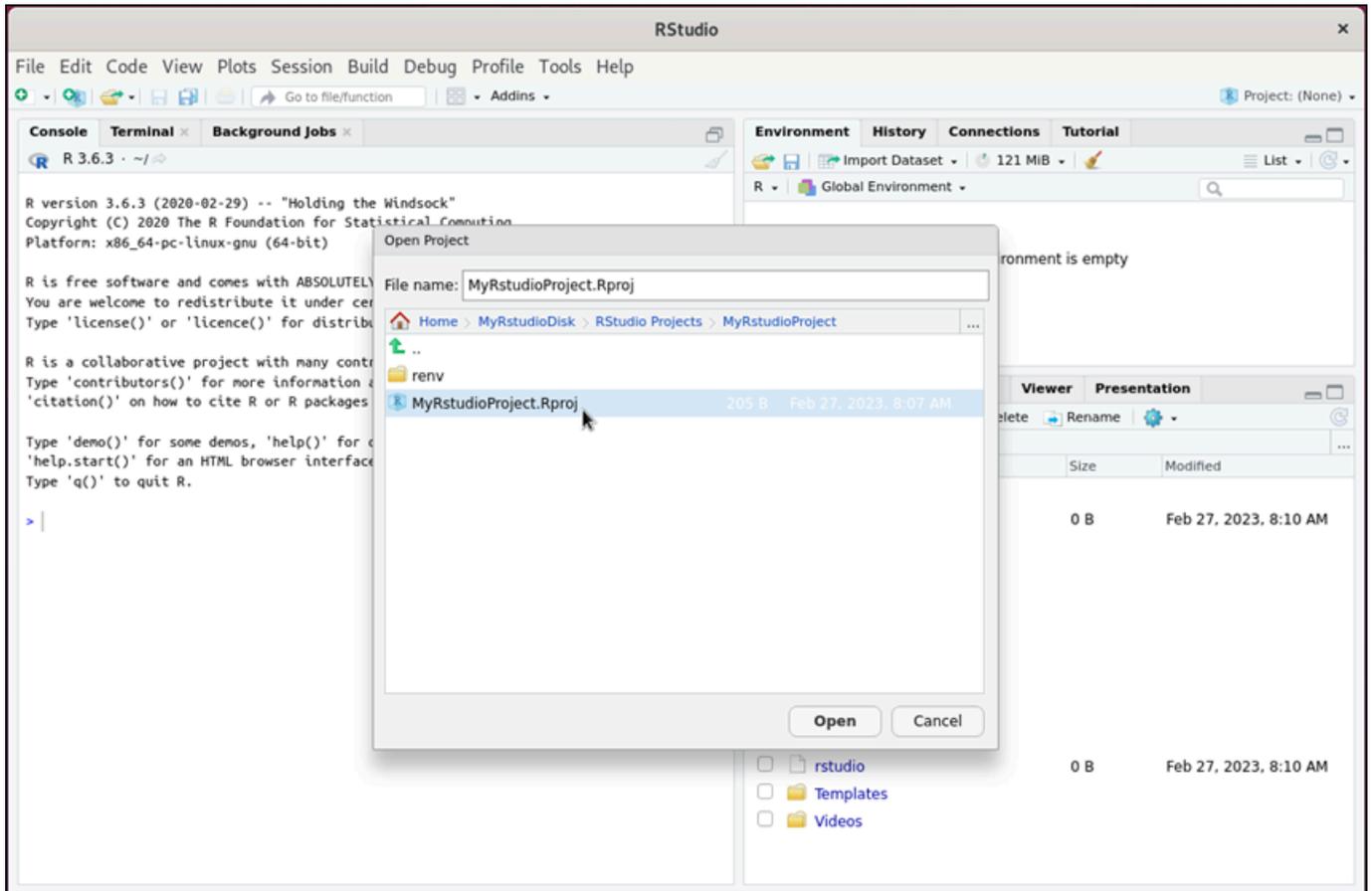
Ubuntu から初期設定を求めるメッセージが表示されることもあります。セットアップが完了し、オペレーティングシステムを使用できるようになるまで、プロンプトに従います。

4. RStudio アプリケーションが開きます。

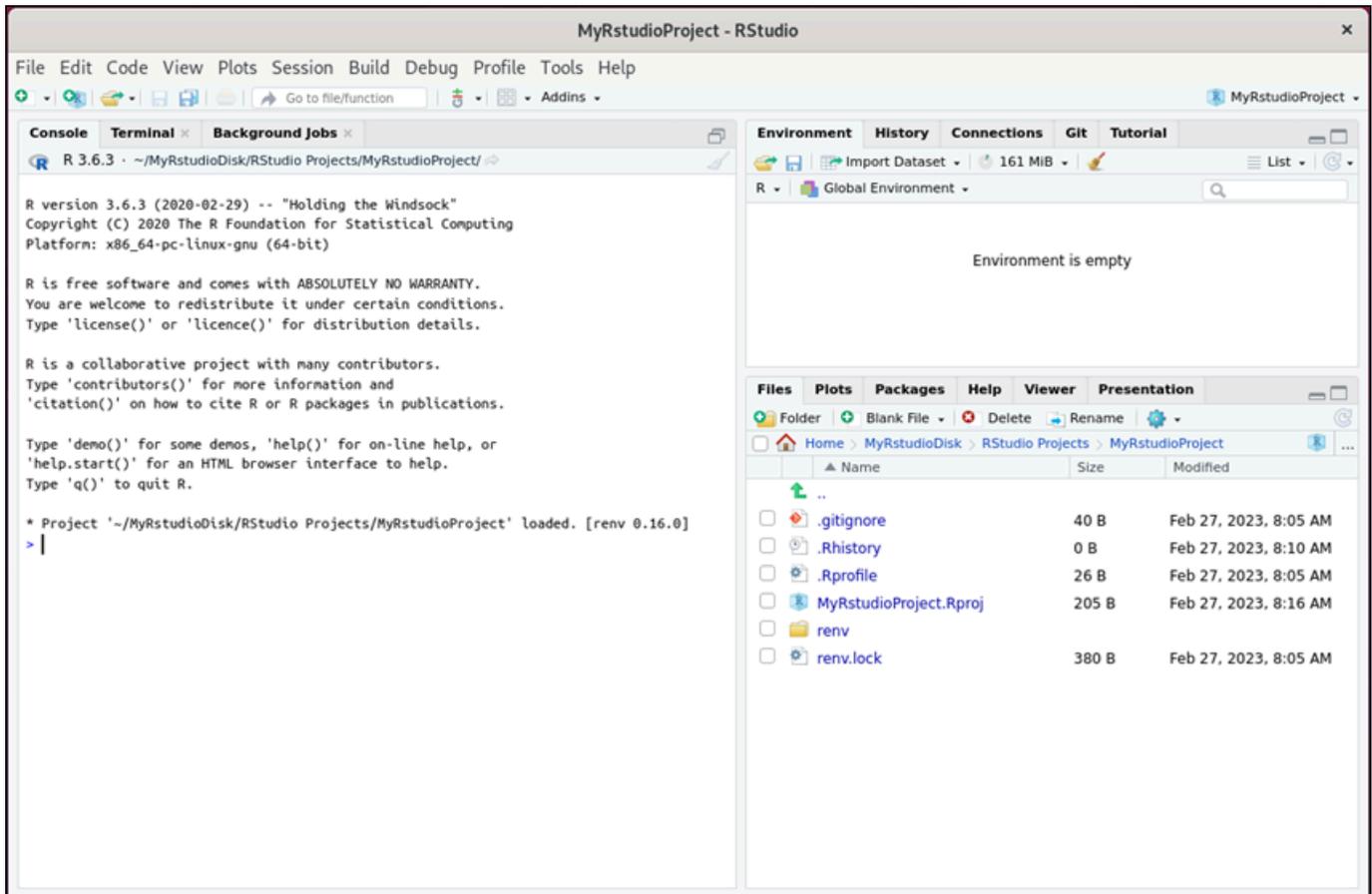
5. でプロジェクトを開くにはRStudio、ファイルメニューを選択し、プロジェクトを開くを選択します。プロジェクトファイルが保存されているディレクトリまたはフォルダに移動します。次に、ファイルを選択して開きます。

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。



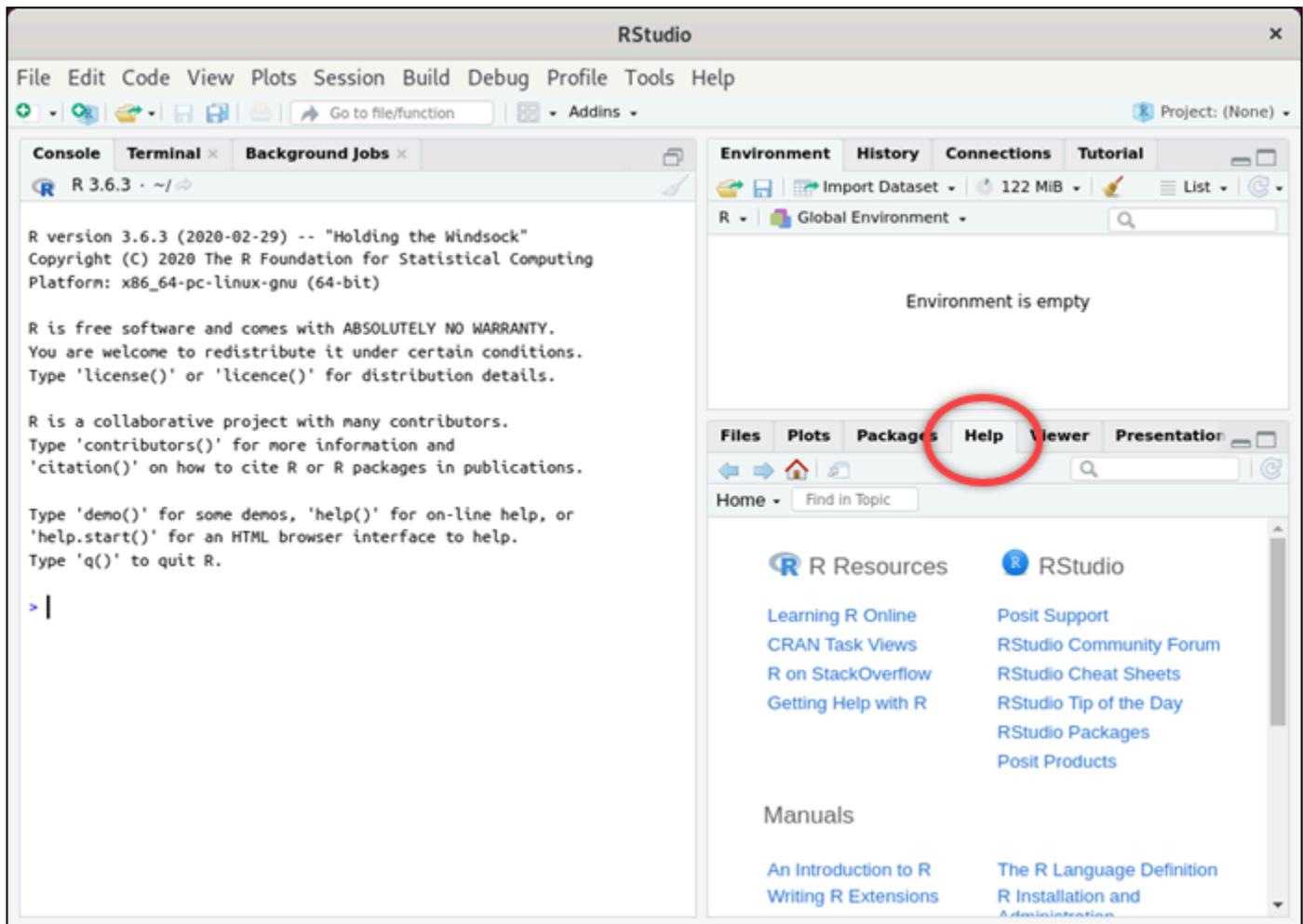
次の例では、MyRstudioProject.Rproj プロジェクトファイルを開きました。



の使用を開始する方法についてはRStudio、このチュートリアルの[ステップ 5: RStudioドキュメントを読む](#)「」セクションに進んでください。

ステップ 5: RStudioドキュメントを読む

RStudio アプリケーションは包括的なドキュメントパッケージにバンドルされています。の学習を開始するにはRStudio、次の例RStudioに示すように、のヘルプタブにアクセスすることをお勧めします。



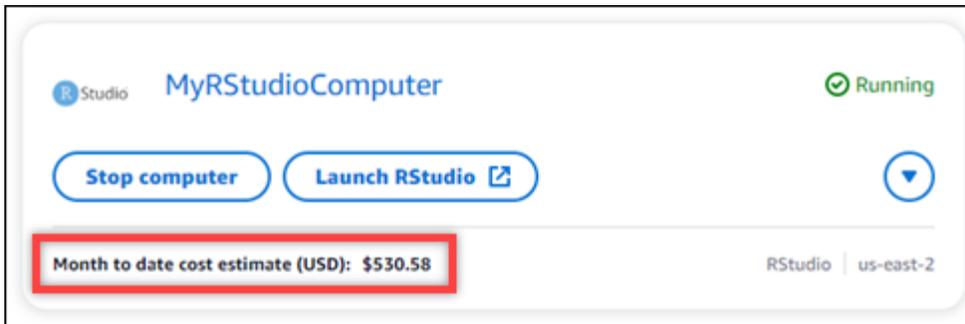
以下のRStudioオンラインリソースも利用できます。

- [Learning R Online](#)
- [の R StackOverflow](#)
- [Getting Help with R](#)
- [Posit Support](#)
- [RStudio コミュニティフォーラム](#)
- [RStudio チートシート](#)
- [RStudio Tip of the Day \(ツイッター\)](#)
- [RStudio パッケージ](#)

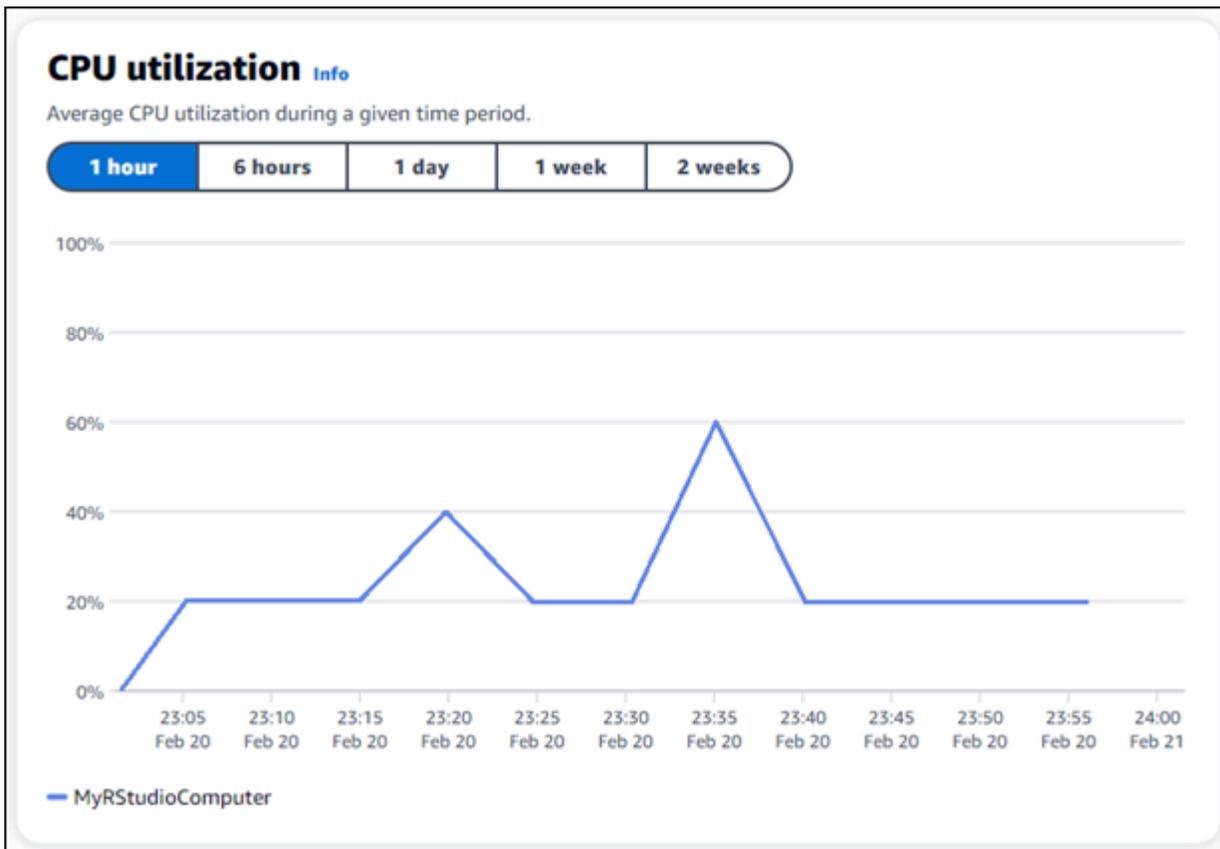
ステップ 6: (オプション) 使用量とコストをモニタリングする

Lightsail for Research リソースの月初来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 リソースの月初来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「使用状況」を選択します。

The screenshot displays two sections of the Amazon Lightsail console. The top section, titled 'Virtual computers', shows a table with columns for Name, Region, Month to date cost estimate (USD), and Usage estimate (hours). The bottom section, titled 'Disks', shows a similar table with columns for Name, Region, Month to date cost estimate (USD), and Usage estimate (GB). Both sections include a search filter and pagination controls.

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

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

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。アイドル状態のルールで Stop 仮想コンピュータを作成し、特定の期間中にCPU使用率が指定された割合に達したときに実行中のコンピュータを停止できます。例えば、ルールは、30 分間のCPU使用率が 5% 以下の場合に、特定のコンピュータを自動的に停止できます。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

アイドル状態で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勧めします。仮想コンピュータの負荷が異なる間は、CPU使用

率を書き留めておきます。例えば、コードのコンパイル時、操作の処理中、アイドル時などです。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内の「[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。

ワークロードよりも高いCPU使用率のしきい値を持つルールを作成すると、そのルールは仮想コンピュータを連続して停止できます。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。

- [Lightsail for Research でコスト管理ルールを管理する](#)
- [Lightsail for Research 仮想コンピュータのコスト管理ルールを作成する](#)
- [Lightsail for Research 仮想コンピュータのコスト管理ルールを削除する](#)

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。

- [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](#)
- [Lightsail for Research での仮想コンピュータとディスクスナップショットの表示と管理](#)
- [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](#)
- [Lightsail for Research コンソールでスナップショットを削除する](#)

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

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、「[Lightsail for Research 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。

Lightsail for Research での仮想コンピュータの作成と管理

Amazon Lightsail for Research を使用すると、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 仮想コンピュータはデフォルトでIMDSv2適用されます。

トピック

- [Lightsail for Research のアプリケーションイメージとハードウェアプランを選択する](#)
- [Lightsail for Research 仮想コンピュータを作成する](#)
- [Lightsail for Research 仮想コンピュータの詳細を表示する](#)
- [Lightsail for Research 仮想コンピュータアプリケーションにアクセスする](#)
- [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](#)
- [Lightsail for Research 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](#)
- [Lightsail for Research 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 Lightsail for Research 仮想コンピュータに接続する](#)
- [Secure Copy を使用して Lightsail for Research 仮想コンピュータにファイルを転送する](#)
- [Lightsail for Research 仮想コンピュータを削除する](#)

Lightsail for Research のアプリケーションイメージとハードウェアプランを選択する

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、メモリ、ストレージ領域vCPUs、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、「[Lightsail for Research スナップショットを使用して仮想コンピュータとディスクをバックアップする](#)」を参照してください。

トピック

- [アプリケーション](#)
- [プラン](#)

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、次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 – は、統計計算とグラフィック用のプログラミング言語である R と Python 用のオープンソースの統合開発環境 (IDE) RStudio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、「[RStudioIDE](#)」を参照してください。

- VSCodium – VSCodiumは、Microsoft のエディタ 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、「」を参照してください[VSCodium](#)。
- 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 に基づくオープンソースの 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 (vCPUs)、SSDベースのストレージボリューム (ディスク) スペース、および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用の費用対効果の高い高性能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

以下は、Lightsail for Research で利用可能な標準プランのハードウェア仕様です。

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

以下は、Lightsail for Research で利用可能なGPUプランのハードウェア仕様です。

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

Lightsail for Research 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、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. 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、「[Lightsail for Research のアプリケーションイメージとハードウェアプランを選択する](#)」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。

6. [概要] パネルで [仮想コンピュータを作成] を選択します。

Lightsail for Research 仮想コンピュータは数分で準備でき、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[Lightsail for Research 仮想コンピュータアプリケーションにアクセスする](#)。

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、[Lightsail for Research 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。

Lightsail for Research 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。
- 月初来のコスト見積もり — 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 使用率を表示することもできます。CPU 使用率は、仮想コンピュータのアプリケーションで使用される処理能力を識別します。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を検索およびフィルタリングしたり、AWS コストを追跡したりできます。

Lightsail for Research 仮想コンピュータアプリケーションにアクセスする

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、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。

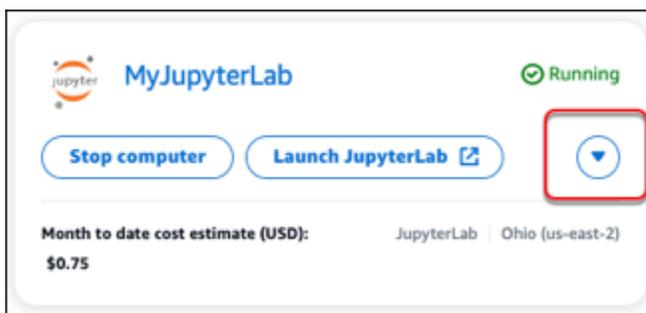
⚠ Important

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。

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

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、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。

Lightsail for Research 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、接続が許可されているプロトコル、ポート、および送信元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2つのファイアウォールがあります。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クライアントとアプリケーション間の接続を確立および維持するために使用します。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。
- User Datagram Protocol (UDP) は、主に、仮想コンピュータで実行されているクライアントとアプリケーション間の低レイテンシーおよび損失許容接続を確立するために使用されます。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。
- Internet Control Message Protocol (ICMP) は、主に、データが意図した宛先にタイムリーに到達しているかどうかを判断するなど、ネットワーク通信の問題を診断するために使用されます。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 - セキュアシェル () に使用されますSSH。
 - 80 - Hypertext Transfer Protocol () に使用されますHTTP。
 - 443 - Hypertext Transfer Protocol Secure () に使用されますHTTPS。
 - 8443 - Hypertext Transfer Protocol Secure () に使用されますHTTPS。

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。例えば、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 TCPを超えることを許可するファイアウォールルールを設定します。この場合、SSH仮想コンピュータへの接続を確立するために IP アドレスを許可しません。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既に設定されている場合は、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することができます。

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](#)
- [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を開く](#)
- [仮想コンピュータのポートを閉じる](#)
- [次のステップに進みます](#)

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、「[Lightsail for Research 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、コマンドリファレンス[get-instance-port-states](#)の「」を参照してください。AWS CLI

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。
- 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
```

レスポンスには、開いているポートとプロトコル、および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。

```
% 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、コマンドリファレンス [open-instance-public-ports](#) の「」を参照してください。AWS CLI

- 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。例えば、などです 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
```

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

```
% 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、[コマンドリファレンス](#) `close-instance-public-ports` の「」を参照してください。AWS CLI

- 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。
- 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。例えば、`tcp` などです 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
```

レスポンスには、閉じられ、仮想コンピュータへの接続が許可されなくなったポート、プロトコル、および IP CIDR 範囲が表示されます。

```
% 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、Open、SSHPu、Linux 用 Windows サブシステムなど TTY、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、「[Lightsail for Research 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。
- を使用して仮想コンピュータに接続 SSH 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 Lightsail for Research 仮想コンピュータにファイルを転送する](#)」を参照してください。
- を使用して仮想コンピュータに接続し SCP、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 Lightsail for Research 仮想コンピュータにファイルを転送する](#)」を参照してください。

Lightsail for Research 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 ID 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。プライベートキーを使用すると、仮想コンピュータで 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。

Amazon Lightsail のデフォルトキーペア (DKP) は、初めて Lightsail インスタンスまたは Lightsail for Research 仮想コンピュータを作成するときに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 (us-east-2) DKP の Lightsail は、作成 DKP 時に使用するよう設定された Lightsail および Lightsail for Research で米国東部 (オハイオ) で作成した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 DKP に のパブリックキーを自動的に保存します。Lightsail サービスを API 呼び出すことで、 のプライベートキーを DKP 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 DKP の を取得する方法について説明します。 を取得したら DKP、Open 、SSHPu 、Linux 用 Windows サブシステムなど TTY、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。この 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、「[Lightsail for Research 仮想コンピュータアプリケーションにアクセスする](#)」および「[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](#)」を参照してください。

トピック

- [前提条件を満たす](#)
- [仮想コンピュータのキーペアを取得する](#)
- [次のステップに進みます](#)

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、「[Lightsail for Research 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、 のJSON出力からキーペアの詳細を抽出するために、以下の手順で使用される軽量で柔軟なコマンドラインJSONプロセッサです AWS CLI。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DKPの Lightsail 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、コマンドリファレンス[download-default-key-pair](#)の「」を参照してください。AWS CLI

1. [コマンドプロンプト] 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 `dcp-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 > dcp-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。



```

{
  "publicKeyBase64": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC/jth+pVU5QhlgZHgsWLSwcoGFUR9DimCRUG1MVQ3jsaQma
+McSV0W/7tMBNDxGMVApQ1mAoZKoAOTFCaUnzzUNbGmBYreybrennuOIRSnUR1FsBzNF2PqBrnM17bY51o5Kkp1g0IKk+m6L
+KW7QA1M2Ry/WeiCponFA48VRfu6peNH4U/w0RKVyw1XqZack5yM2n0ExhvybmaQwJNBQnzt5/FFxhYgB
+OJMN241viASUY4EMgMiCsfwayTwOULjdr+ps1wIwlgM33TyoyRe1Rrx03qP53AgDtEk1SDILSxNR+kzDe8N8x
+S13hkqkA1ZT9kCtuNYdtSXDePotsmwL",
  "privateKeyBase64": "-----BEGIN RSA PRIVATE KEY-----
\EXAMPLEBAAKCAQEAv47YfqVVOUIZYGR4LF17HMKbHVEfQ4pgkVINTFUN47GkJmvj
\nEXAMPLE7TATQ8RjFQKUNzGKGSqADrRQm1J881DwXpgWk3sm63p57jiEUp1EdRbAc
\nEXAMPLE5zNe220da0SpKdYnCCpPpui/ilu0AJTNkcv1nogqaJ3wOPFUX7uqXjR+F
\nEXAMPLEsJV6mWnJ0cJn9BMYb8m5mkMCTQUJ87efxRcYwIAfjiTDduNb4gE1G0BD\nEXAMPLEGsk8D1C43a/qbNcFoJTHd908qMkXtUa8T6j
+dwIA7RjNUgyC0sTufPmW\nEXAMPLEEot4ZKpANWU/ZArbjwHbU1w3j6LbJscwIDAQABAoIBACSwVleCcQLc0gM
\nEXAMPLEFoU07uQMhNwZki9G2tU52keoc1WaDxNotwrLEgLxshNDSNfr0JH6AjfMz
\nEXAMPLExdFtH17yyP5V1jCuDuhQzdCnpd7bc7uK2oiq0UwKg3iTpJQvJJiYstoov
\nT1IotsxkQp2MNY1IBSXh1j6D6mxh4cjF2/990yeJtvttdtEsjDgJ1bSsePEejp1z
\nbRskG9ktq8huRLeixjVby1FdJNU5/OGaz0IeiIneKy58ejt2ZAvCXdXh1VwxQL6Q
\nCN0HGjHBbho6SNfmE3raLrJML6RfVbzYtVFe72GuFkKjID6ypU2ffPNZLNI9TaxL
\nq2PPKuECgYEA9Jh4cv8zeS1zYL1vpmuJL7FAEfVuj0WswnoXC14DRJWzweb/Pnx/\nxLXLUZ4WxreSq0/j503VgJVf8182lg
+F15t5naH13Lf/AIzfJ2Im2Bw+hHk1GFp\nLIVc4imaRk2g6ykfm7Y20q5RHfzow8MPMeWhFQR27ibqdKJxNBR9iBMCgYEAyH1P
\nfHxSY0Cxb0n5/0Pv72tNdDi4z2aDX8AiljtYLL1DMJFHpB00M/yCp+qhmhvI3lry\nVHnMthfkwGxEU7nQnyL
+d1hgA3tAFnKa1ckpvVmqfQgNlyI9Wpkgm/F1BNecCSSQ\nnyF2bURFFKirHwCS2tXX3C55V31tZfYEDum/+ykCgYEA6PZfoofWqswEDFgSM1vJ
\nrZ8Q+xANA4Csa3aFhFoimqwykCtYwKJXv4Wd1DsSTmqB05DF6idsdm/PVogJYZu\nnfSt/WUYD0/yhwREHo0Ua04L11IM
+Rusos7DyzKX7PoKphdFBPbmrNba5o+pCeFHM\nnoyWm6rG55NjD9JrTX1s0xOkCgYAZCIR/P6qt1+sPwUXk2J/B3j0KkPaKdvtaXkwz\nnQ+
+rjmowS0Nuh9cYGAUBVjuPB/lm6d8YsTry6n1pWcd1SOZCqITrc+5XiNeMtfy
\nndSwPaL7L4760A81zYYFP12NMGnvSLG2jhwSYqIYm0LaZf9VsbPF00xN0WbAONhy1\nnnAwrmQKBgELp/Bz6bX85aqby1IxRkGS69Wjb1Aq
+gwEhUb6//Rpej4CLN1MLAV1\nnvrSHQe0GYnhvdhkhxeX7NYGsUA/udwr6zn1800LyWh9RgVEh1pNtP8KRLQ873c1jW
\negFu1PWyvpa944PUI5AbXIs1LudJNV0LeCWZ2/Qcji40W3RqaLMh\n-----END RSA PRIVATE KEY-----\n",
  "createdAt": "2022-02-02T16:17:09.600000-08:00"
}

```

- 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。

```

-----BEGIN RSA PRIVATE KEY-----
EXAMPLEBAAKCAQEAv47YfqVVOUIZYGR4LFi7HMKBhVEfQ4pgkVINTFUN47GkJmvj
EXAMPLE7TATQ8RjFQKUNZjKGSqADrRQm1J881DwxpgWk3sm63p57j1EUp1EdRbAc
EXAMPLE5zNe220daOSpKdYnCCpPpui/ilu0AJTNkcv1nogqaJ3wOPFUX7uqXjR+F
EXAMPLEsJV6mWnJ0cjNp9BMYb8m5mkMCTQUJ87efxRcYwIAfjiTDduNb4gE1GOBD
EXAMPLEGsk8D1C43a/qbNcFoJTHd908qMkXtUa8Tt6j+dwIA7RJNUgyC0sTUfpMw
EXAMPLERot4ZKpANWU/ZArbjwHbU1w3j6LbJscwIDAQABoIBACSWv1eCcQLc00gM
EXAMPLERFoU07uQMhNwZki9G2tU52keoc1WaDxNotwrLEgLxshNDSNfr0JH6AjfMz
EXAMPLERkdFtH17yyP5V1JCuDuhQzdCnpd7bc7uK2oiq0UWKg3iTpJQvJJYIystoov
t1IotsxkQp2MNY1IBSXh1j6D6mxh4cjF2/990yeJtvttdtEsjDgJ1bSsePEejp1z
bRskG9ktq8huRLeixjVby1FdJNU5/OGaz0IeiNeKy58ejt2ZAvXdxh1VwQL6Q
CN0HGjHbho6SNfmE3raLrJML6RfVbzYtVfE72GuFkKjID6ypU2ffPNZLNI9TaxL
q2PPKuECgYEA9Jh4cv8zeS1zYL1vpmujL7FAEfVuj0WswnoXC14DRJWZweb/Pnx/
xLXLUZ4WxreSq0/j503VgJVf8i821g+F15t5naH13Lf/AIzFJ2Im2Bw+hHk1GfP
LIvc4imaRk2g6ykfm7Y20q5RHfzow8MPMeWhFQR271bqdKJxNBR9iBMCgYEAyH1P
fHxSY0Cxb0n5/0Pv72tNdD14z2aDX8A11jtYLL1DMJFHpB00M/yCp+qhmhvI31ry
VHnMthfkwtGxEU7nQnyL+d1hgA3tAFnKa1ckpvVmqfQgNyI9Wpkgm/F1BNecCSSQ
yF2bURFFK1rHwC52tXX3C55Vv31tZfYEDum/+ykCgYEA6PZfoofWqswEDFgSM1vJ
rZ8Q+ANA4Csa3aFhFoimqvyKjCtYwKJXv4Wd1DsStmqB05Df6idsdm/PVogJYZu
fSt/WUYD0/yhwREHoOUa04Li1IM+Rusos7DyzKX7PoKphdFBPbmrNba5o+pCeFHM
oyWm6rG55NJD9JrTX1s0xOkCgYAZCIR/P6qt1+sPwUXk2J/B3j0KkPaKdvtaXkwz
Q++rjmowS00Nuh9cYGAUBVjuPB/1m6d8YsTry6n1pWcdiS0ZCqITrc+5xINeMtfy
dSwPaL7L4760A81zYFFP21NMGnvSLG2jhwSYqIYm0LaZf9VsbPF00xN0WbA0Nhy1
nAwrnQKbGELp/Bz6bX85aqby1IxRkGS69Wjb1Aq+gwhEhUb6//Rpej4CLN1MLAV1/
vrSHQeOGYnhvdkhkeX7NYGsUA/udwr6zn1800LyWh9RgVEh1pNtP8KRLQ873cijw
egFu1PWyvpa944PUI5AbXI51LudJNV0LeCWZ2/Qcjl40W3RqaLMh
-----END RSA PRIVATE KEY-----

```

これで、仮想コンピュータへの SSH または SCP 接続を確立するために必要なプライベートキーができました。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、コマンドリファレンス [download-default-key-pair](#) の「」を参照してください。AWS CLI

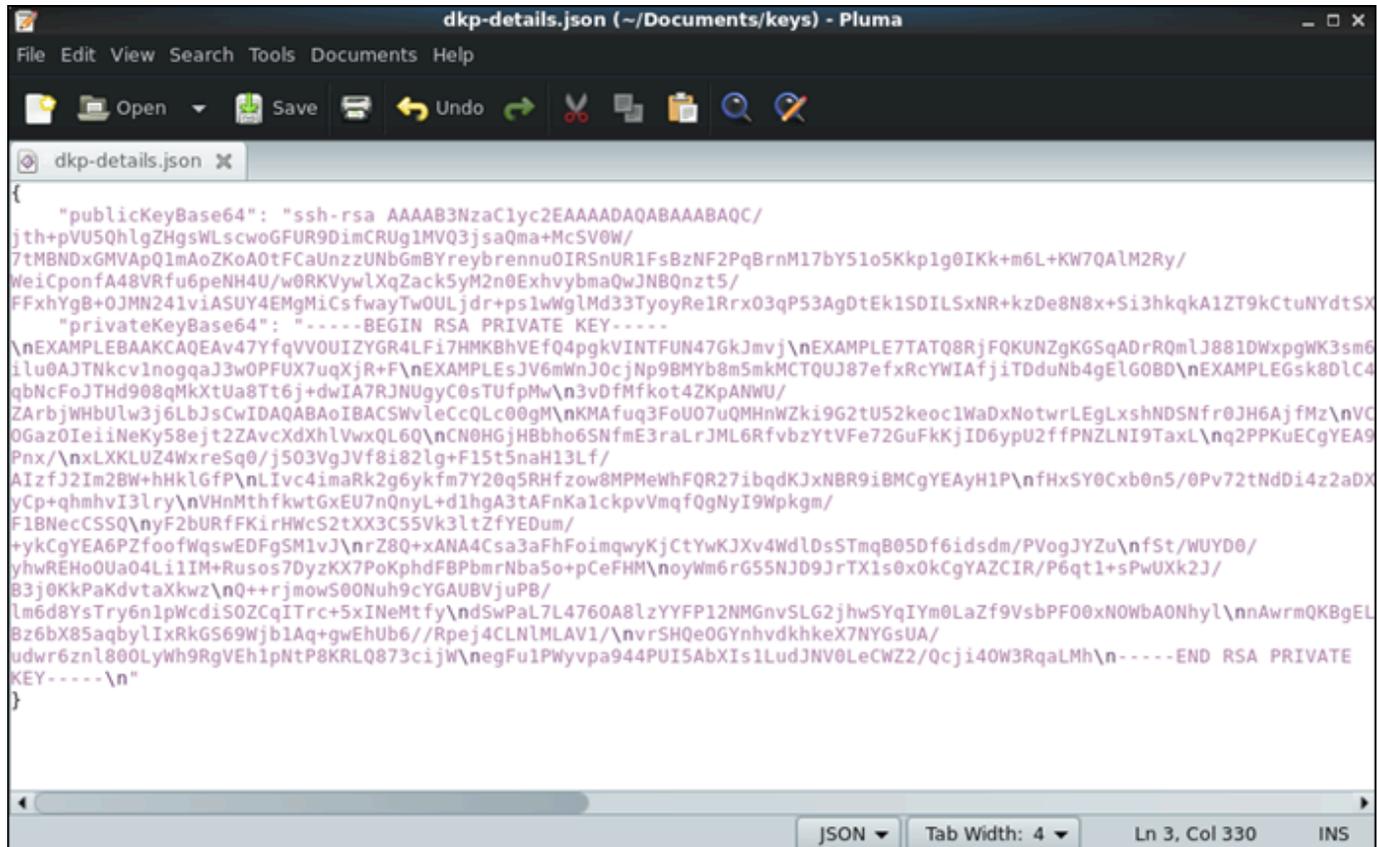
1. ターミナルウィンドウを開きます。
2. 次のコマンドを入力して、特定の AWS リージョンの Lightsail DKP を取得します。このコマンドは、情報を `dkp-details.json` ファイルに保存します。コマンドで、 をなどの仮想コンピュータが作成された AWS リージョンのコード `region-code` に置き換えます `us-east-2`。

```
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。

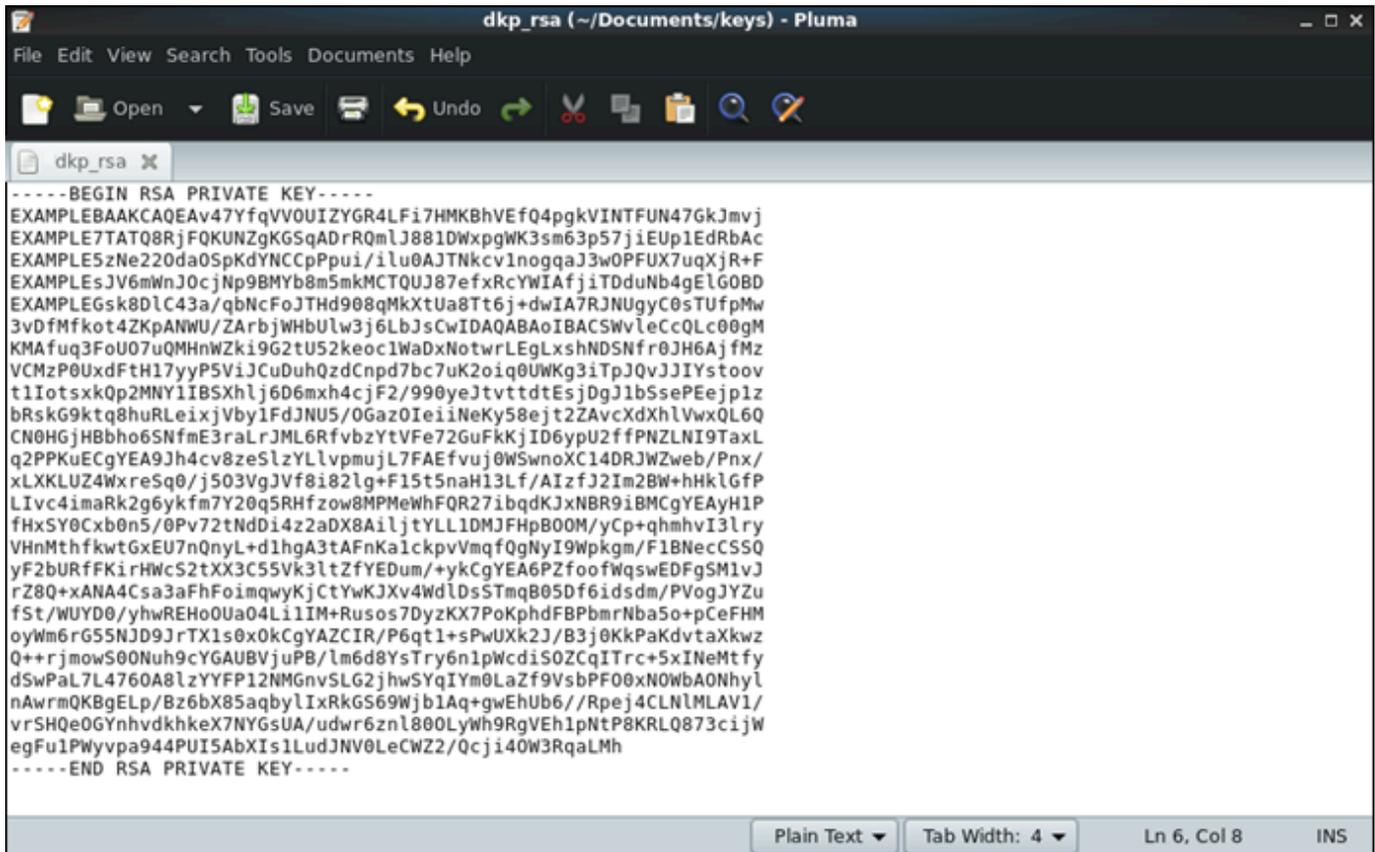


```
{
  "publicKeyBase64": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBAQC/
jth+pVU5QhlgZHgswLscwoGFUR9DmCRUGlMVQ3jsaQma+McSV0W/
7tMBNDxGMVApQ1mAoZKoA0tFCaUnzzUNbGmBYreybrennu0IRSnUR1FsBzNF2PqBrnM17bY51o5Kkp1g0IKk+m6L+KW7QA1M2Ry/
WeiCponfaA48VRfu6peNH4U/w0RKVywLXqZack5yM2n0ExhvybmaQwJNBQnzt5/
FFxhYgB+0JMN241viASUY4EMgMiCsfwayTw0ULjdr+ps1Wg1Md33TyoyRe1Rrx03qP53AgDtEk1SDILSxNR+kzDe8N8x+Si3hkqkA1ZT9kCtuNYdtSX
"privateKeyBase64": "-----BEGIN RSA PRIVATE KEY-----
\nEXAMPLEBAAKCAQEAv47YfqVV0UIZYGR4LFi7HMKbHVEf04pgkVINTFUN47GkJmvj\nEXAMPLE7TATQ8RjFQKUNZgKGSqADrRQmLJ881DWxpgWK3sm6
ilu0AJTNkcV1nogqaJ3w0PFUX7uqXjR+F\nEXAMPLEsJV6mWnJ0cjNp9BMYb8m5mkMCTOUJ87efxRcYwIAfjiTDduNb4gELG0BD\nEXAMPLEGsk8D1C4
qbNcFoJTHd908qMkXtUa8Tt6j+dwIA7RJNUgyC0sTufpMw\n3vDfMfkot4ZKpANWU/
ZARbjWHbUlW3j6LbJscwIDAQAABAoIBACSWvleCcQLc00gM\nKMAfuq3FoU07uQMHNWZki9G2tU52keoc1WaDxNotwrLEgLxshNDSnfr0JH6AjfMz\nnVC
0Gaz0IeiNeKy58ejt2ZAvXdxhLvwXQL6Q\nCN0HGjHbho6SNfmE3raLrJML6RfvbZytVfE72GuFkKjID6ypU2fFPNZLNI9TaxL\nnq2PPKuECgYEAS
Pnx/\nXLXLUZ4WxreSq0/j503VgJVf8i82lg+F15t5naH13Lf/
AIzfJ2Im2BW+hHklGfP\nLlvc4imaRk2g6ykfm7Y20q5RHfzow8MPMEwhFQR27ibqdKJxNBR9iBMCgYEAyH1P\nfhXSY0Cxb0n5/0Pv72tNdDi4z2aDX
Ycp+qmhvI3lry\nVHnMthfkwGxEU7nQnyL+d1hgA3tAFnKa1ckpvVmqfQgNyI9Wpkgm/
F1BNecCSSQ\nyF2bURfFKirHWcS2tXX3C55Vvk3ltZfYEDum/
+ykCgYEA6PZfoofWqswEDFgSMlvJ\nrZ8Q+xANA4Csa3aFhF0imqwyKjCtYwKJXv4WdlDsStmqB05Df6idsdm/PVogJYZu\nnfSt/WUYD0/
yhwREHo0Ua04Li1IM+Rusos7DyzKX7PoKphdF8PbmrNba5o+pCeFHM\nnoyWm6rG55ND9JrTX1s0x0kCgYAZCIR/P6qt1+sPwUXk2J/
B3j0KkPaKdvtaXkwz\nQ++rjmowS00Nuh9cYGAUBVjuPB/
lm6d8YsTry6nlpWcdi50ZCqITrc+5xINeMtfy\nndSwPal7L4760A8lzYFFP12NMGnvSLG2jhwSYqIYm0LaZf9VsbPF00xN0WbA0Nhy\nlnAwrm0KBgEL
Bz6bX85aqblyIxrK6G569WjblAq+gwehUb6//Rpej4CLN\nMLAV1/\nvrSHQe0GYnhvdkhkeX7NYGsUA/
udwr6znl800LyWh9RgVehlpNtP8KRLQ873cijw\nnegFu1Pwyvpa944PUI5AbXIs1LudJNV0LeCWZ2/Qcji40W3RqaLMh\n
-----END RSA PRIVATE
KEY-----\n"
}
```

- 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。



```
-----BEGIN RSA PRIVATE KEY-----
EXAMPLEBAAKCAQEAv47YfqVV0UIZYGR4LFi7HMKBhVEfQ4pgkVINTFUN47GkJmvj
EXAMPLE7TATQ8RjFQKUNZgKGSqADrRQmLJ881DWxpgWK3sm63p57jiEUp1EdRbAc
EXAMPLE5zNe220da0SpKdYNCpPpui/ilu0AJTNkcv1nogqaJ3w0PFUX7uqXjR+F
EXAMPLEsJV6mWnJ0cjNp9BMYb8m5mkMCTQUJ87efxRcYWIafjiTDduNb4gElG0BD
EXAMPLEGsk8DlC43a/qbNcFoJTHd908qMkXtUa8Tt6j+dwIA7RJNUgyC0sTufpMw
3vdFmfkot4ZKpANWU/ZArbjWHbUlw3j6LbJsCwIDAQABAoIBACSwleCcQLc00gM
KMAfuq3FoU07uQMhWZki9G2tU52keoc1WaDxNotwrLEgLxshNDSNfr0JH6Ajfmz
VCMzP0UxdFtH17yyP5ViJCuDuhQzdCnPD7bc7uK2oiq0UWKg3iTpJQvJJIIystoov
t1IotsxkQp2MNYiIBSxhlj6D6mxh4cjF2/990yeJtvtttdtEsjDgJ1bSsePEejPlz
bRskG9ktq8huRLeixjvby1FdJNU5/0Gaz0Iei1NeKy58ejt2ZAvCxHlVwQL6Q
CN0HGjHBbho6SNfmE3raLrJML6RfvbzYtVFe72GuFkKjID6ypU2ffPNZLNi9TaxL
q2PPKuECgYEA9Jh4cv8zeSlzYLlvpmujL7FAEfvuj0WSwnoXC14DRJWzweb/Pnx/
xLXLKLUZ4WxreSq0/j503VgJVf8i82lg+F15t5naH13Lf/AIzfJ2Im2Bw+hHkLGFp
LIvc4imaRk2g6yKfm7Y20q5RHfzow8MPMeWhFQR27ibqdKJxNBR9iBMCgYEAyH1P
fHxSY0Cxb0n5/0Pv72tNdD14z2aDX8AiljtYLL1DMJFHpB00M/yCp+qhmhvI3lry
VHnMthfkwTgxEU7nQnyL+d1hgA3tAFnKalckpvVmQfQgNyI9WpKgm/F1BNecCSSQ
yF2bURfFKirHwCs2tXX3C55Vk3ltzFYEDum/+ykCgYEA6P2foofWqswEDFgSM1vJ
rZ8Q+xANA4Csa3aFhFoimqwyKjCtYwKJXv4WdlDs5TmqB05Df6idsdm/PVogJYZu
fSt/WUYD0/yhwREHo0Ua04Li1IM+Rusos7DyzKX7PoKphdFBPbmrNba5o+pCeFHM
oyWm6rG55NJD9jRTX1s0x0kCgYAZCIR/P6qt1+sPwUXk2J/B3j0KkPaKdvtaXkwz
Q++rjmowS00Nuh9cYGAUBVjuPB/lm6d8YsTry6n1pWcdiS0ZCqITrc+5xINeMtfy
dSwPaL7L4760A8LzYFFP12NMGnvSLG2jhwSYqIYm0LaZf9VsbPF00xNOWbAONhyl
nAwrMQKBgElp/Bz6xb85aQbylIxRkGS69WjblAq+gwEhUb6//Rpej4CLNlMLAV1/
vr5HQe0GYnhvdkhkeX7NYGsUA/udwr6zn1800LyWh9RgVEh1pNtP8KRLQ873cijw
egFu1PWyvpa944PUI5AbXiS1LudJNV0LeCWZ2/Qcji40W3RqaLMh
-----END RSA PRIVATE KEY-----
```

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 接続を確立するために必要なプライベートキーができました。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。

- を使用して仮想コンピュータに接続し SSH、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 Lightsail for Research 仮想コンピュータに接続する](#)」を参照してください。
- を使用して仮想コンピュータに接続し SCP、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 Lightsail for Research 仮想コンピュータにファイルを転送する](#)」を参照してください。

Secure Shell を使用して Lightsail for Research 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で管理し、インターネット経由で仮想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、「[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](#)」を参照してください。

トピック

- [前提条件を満たす](#)
- [を使用して仮想コンピュータに接続する SSH](#)
- [次のステップに進みます](#)

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、「[Lightsail for Research 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、「[Lightsail for Research 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、に使用されるデフォルトのポートですSSH。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、「[Lightsail for Research 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予定がある場合は、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、「[とはAWS 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 用に 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、キーペアの詳細を抽出するために以下の手順で使用される軽量で柔軟なコマンドライン JSON プロセッサです。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。

を使用して仮想コンピュータに接続する SSH

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

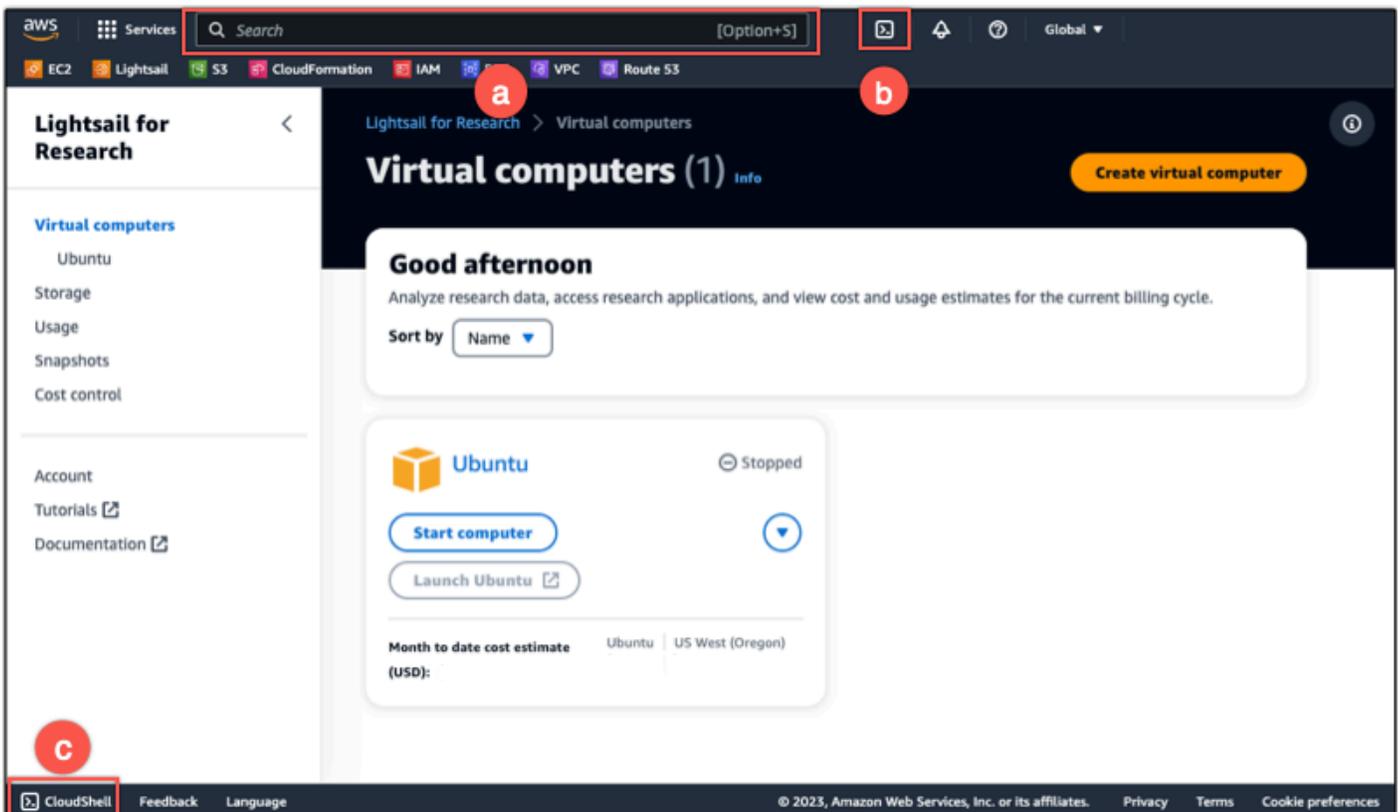
を使用して仮想コンピュータに接続する AWS CloudShell

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する場合に適用されます。は、ブラウザベースの事前認証済みシェル AWS CloudShell を使用し、 から直接起動できます 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。

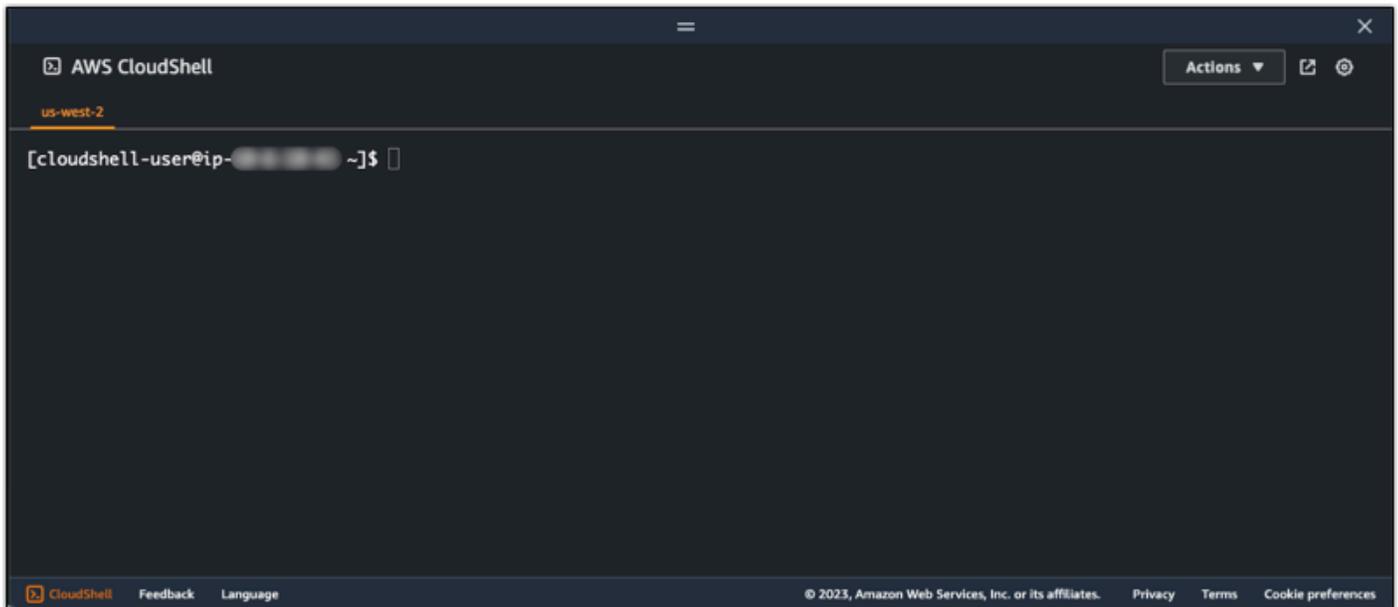
⚠ Important

開始する前に、接続先の仮想コンピュータの Lightsail の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、「[Lightsail for Research 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. CloudShell コンソールの左下にあるコンソールツールバーで 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、または macOS ローカルコンピュータSSHで 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の詳細については、CloudShell「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SSHで 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) を取得してください。詳細については、「[Lightsail for Research 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 のプライベートキーDKP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. [コマンドプロンプト] 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 AWS リージョンで、`us-east-2` をなどの仮想コンピュータが作成されたのコード `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。

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

3. 次のコマンドを入力して、仮想コンピュータとSSHの接続を確立します。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 で Ubuntu 仮想コンピュータと確立されたSSH接続を示す、次の例のようなレスポンスが表示されます。

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

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

https://ubuntu.com/aws/pro

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

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

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

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

仮想コンピュータSSHへの接続が正常に確立されたので、[次のセクション](#)に進み、追加の次のステップに進みます。

Linux、Unix、または macOS ローカルコンピュータSSHで 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 の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、「[Lightsail for Research 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 のプライベートキー-DKP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、`region-code` を `us-east-2` 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。 `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。

```
ubuntu@ip-10-0-10-10:~$ 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'
[1] 31203 31204
ubuntu
18.118.120.226
```

3. 次のコマンドを入力して、仮想コンピュータとSSHの接続を確立します。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 で Ubuntu 仮想コンピュータと確立されたSSH接続を示す、次の例のようなレスポンスが表示されます。

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

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

System load: 0.0
Usage of /: 0.3% of 620.36GB
Memory usage: 1%
Swap usage: 0%
Processes: 161
Users logged in: 0
IPv4 address for eth0: 192.0.2.0
IPv6 address for eth0: fe80::200:0:0:0

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

https://ubuntu.com/aws/pro

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

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

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

*** System restart required ***
Last login: Thu Feb 9 19:59:52 2023 from 192.0.2.0
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

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

仮想コンピュータSSHへの接続が正常に確立されたので、[次のセクション](#)に進み、追加の次のステップに進みます。

次のステップに進みます

仮想コンピュータSSHへの接続が正常に確立されたら、次の追加の次のステップを完了できます。

- を使用して仮想コンピュータに接続しSCP、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 Lightsail for Research 仮想コンピュータにファイルを転送する](#)」を参照してください。

Secure Copy を使用して Lightsail for Research 仮想コンピュータにファイルを転送する

Secure Copy () 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SCP。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 コンソールで利用可能なブラウザベースの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、個々のファイルをすばやく転送できます。詳細については、「[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](#)」を参照してください。

トピック

- [前提条件を満たす](#)
- [を使用して仮想コンピュータに接続する SCP](#)

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、「[Lightsail for Research 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、「[Lightsail for Research 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、キーペアの詳細を抽出するために以下の手順で使用される軽量で柔軟なコマンドラインJSONプロセッサです。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、に使用されるデフォルトのポートですSSH。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、「[Lightsail for Research 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、「[Lightsail for Research 仮想コンピュータを作成する](#)」を参照してください。

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SCP。

Windows ローカルコンピュータSCPで 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) を取得してください。詳細については、「[Lightsail for Research 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 のプライベートキーDKP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. [コマンドプロンプト] 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 `region-code` 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。

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

3. 次のコマンドを入力して、仮想コンピュータとSCPの接続を確立し、そのコンピュータに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、または macOS ローカルコンピュータ 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 の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、「[Lightsail for Research 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 のプライベートキー DKP 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、`us-east-2` を `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。

```
ubuntu@ip-10-0-10-10:~$ aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer | jq -r  
'instance.username' & aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer | jq -r '.in  
stance.publicIpAddress'  
[1] 31203 31204  
ubuntu  
18.118.120.226
```

3. 次のコマンドを入力して、仮想コンピュータとSCPの接続を確立し、そのコンピュータに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。

```
(Ubuntu 16.04 LTS) <0> [~/Documents/Keys]
$ scp -i dkp_rsa -r 'Files' ubuntu@192.0.2.0:/home/lightsail-user/Uploads/
myfile2.txt          100% 10   0.2KB/s  00:00
myfile6.txt          100% 10   0.2KB/s  00:00
myfile7.txt          100%  8   0.1KB/s  00:00
myfile10.txt         100%  7   0.1KB/s  00:00
myfile1.txt          100%  9   0.2KB/s  00:00
myfile3.txt          100% 10   0.2KB/s  00:00
myfile12.txt         100% 13   0.2KB/s  00:00
myfile.txt           100% 11   0.2KB/s  00:00
myfile9.txt          100%  9   0.2KB/s  00:00
myfile11.txt         100%  4   0.1KB/s  00:00
myfile5.txt          100% 10   0.2KB/s  00:00
myfile4.txt          100%  9   0.2KB/s  00:00
myfile8.txt          100%  9   0.2KB/s  00:00
```

Lightsail for Research 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。

Lightsail for Research ボリュームによるデータの保護と保存

Amazon Lightsail for Research には、実行中の Lightsail for Research 仮想コンピュータにアタッチ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) が用意されています。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、ディスクが推奨されるストレージオプションです。

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

- [Lightsail for Research コンソールでストレージディスクを作成する](#)
- [Lightsail for Research コンソールでストレージディスクの詳細を表示する](#)
- [Lightsail for Research の仮想コンピュータにストレージを追加する](#)
- [Lightsail for Research の仮想コンピュータからディスクをデタッチする](#)
- [Lightsail for Research で未使用のストレージディスクを削除する](#)

Lightsail for Research コンソールでストレージディスクを作成する

Lightsail for Research 仮想コンピュータ用のディスクを作成するには、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 内で一意であること。
 - 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 AWS リージョン の 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。

Lightsail for Research コンソールでストレージディスクの詳細を表示する

Lightsail for Research アカウントのディスクとその詳細を表示するには、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、[ストレージ] を選択します。

ストレージページには、Lightsail for Research アカウントのディスクの包括的なビューが表示されます。

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 — ディスクがアタッチされている Lightsail コンピュータ。
- 作成日 — ディスクが作成された日付。

Lightsail for Research の仮想コンピュータにストレージを追加する

Lightsail for Research の仮想コンピュータにディスクをアタッチするには、以下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

コンソールを使用してディスクを仮想コンピュータにアタッチすると、サービスによって自動的にフォーマットおよびマウントされます。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。ここで、`<disk-name>` はディスクに付けた名前です。

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。

Lightsail for Research の仮想コンピュータからディスクをデタッチする

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。

Lightsail for Research で未使用のストレージディスクを削除する

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、「[Lightsail for Research の仮想コンピュータからディスクをデタッチする](#)」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、[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。

Lightsail for Research スナップショットを使用して仮想コンピュータとディスクをバックアップする

スナップショットはデータ point-in-time のコピーです。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、それら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

- [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](#)
- [Lightsail for Research での仮想コンピュータとディスクスナップショットの表示と管理](#)
- [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](#)
- [Lightsail for Research コンソールでスナップショットを削除する](#)

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

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、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. 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 内で一意であること。
- 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. [スナップショットを作成] を選択します。

Lightsail for Research での仮想コンピュータとディスクスナップショットの表示と管理

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、次のステップを実行します。

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。

Lightsail for Research コンソールでスナップショットを削除する

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。

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もりを提供します。これらの見積りは、Lightsail for Research を使用する際の支出計画、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ちます。

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もりが表示されます。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もりが反映されます。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も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、で AWS Billing コンソールを開きます <https://console.aws.amazon.com/billing/>。

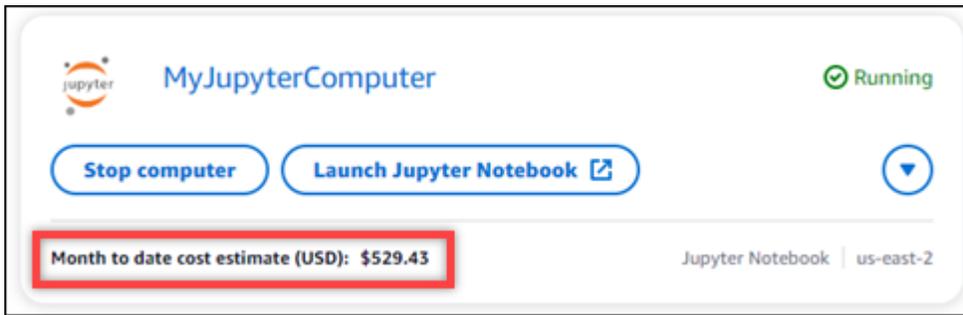
トピック

- [Lightsail for Research でリソースのコストと使用状況の見積もりを表示する](#)

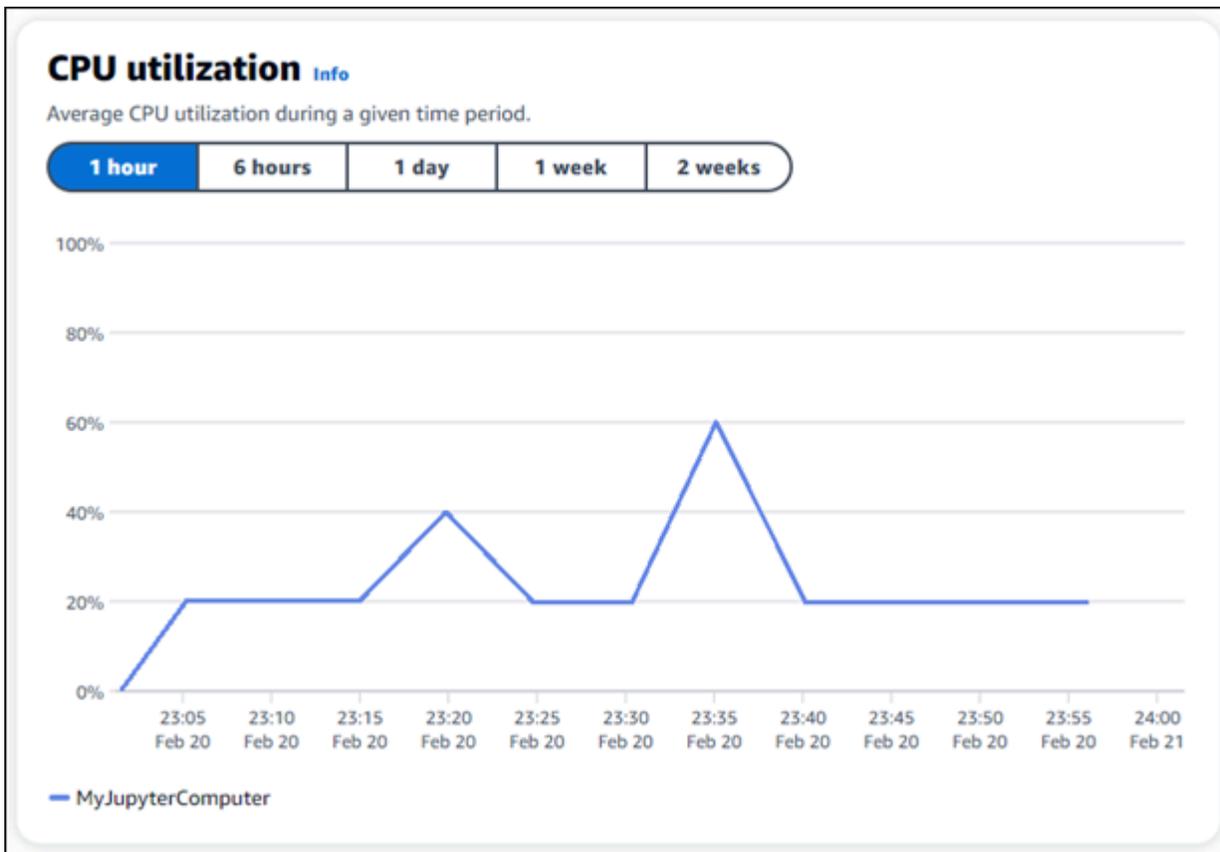
Lightsail for Research でリソースのコストと使用状況の見積もりを表示する

Lightsail for Research リソースの月初来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せん。



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 リソースの月初来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「使用状況」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.

< 1 > ⚙

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

Disks

< 1 > ⚙

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

Lightsail for Research でコスト管理ルールを管理する

コスト管理では、Lightsail for Research 仮想コンピュータの使用とコストを管理するために定義したルールを使用します。

アイドル状態のルールで停止仮想コンピュータを作成し、特定の期間に実行中のコンピュータが CPU 指定された使用率に達したときに停止させることができます。例えば、ルールは、30 分間の CPU 使用率が 5% 以下の場合に、特定のコンピュータを自動的に停止できます。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することを意味します。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

- [Lightsail for Research 仮想コンピュータのコスト管理ルールを作成する](#)
- [Lightsail for Research 仮想コンピュータのコスト管理ルールを削除する](#)

Lightsail for Research 仮想コンピュータのコスト管理ルールを作成する

Lightsail for Research 仮想コンピュータのルールを作成するには、次のステップを実行します。

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、現在ルールによってモニタリングされている唯一のメトリクスであり、サポートされている唯一のオペレーションは 以下です。

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. ルールを実行する CPU 使用率と期間を指定します。

例えば、「5%」、「30 分」といった指定ができます。Lightsail for Research は、30 分間 CPU の使用率が 5% 以下の場合、コンピュータを自動的に停止します。

6. [ルール作成] 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。

Lightsail for Research 仮想コンピュータのコスト管理ルールを削除する

Lightsail for Research 仮想コンピュータのルールを削除するには、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 [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. [削除] を選択します。
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。

Lightsail for Research リソースをタグで整理する

Amazon Lightsail for Research では、リソースにタグを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。

Amazon Lightsail for Research コンソールでは、次のリソースに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 用に予約されています。

トピック

- [Lightsail for Research リソースにタグを付ける](#)
- [Lightsail for Research リソースからタグを削除する](#)

Lightsail for Research リソースにタグを付ける

Lightsail for Research 仮想コンピュータのタグを作成するには、次のステップを実行します。これらの手順は、Lightsail for Research のディスクとスナップショットでも同様です。

1. Lightsail for Research コンソールで [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. [タグを管理] 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。

Lightsail for Research リソースからタグを削除する

Lightsail for Research 仮想コンピュータからタグを削除するには、次のステップを実行します。これらの手順は、Lightsail for Research のディスクとスナップショットでも同様です。

1. Lightsail for Research コンソールで [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. [タグを管理] 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、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 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](#)
- [Amazon Lightsail for Research の Identity and Access Management](#)
- [Amazon Lightsail for Research のコンプライアンス検証](#)
- [Amazon Lightsail for Research の耐障害性](#)
- [Amazon Lightsail for Research のインフラストラクチャセキュリティ](#)
- [Amazon Lightsail for Research の設定と脆弱性の分析](#)
- [Amazon Lightsail for Research のセキュリティのベストプラクティス](#)

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FAQ](#)」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」の[AWS 「責任共有モデル」とGDPR](#)ブログ記事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 () 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IAM。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。1TLS.2 が必要で、1.3 TLS をお勧めします。
- を使用して 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 AWS を介して にアクセスするときに FIPS 140-3 検証済みの暗号化モジュールが必要な場合はAPI、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 \(FIPS\) 140-3](#)」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、または 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API AWS CLI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。URL を外部サーバーに提供する場合は、そのサーバーへのリクエストを検証URLするために認証情報を に含めないことを強くお勧めします。

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](#)
- [アイデンティティを使用した認証](#)
- [ポリシーを使用したアクセスの管理](#)
- [Amazon Lightsail for Research と の連携方法 IAM](#)
- [Amazon Lightsail for Research のアイデンティティベースのポリシーの例](#)
- [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](#)

対象者

AWS Identity and Access Management (IAM) の使用 방법은、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、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。次に、サービスユーザーのアクセス許可を変更するリクエストを IAM 管理者に送信する必要があります。このページの情報を確認して、の

基本概念を理解してくださいIAM。会社で Lightsail for Research 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 の連携方法 IAM](#)。

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。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IAM、「」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ロールを引き受けることによって認証 (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、フェデレーテッド ID の例です。フェデレーテッド ID としてサインインすると、管理者は以前に IAMロールを使用して ID フェデレーションをセットアップしていました。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となります。

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、 はソフトウェア開発キット (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[AWS API「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、アカウントのセキュリティを高めるために多要素認証 (MFA) を使用す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「[多要素認証](#)」および「[ユーザーガイド](#)」の「[での多要素認証 \(MFA\) AWS IAM 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 AWS のサービス およびリソースへの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[「ルートユーザーの認証情報を必要とするタスク」](#)を参照してください。

フェデレーテ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が、一時的な認証情報を使用してにアクセスするために ID プロバイダーとのフェデレーションを使用することを要求 AWS のサービスします。

フェデレーテッド 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、アイデンティティセンター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、「ユーザーガイド」の[IAM 「Identity Center」とはAWS IAM Identity Center](#)」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持つIAMユーザーを作成するのではなく、一時的な認証情報を使用することをお勧めします。ただし、IAMユーザーとの長期的な認証情報を必要とする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、「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でアクセスキーを定期的にローテーションするIAM」](#)を参照してください。

[IAM グループ](#)は、IAMユーザーのコレクション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、 という名前のグループIAMAdminsを作成し、そのグループにIAMリソースを管理するアクセス許可を付与できます。

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、ロールでは一時認証情報が提供されます。詳細については、「[ユーザーガイド](#)」のIAM「[\(ロールの代わりに\) ユーザーを作成する場合IAM](#)」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 ユーザーと似ていますが、特定のユーザーに関連付けられていません。IAM ロール を切り替える AWS Management Console ことで、[で 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 オペレーションを AWS CLI 呼び出すか、カスタム を使用します URL。ロールの使用の詳細については、「[ユーザーガイド](#)」のIAM「[ロールの使用IAM](#)」を参照してください。

IAM 一時的な認証情報を持つ ロールは、以下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 ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールの詳細については、「[ユーザーガイド](#)」の「[サードパーティー ID プロバイダーのロールの作成IAM](#)」を参照してください。IAM Identity Center を使用する場合は、アクセス許可セットを設定します。ID が認証後にアクセスできる内容を制御するために、IAM Identity Center はアクセス許可セットを のロールに関連付けますIAM。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「[アクセス許可セット](#)」を参照してください。
- 一時的なIAMユーザーアクセス許可 – IAM ユーザーまたはロールは、IAMロールを引き受けて、特定のタスクに対して異なるアクセス許可を一時的に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、別のアカウントのユーザー (信頼されたプリンシパル) がアカウントのリソースにアクセスすることを許可できます。クロスアカウントアクセスを許可する主な方法は、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のロールとリソースベースのポリシーの違いについては、「[ユーザーガイド](#)」の「[でのクロスアカウントリソースアクセスIAMIAM](#)」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、サービスで呼び出しを行うと、そのサービスが Amazon でアプリケーションを実

行EC2したり、Amazon S3 にオブジェクトを保存したりするのが一般的です。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンク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権限が必要です。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 – サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける [IAMロール](#)です。IAM 管理者は、内からサービスロールを作成、変更、削除できますIAM。詳細については、「[ユーザーガイド](#)」の「[にアクセス許可を委任するロールの作成 AWS のサービスIAM](#)」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アクセス許可を表示できますが、編集することはできません。
- Amazon で実行されているアプリケーション EC2 – 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インスタンス内にアクセスキーを保存するよりも望ましいです。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ており、EC2インスタンスで実行されているプログラムが一時的な認証情報を取得できるようにします。詳細については、「[ユーザーガイド](#)」の「[IAMロールを使用して Amazon EC2インスタンスで実行されているアプリケーションにアクセス許可を付与するIAM](#)」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、「[ユーザーガイド](#)」の「[IAMロールを作成するタイミング \(ユーザーではなく \) IAM](#)」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、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、「[ユーザーガイド](#)」の[JSON「ポリシーの概要IAM」](#)を参照してください。

管理者はポリシーを使用して AWS JSON、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対してどのような条件下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。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行に使用するメソッドに関係なく、アクションのアクセス許可を定義します。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 からロール情報を取得できますAPI。

アイデンティティベースのポリシー

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなど、ID にアタッチできるJSONアクセス許可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、「[ユーザーガイド](#)」の[IAM「ポリシーの作成IAM」](#)を参照してください。

アイデンティティベースのポリシーは、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。管理ポリシーとインラインポリシーのどちらかを選択する方法については、IAM ユーザーガイドの[「管理ポリシーとインラインポリシーの選択」](#)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、リソースにアタッチする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の例としては、IAMロールの信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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コントロールできます。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IAMでは、 の AWS 管理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 (ACLs)

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs 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を使用しません。

Amazon S3、AWS WAF、および Amazon VPCは、 をサポートするサービスの例ですACLs。の詳細についてはACLs、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がIAMエンティティ (IAMユーザーまたはロール) に付与できるアクセス許可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。アクセス許可の境界の詳細については、「IAMユーザーガイド」の [「IAMエンティティのアクセス許可の境界」](#) 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

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 (SCPs) をアカウントの一部またはすべてに適用できます。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SCPを制限します AWS アカウントのルートユーザー。Organizations と の詳細についてはSCPs、「AWS Organizations ユーザーガイド」の「[サービスコントロールポリシー](#)」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があります。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、「ユーザーガイド」の「[セッションポリシーIAM](#)」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、ユーザーガイドの「[ポリシー評価ロジックIAM](#)」を参照してください。

Amazon Lightsail for Research と の連携方法 IAM

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。

IAM Amazon Lightsail for Research で使用できる 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	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	あり

IAM 機能	Lightsail for Research のサポート
ACLs	なし
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
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	なし

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 「と連携する のサービスIAM」](#)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のポリシーのサポート: あり

ID ベースのポリシーは、IAMユーザー、ユーザーのグループ、ロールなど、ID にアタッチできる JSONアクセス許可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、「ユーザーガイド」の[IAM 「ポリシーの作成IAM」](#)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、許可または拒否されたアクションとリソース、およびアクションが許可または拒否され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、「ユーザーガイド」の「[IAMJSONポリシー要素のリファレンスIAM](#)」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: なし

リソースベースのポリシーは、リソースにアタッチする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の例としては、IAMロールの信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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コントロールできます。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、リソースベースのポリシーのプリンシパルとして、アカウント全体または別のアカウントのIAMエンティティを指定できます。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 がある場合 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さらに付与する必要はありません。詳細については、「[ユーザーガイド](#)」の「[でのクロスアカウントリソースアクセスIAMIAM](#)」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のサポート: あり

管理者はポリシーを使用して AWS JSON、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対してどのような条件下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要素は、ポリシーで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を記述します。ポリシーアクションの名前は通常、関連する AWS APIオペレーションと同じです。一致するAPIオペレーションがないアクセス許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数の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

ポリシーリソースのサポート: あり

管理者はポリシーを使用して AWS JSON、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対してどのような条件下でアクションを実行できるかということです。

Policy ResourceJSON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、リソースレベルの許可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 のリストを確認するには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ARNの 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: あり

管理者はポリシーを使用して AWS JSON、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、どのリソースに対してどのような条件下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 要素を指定する場合、または 1つの Condition 要素に複数のキーを指定する場合、AWS では 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、リソースにIAMユーザー名でタグ付けされている場合にのみ、リソースへのアクセス許可をIAMユーザーに付与できます。詳細については、「ユーザーガイド」の[IAM 「ポリシー要素: 変数とタグIAM」](#)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、「ユーザーガイド」の[AWS 「グローバル条件コンテキストキーIAM」](#)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](#)。

ACLs Lightsail for Research の

をサポートACLs : いいえ

アクセスコントロールリスト (ACLs) は、リソースへのアクセス許可を持つプリンシパル (アカウントメンバー、ユーザー、またはロール) を制御します。ACLs 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を使用しません。

ABAC Lightsail for Research を使用する

サポート ABAC (ポリシー内のタグ): 部分的

属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可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、の最初のステップですABAC。次に、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する場合に、オペレーションを許可するABACポリシーを設計します。

ABAC は、急速に成長している環境や、ポリシー管理が煩雑になる状況に役立ちます。

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ありです。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。

の詳細についてはABAC、「IAMユーザーガイド」の「[とはABAC](#)」を参照してください。の設定手順を含むチュートリアルを表示するにはABAC、「ユーザーガイド」の「[属性ベースのアクセスコントロール \(ABAC\)](#)」を使用するIAM」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: あり

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、「ユーザーガイド [AWS のサービス](#)」の「[と連携IAM](#)する IAM」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、会社のシングルサインオン (SSO) リンク AWS を使用して にア

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。ロールの切り替えの詳細については、「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 を使用して手動で作成できます AWS API。その後、これらの一時的な認証情報を使用して . AWS recommends にアクセスできます AWS。これは、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推奨しています。詳細については、「」の「[一時的なセキュリティ認証情報IAM](#)」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をサポート (FAS): 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権限が必要です。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: なし

サービスロールは、ユーザーに代わってアクションを実行するためにサービスが引き受ける [IAM ロール](#)です。IAM 管理者は、内からサービスロールを作成、変更、削除できますIAM。詳細については、「ユーザーガイド」の「[にアクセス許可を委任するロールの作成 AWS のサービスIAM](#)」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: なし

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アクセス許可を表示できますが、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、「[AWS と連携する のサービス IAM](#)」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。サービスリンク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、はい 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 を使用してタスクを実行することはできません AWS API。必要なリソースに対してアクションを実行するアクセス許可をユーザーに付与するために、IAM管理者はIAMポリシーを作成できます。その後、管理者はIAMポリシーをロールに追加し、ユーザーはロールを引き受けることができます。

これらのポリシードキュメント例を使用してIAMアイデンティティベースのJSONポリシーを作成する方法については、「ユーザーガイド」の[IAM 「ポリシーの作成IAM」](#)を参照してください。

Lightsail for Research で定義されるアクションとリソースタイプの詳細については、ARNs各リソースタイプの の形式など、「[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、または削除できるか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、「ユーザーガイド」の「[AWS 管理ポリシー](#)」または「[ジョブ機能の管理ポリシーIAM](#)」を参照してください。 [AWS](#)
- 最小特権のアクセス許可を適用する – IAMポリシーでアクセス許可を設定する場合は、タスクの実行に必要なアクセス許可のみを付与します。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、最小特権アクセス許可とも呼ばれています。IAM を使用してアクセス許可を適用する方法の詳細については、「ユーザーガイド」の「[のポリシーとアクセス許可IAMIAM](#)」を参照してください。
- IAM ポリシーの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、アクションと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を使用して送信する必要があることを指定できますSSL。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、「ユーザーガイド」の[IAMJSON](#)「[ポリシー要素: 条件IAM](#)」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、安全で機能的なアクセス許可を確保する – IAM Access Analyzer は、ポリシーがポリシー言語 (JSON) とIAMベストプラクティスに準拠するように、新規および既存のIAMポリシーを検証します。IAM Access Analyzer には、安全で機能的なポリシーの作成に役立つ 100 を超えるポリシーチェックと実用的な推奨事項が用意されています。詳細については、「ユーザーガイド」のIAM「[Access Analyzer ポリシーの検証IAM](#)」を参照してください。
- 多要素認証を要求する (MFA) – 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MFAするためにをオンにします。API オペレーションが呼び出されるMFAタイミングを要求するには、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](#)「[で保護されたAPIアクセスの設定](#)」を参照してください。

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「[のセキュリティのベストプラクティスIAMIAM](#)」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 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 AWS API。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を許可します。

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、「[ユーザーガイド](#)」の「[ユーザーへのアクセス許可の追加IAM](#)」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、IAMユーザーがユーザー ID にアタッチされているインラインポリシーと管理ポリシーを表示できるようにするポリシーを作成する方法を示します。このポリシーには、コンソールで、または AWS CLI または 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 AWS API。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "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 および 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IAM。

トピック

- [Lightsail for Research でアクションを実行する権限がない](#)
- [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](#)

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。

次の例のエラーは、mateojacksonIAMユーザーが コンソールを使用して架空の`my-example-widget`リソースの詳細を表示しようとしているが、架空の`lightsail:GetWidget`アクセス許可がない場合に発生します。

```
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。サインイン認証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、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 (ACLs) をサポートするサービスでは、これらのポリシーを使用して、ユーザーにリソースへのアクセスを許可できます。

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 の連携方法 IAM](#)。
- 所有している のリソースへのアクセスを提供する方法については、AWS アカウント「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通じ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 [「外部認証されたユーザーへのアクセスの提供 \(ID フェデレーション\)」](#) 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については、「ユーザーガイド」の [「でのクロスアカウントリソースアクセスIAMIAM」](#) 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。では、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HIPAAのセキュリティとコンプライアンスのためのアーキテクチャ](#) – 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

すべての AWS のサービスがHIPAA対象となるわけではありません。詳細については、[HIPAA「対象サービスリファレンス」](#)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 (米国立標準技術研究所 (NIST)、Payment Card Industry Security Standards Council ()、PCI国際標準化機構 (ISO) など) 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られています。
- [「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。

- [Amazon GuardDuty](#) – これにより AWS アカウント、疑わしいアクティビティや悪意のあるアクティビティがないか環境を監視することで、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービスを検出します。GuardDuty は、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで DSS、PCI などのさまざまなコンプライアンス要件に対応するのに役立ちます。
- [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ゾーン AWS リージョンを提供します。アベイラビリティゾーンでは、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。

Lightsail for Research は、AWS グローバルインフラストラクチャに加えて、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いくつかの機能を提供しています。詳細については、「[Lightsail for Research スナップショットを使用して仮想コンピュータとディスクをバックアップする](#)」および「[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](#)」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によって保護されています。AWS セキュリティサービスと [ガ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、「Security Pillar AWS Well-Architected Framework」の「[Infrastructure Protection](#)」を参照してください。

が AWS 公開した API 呼び出しを使用して、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)。1 TLS.2 が必要で、1.3 TLS をお勧めします。
- (Ephemeral Diffie-Hellman PFS) や DHE (Elliptic Curve Ephemeral Diffie-Hellman) などの完全前方秘匿性 ECDHE () を備えた暗号スイート。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。

さらに、リクエストは、IAM プリンシパルに関連付けられたアクセスキー ID と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ため、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。