aws

Guide de l’utilisateur

Amazon Lightsail pour la recherche

Amazon Lightsail pour la recherche: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon Lightsail for Research ?

Avec Amazon Lightsail for Research, les universitaires et les chercheurs peuvent créer de puissants ordinateurs virtuels dans le cloud Amazon Web Services AWS(). Ces ordinateurs virtuels sont fournis avec des applications de recherche préinstallées, telles que RStudio Scilab.

Avec Lightsail for Research, vous pouvez télécharger des données directement depuis un navigateur Web pour commencer votre travail. Vous pouvez créer et supprimer vos ordinateurs virtuels à tout moment, ce qui vous permet d'accéder à la demande à de puissantes ressources informatiques.

Vous ne payez que tant que vous avez besoin de l'ordinateur virtuel. Lightsail for Research propose des contrôles budgétaires qui peuvent automatiquement arrêter votre ordinateur lorsqu'il atteint une limite de coûts préconfigurée, afin que vous n'ayez pas à vous soucier des frais d'utilisation excédentaire.

Tout ce que vous faites dans la console Lightsail for Research est soutenu par une API accessible au public. Découvrez comment installer et utiliser l'API AWS CLIand pour Amazon Lightsail.

Tarification

Avec Lightsail for Research, vous ne payez que pour les ressources que vous créez et utilisez. Pour plus d'informations, consultez la section Tarification de Lightsail for Research.

Disponibilité

Lightsail for Research est disponible dans les AWS mêmes régions qu'Amazon Lightsail, à l'exception de la région USA Est (Virginie du Nord). Lightsail for Research utilise également les mêmes points de terminaison que Lightsail. Pour consulter les AWS régions et les points de terminaison actuellement pris en charge pour Lightsail, consultez la section Points de terminaison et quotas Lightsail dans le manuel de référence général.AWS

Configuration d'Amazon Lightsail pour la recherche

Si vous êtes un nouveau AWS client, répondez aux exigences de configuration répertoriées sur cette page avant de commencer à utiliser Amazon Lightsail for Research.

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .

2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Tutoriel : Démarrez avec les ordinateurs virtuels Lightsail for Research

Utilisez ce didacticiel pour démarrer avec les ordinateurs virtuels Amazon Lightsail for Research. Vous apprendrez à créer un ordinateur virtuel, à vous y connecter et à l'utiliser. Dans Lightsail for Research, un ordinateur virtuel est un poste de travail de recherche que vous créez et gérez dans le. AWS Cloud Les ordinateurs virtuels sont basés sur des instances Linux Lightsail avec le système d'exploitation Ubuntu. Sur votre ordinateur virtuel, vous pouvez préconfigurer une application de recherche telle que JupyterLab Scilab, etc. RStudio

L'ordinateur virtuel que vous créez dans ce tutoriel sera soumis à des frais d'utilisation à partir du moment où vous le créez et jusqu'à ce que vous le supprimiez. La suppression est la dernière étape de ce tutoriel. Pour plus d'informations sur les tarifs, consultez la section Tarification de Lightsail for Research.

Rubriques

Étape 1 : Exécuter les prérequis

Si vous êtes un nouveau AWS client, remplissez les conditions de configuration requises avant de commencer à utiliser Amazon Lightsail for Research. Pour de plus amples informations, veuillez consulter Configuration d'Amazon Lightsail pour la recherche.

Étape 2 : créer un ordinateur virtuel

Vous pouvez créer un ordinateur virtuel à l'aide de la console Lightsail for Research, comme décrit dans la procédure suivante. Ce tutoriel a pour but de vous aider à lancer rapidement votre premier

ordinateur virtuel. Nous vous recommandons également d'explorer les applications et les plans matériels disponibles. Pour plus d'informations, consultez Choisissez les images des applications et les forfaits matériels pour Lightsail for Research et Création d'un ordinateur virtuel Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research.
2. Sur la page d'accueil, choisissez Créer un ordinateur virtuel.
3. Sélectionnez un Région AWS pour votre ordinateur virtuel.

   Choisissez Région AWS celui qui est le plus proche de votre emplacement physique pour réduire le temps de latence.
4. Choisissez une application, également connue sous le nom de plan dans l'API Lightsail.

   L'application que vous choisissez est installée et configurée sur votre ordinateur virtuel lorsque vous la créez.
5. Choisissez un plan matériel, également appelé bundle dans l'API Lightsail.

   Les plans de matériel offrent différentes puissances de traitement, notamment les cœurs de vCPU, la mémoire, le stockage et le transfert de données mensuel. Lightsail for Research propose des forfaits standard et des plans GPU pour les ordinateurs virtuels. Choisissez un plan standard lorsque les exigences informatiques de votre travail sont faibles. Choisissez un plan GPU lorsque cette exigence est élevée, par exemple lors de l'exécution de modèles de machine learning ou d'autres tâches gourmandes en calculs.
6. Saisissez un nom pour votre ordinateur virtuel.
7. Choisissez Créer un ordinateur virtuel dans le panneau Résumé.

Une fois que votre nouvel ordinateur virtuel est opérationnel, passez à l'étape suivante de ce tutoriel pour savoir comment lancer l'application de l'ordinateur.

Étape 3 : lancer l'application d'un ordinateur virtuel

Une fois que vous avez créé un ordinateur virtuel et qu'il est en cours d'exécution, vous pouvez lancer une session virtuelle dans votre navigateur Web. La session vous permet d'interagir avec l'application installée sur votre ordinateur virtuel et de la gérer.

1. Choisissez Ordinateurs virtuels dans le volet de navigation de la console Lightsail for Research.

2. Recherchez le nom de l'ordinateur virtuel que vous avez créé à l'étape 1, puis choisissez Lancer l'application. Par exemple, Launch JupyterLab. Une session d'application s'ouvre dans une nouvelle fenêtre du navigateur Web.

   > **Important**
   >
   > Si un bloqueur de fenêtres contextuelles est installé sur votre navigateur Web, vous devrez peut-être autoriser les fenêtres contextuelles provenant du domaine aws.amazon.com avant d'ouvrir votre session.

Pour savoir comment vous connecter à votre ordinateur virtuel, passez à l'étape suivante de ce tutoriel.

Étape 4 : connexion de votre ordinateur virtuel

Vous pouvez vous connecter à votre ordinateur virtuel à l'aide des méthodes suivantes :

- Utilisez le client Amazon DCV basé sur un navigateur disponible dans la console Lightsail for Research. Avec Amazon DCV, vous pouvez utiliser une interface utilisateur graphique (GUI) pour interagir avec votre application de recherche et le système d'exploitation de votre ordinateur virtuel.

  Vous pouvez également accéder à l'interface de ligne de commande de votre ordinateur virtuel et transférer des fichiers à l'aide du client Amazon DCV basé sur un navigateur.
- Utilisez un client Secure Shell (SSH) tel qu'OpenSSH, PuTTY ou Windows Subsystem for Linux pour accéder à l'interface de la ligne de commande de votre ordinateur virtuel. Avec un client SSH, vous pouvez modifier des scripts et des fichiers de configuration.
- Utilisez Secure Copy (SCP) pour transférer des fichiers en toute sécurité entre votre ordinateur local et votre ordinateur virtuel. Avec SCP, vous pouvez démarrer votre travail localement et le poursuivre sur votre ordinateur virtuel. Vous pouvez également télécharger des fichiers depuis votre ordinateur virtuel pour copier votre travail sur votre ordinateur local.

Vous devez fournir la paire de clés de votre ordinateur virtuel pour vous y connecter via SSH ou pour transférer des fichiers via SCP. Une paire de clés est un ensemble d'informations de sécurité que vous utilisez pour prouver votre identité lorsque vous vous connectez à un ordinateur virtuel Lightsail for Research. Une paire de clés se compose d'une clé publique et d'une clé privée.

Pour plus d'informations sur la connexion à votre ordinateur privé, consultez la documentation suivante :

- Établissez une connexion au protocole d'affichage à distance :
  - Accédez à une application informatique virtuelle Lightsail for Research
  - Accédez au système d'exploitation de votre ordinateur virtuel Lightsail for Research
- Établissez une connexion SSH ou transférez des fichiers à l'aide de SCP :
  - Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research
  - Connectez-vous à un ordinateur virtuel Lightsail for Research à l'aide de Secure Shell
  - Transférez des fichiers vers des ordinateurs virtuels Lightsail for Research à l'aide de Secure Copy

Pour plus d'informations sur le stockage pour votre ordinateur virtuel, passez à l'étape suivante de ce tutoriel.

Étape 5 : ajouter du stockage sur votre ordinateur virtuel

Lightsail for Research fournit des volumes de stockage par blocs (disques) que vous pouvez associer à un ordinateur virtuel. Même si votre ordinateur virtuel est doté d'un disque système, vous pouvez y attacher des disques supplémentaires en fonction de l'évolution de vos besoins de stockage. Vous pouvez également détacher un disque d'un ordinateur virtuel et l'associer à un autre ordinateur virtuel.

Lorsque vous connectez un disque à votre ordinateur virtuel à l'aide de la console, Lightsail for Research formate et monte automatiquement le disque dans votre système d'exploitation. Ce processus prend quelques minutes. Vous devez donc vérifier que le disque est à l'état Monté avant de commencer à l'utiliser.

Pour plus d'informations sur la création, l'attachement et la gestion d'un disque, consultez la documentation suivante :

- Création d'un disque de stockage dans la console Lightsail for Research
- Afficher les détails du disque de stockage dans la console Lightsail for Research
- Ajouter de l'espace de stockage à un ordinateur virtuel dans Lightsail for Research
- Détacher un disque d'un ordinateur virtuel dans Lightsail for Research
- Supprimer les disques de stockage inutilisés dans Lightsail for Research

Pour plus d'informations sur la sauvegarde de votre ordinateur virtuel, passez à l'étape suivante de ce tutoriel.

Étape 6 : créer un instantané

Les instantanés sont une point-in-time copie de vos données. Vous pouvez créer des instantanés de vos ordinateurs virtuels et les utiliser comme base de référence pour créer de nouveaux ordinateurs ou pour sauvegarder des données. Un instantané contient toutes les données nécessaires pour restaurer votre ordinateur (au moment où l'instantané a été pris).

Pour plus d'informations sur la création et la gestion des instantanés, consultez la documentation suivante :

- Créez des instantanés d'ordinateurs ou de disques virtuels Lightsail for Research
- Afficher et gérer des instantanés d'ordinateurs virtuels et de disques dans Lightsail for Research
- Créer un ordinateur ou un disque virtuel à partir d'un instantané
- Supprimer un instantané dans la console Lightsail for Research

Pour en savoir plus sur le nettoyage des ressources de votre ordinateur virtuel, passez à l'étape suivante de ce tutoriel.

Étape 7 : nettoyer

Une fois que vous avez fini avec l'ordinateur virtuel que vous avez créé dans le cadre de ce tutoriel, vous pouvez le supprimer. Cela permet de ne plus facturer de frais pour l'ordinateur virtuel si vous n'en avez pas besoin.

La suppression d'un ordinateur virtuel ne supprime pas les instantanés ou les disques attachés qui lui sont associés. Si vous avez créé des instantanés et des disques, vous devez les supprimer manuellement pour ne plus vous facturer de frais.

Pour enregistrer votre ordinateur virtuel pour plus tard, mais pour éviter de payer des frais aux prix horaires standard, vous pouvez arrêter l'ordinateur virtuel au lieu de le supprimer. Ensuite, vous pourrez le redémarrer plus tard. Pour de plus amples informations, veuillez consulter Afficher les détails de l'ordinateur virtuel Lightsail for Research. Pour plus d'informations sur les tarifs, consultez la section Tarification de Lightsail for Research.

> **Important**
>
> La suppression d'une ressource Lightsail for Research est une action permanente. Les données supprimées ne peuvent pas être récupérées. Si vous avez besoin des données ultérieurement, créez un instantané de votre ordinateur virtuel avant de le supprimer. Pour plus d'informations, consultez Création d'un instantané (français non garanti).

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, sélectionnez Ordinateurs virtuels.
3. Choisissez l'ordinateur virtuel à supprimer.
4. Choisissez Actions, puis sélectionnez Supprimer l'ordinateur virtuel.
5. Tapez confirmer dans le bloc de texte. Choisissez ensuite Supprimer l'ordinateur virtuel.

Commencez à utiliser les applications de science des données sur Lightsail for Research

Les didacticiels suivants fournissent des informations supplémentaires sur la manière de démarrer avec des applications spécifiques disponibles dans Lightsail for Research.

Rubriques

> **Note**
>
> Un didacticiel détaillé pour démarrer avec Lightsail for Research est publié sur le RStudio blog AWS du secteur public. Pour plus d'informations, consultez Getting started with Amazon Lightsail for Research : A tutorial using. RStudio

Lancement et utilisation JupyterLab sur Lightsail for Research

Dans ce didacticiel, nous vous expliquons comment commencer à gérer et à utiliser votre ordinateur JupyterLab virtuel dans Amazon Lightsail for Research.

Rubriques

Étape 1 : Exécuter les prérequis

Créez un ordinateur virtuel à l'aide de l' JupyterLab application si ce n'est pas déjà fait. Pour de plus amples informations, veuillez consulter Création d'un ordinateur virtuel Lightsail for Research.

Une fois que votre nouvel ordinateur virtuel est opérationnel, passez à la section Lancer l' JupyterLab application de ce didacticiel.

Étape 2 : (Facultatif) ajouter de l'espace de stockage

Votre ordinateur virtuel est fourni avec un disque système. Toutefois, à mesure que vos besoins de stockage évoluent, vous pouvez attacher des disques supplémentaires à votre ordinateur virtuel pour augmenter son espace de stockage.

Vous pouvez également stocker vos fichiers de travail sur un disque attaché. Vous pouvez ensuite détacher le disque et l'attacher à un autre ordinateur virtuel pour déplacer rapidement vos fichiers d'un ordinateur à un autre.

Vous pouvez également créer un instantané d'un disque attaché sur lequel se trouvent vos fichiers de travail, puis créer une copie de disque à partir de l'instantané. Vous pouvez ensuite attacher le nouveau disque copié à un autre ordinateur pour copier votre travail sur différents ordinateurs virtuels. Pour plus d'informations, consultez Création d'un disque de stockage dans la console Lightsail for Research et Ajouter de l'espace de stockage à un ordinateur virtuel dans Lightsail for Research.

> **Note**
>
> Lorsque vous connectez un disque à votre ordinateur virtuel à l'aide de la console, Lightsail for Research formate et monte automatiquement le disque. Ce processus prend quelques minutes. Vous devez donc vérifier que le disque a atteint l'état de montage Monté avant de commencer à l'utiliser. Par défaut, Lightsail for Research monte les disques dans le répertoire. `/home/lightsail-user/<disk-name>` `<disk-name>`est le nom que vous avez donné à votre disque.

Étape 3 : charger et télécharger des fichiers

Vous pouvez télécharger des fichiers sur votre ordinateur JupyterLab virtuel et télécharger des fichiers à partir de celui-ci. Pour ce faire, exécutez les étapes suivantes :

1. Procurez-vous une paire de clés auprès d'Amazon Lightsail. Pour de plus amples informations, veuillez consulter Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research.
2. Une fois que vous avez la paire de clés, vous pouvez l'utiliser pour établir une connexion à l'aide de l'utilitaire Secure Copy (SCP). Le SCP vous permet de charger et de télécharger des fichiers à l'aide d'une invite de commande ou d'un terminal. Pour de plus amples informations, veuillez consulter Transférez des fichiers vers des ordinateurs virtuels Lightsail for Research à l'aide de Secure Copy.
3. (Facultatif) Vous pouvez également utiliser la paire de clés pour vous connecter à votre ordinateur virtuel via SSH. Pour de plus amples informations, veuillez consulter Connectez-vous à un ordinateur virtuel Lightsail for Research à l'aide de Secure Shell.

> **Note**
>
> Vous pouvez également accéder à l'interface de ligne de commande de votre ordinateur virtuel et transférer des fichiers à l'aide du client Amazon DCV basé sur un navigateur. Amazon DCV est disponible dans la console Lightsail for Research. Pour plus d'informations, consultez Accédez à une application informatique virtuelle Lightsail for Research et Accédez au système d'exploitation de votre ordinateur virtuel Lightsail for Research.

Pour gérer les fichiers de votre projet sur un disque de stockage attaché, assurez-vous de les charger dans le répertoire de montage approprié pour le disque attaché. Lorsque vous connectez un disque à votre ordinateur virtuel à l'aide de la console, Lightsail for Research formate et monte automatiquement le disque dans le répertoire. `/home/lightsail-user/<disk-name>` *<disk-name>*est le nom que vous avez donné à votre disque.

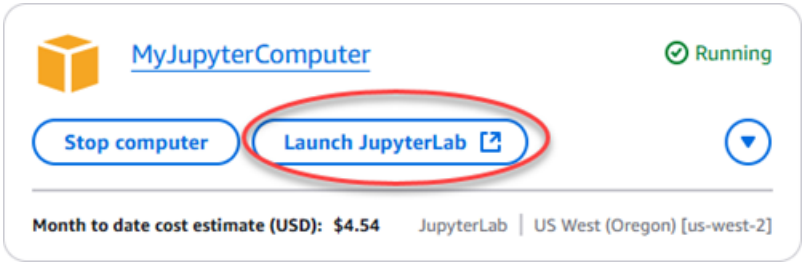
Étape 4 : Lancez l' JupyterLabapplication

Procédez comme suit pour lancer l' JupyterLab application sur votre nouvel ordinateur virtuel.

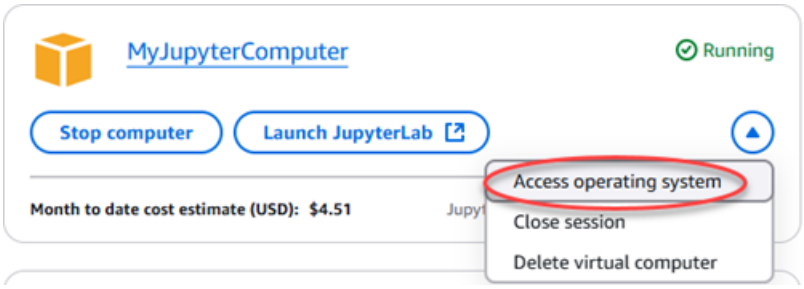
> **Important**
>
> Ne mettez pas à jour le système d'exploitation ou JupyterLab l'application même si vous y êtes invité. Choisissez plutôt l'option permettant de fermer ou d'ignorer ces invites. De plus, ne modifiez aucun des fichiers qui se trouvent dans le répertoire /home/lightsail-admin/. Ces actions peuvent rendre l'ordinateur virtuel inutilisable.

1. Connectez-vous à la console Lightsail for Research.
2. Choisissez Ordinateurs virtuels dans le panneau de navigation pour afficher les ordinateurs virtuels disponibles dans votre compte.
3. Sur la page Ordinateurs virtuels, recherchez votre ordinateur virtuel et choisissez l'une des options suivantes pour vous y connecter :

   a. (Recommandé) Choisissez Lancer JupyterLab pour lancer l' JupyterLab application en mode ciblé. Si vous ne vous êtes pas connecté récemment à votre ordinateur virtuel, vous devrez peut-être attendre quelques minutes pendant que Lightsail for Research prépare votre session.



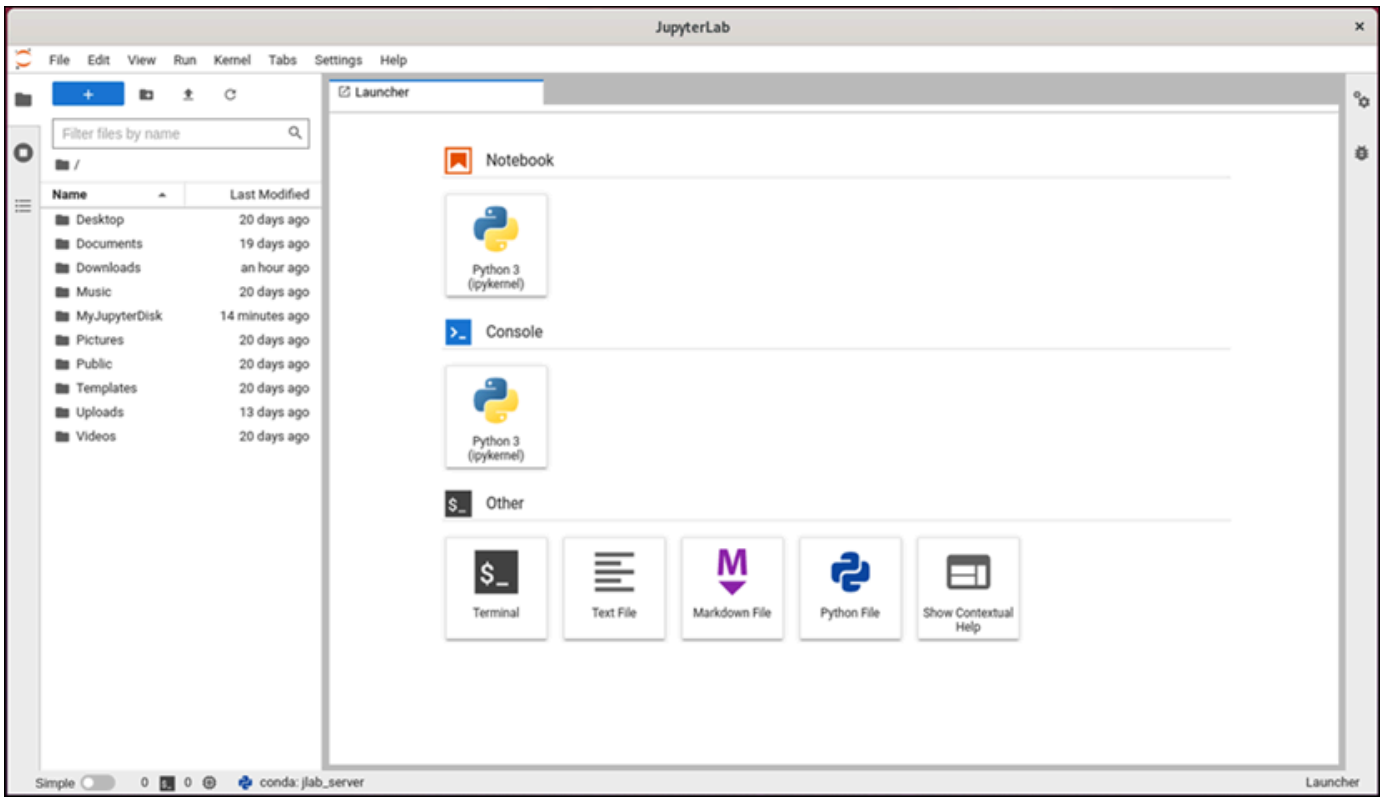
   b. Choisissez le menu déroulant de l'ordinateur, puis sélectionnez Accéder au système d'exploitation pour accéder au bureau de votre ordinateur virtuel.



Lightsail for Research exécute quelques commandes pour établir la connexion au protocole d'affichage à distance. Après quelques instants, un nouvel onglet de navigateur s'ouvre avec une connexion de bureau virtuel établie avec votre ordinateur virtuel. Si vous avez choisi l'option Lancer l'application, passez à l'étape suivante de cette procédure pour ouvrir un fichier dans l' JupyterLab application. Si vous avez choisi l'option Accéder au système d'exploitation, vous pouvez ouvrir d'autres applications via le bureau Ubuntu.

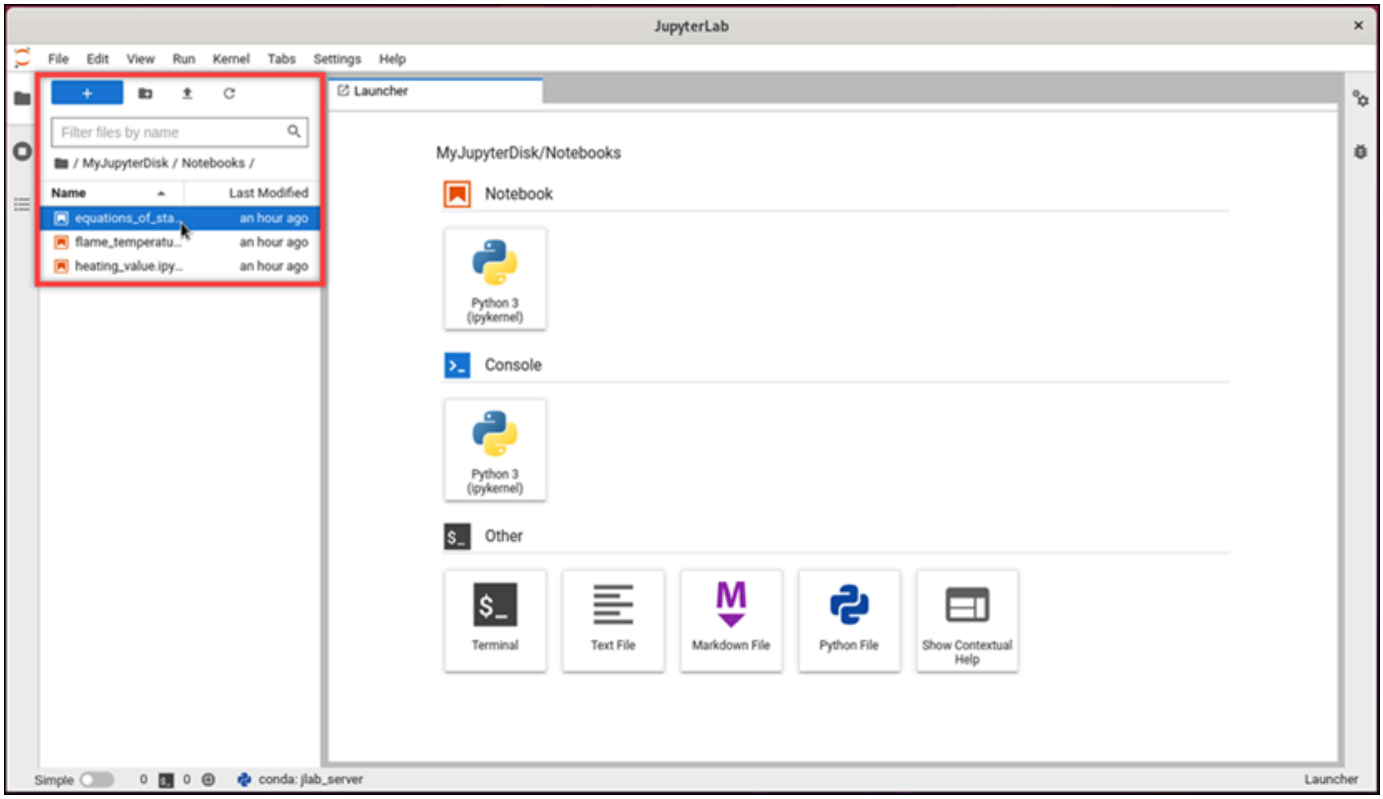
> **Note**
>
> Votre navigateur peut vous demander d'autoriser le partage de votre presse-papiers. Cette option vous permet de copier-coller entre votre ordinateur local et votre ordinateur virtuel.
>
> Ubuntu peut également vous demander une configuration initiale. Suivez les invites jusqu'à ce que vous ayez terminé la configuration et que vous puissiez utiliser le système d'exploitation.

4. L' JupyterLab application s'ouvre. Dans le menu du lanceur, vous pouvez créer un nouveau bloc-notes, lancer la console, le terminal et créer divers fichiers.

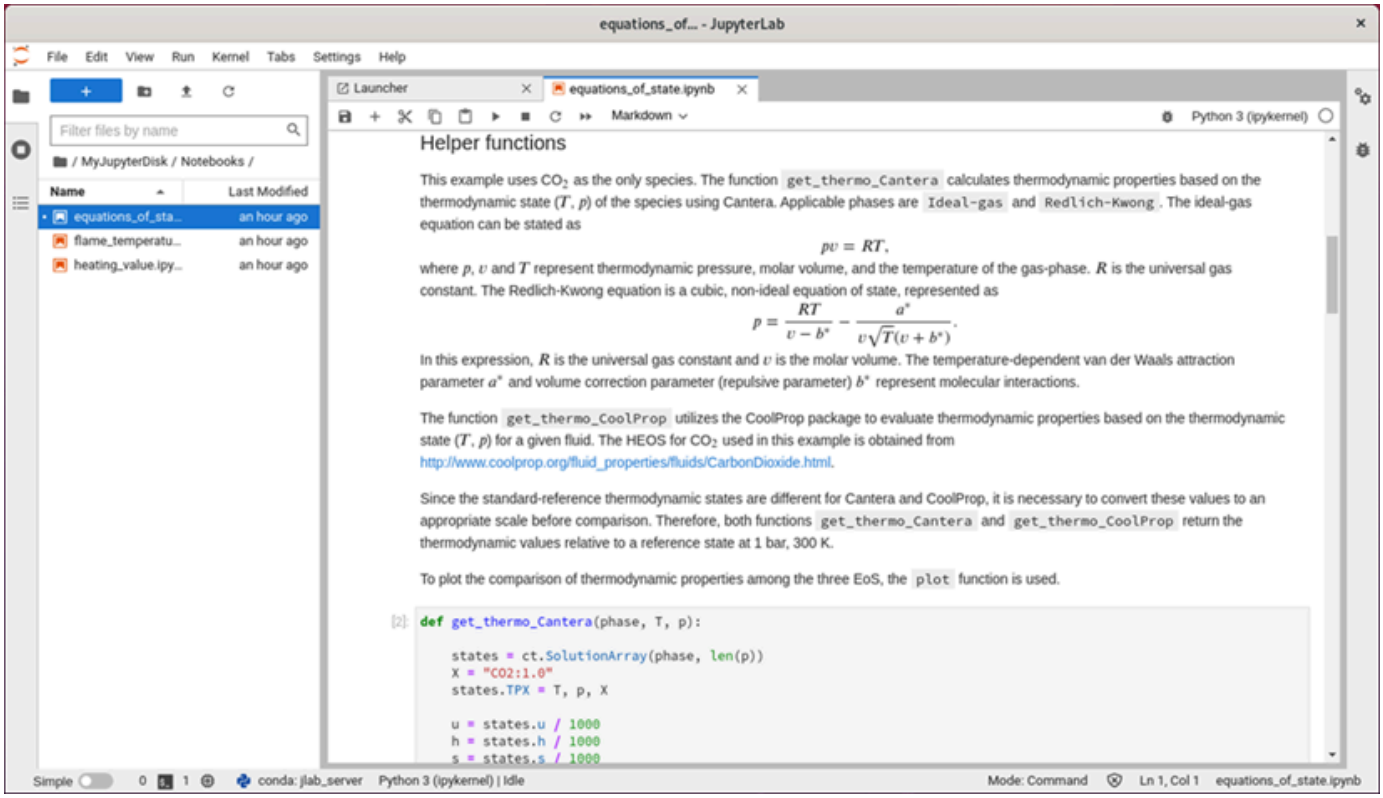


5. Pour ouvrir un fichier JupyterLab, dans le volet Explorateur de fichiers, choisissez le répertoire ou le dossier dans lequel les fichiers de votre projet sont stockés. Puis choisissez le fichier à ouvrir.

   Si vous avez chargé les fichiers de votre projet sur un disque attaché, recherchez le répertoire dans lequel le disque est monté. Par défaut, Lightsail for Research monte les disques dans le répertoire. `/home/lightsail-user/<disk-name>` `<disk-name>`est le nom que vous avez donné à votre disque. Dans l'exemple suivant, le répertoire `MyJupyterDisk` représente le disque monté et le sous-répertoire `Notebooks` contient nos fichiers de bloc-notes Jupyter.



Dans l'exemple suivant, nous avons ouvert le fichier de bloc-notes Jupyter `equations_of_state.ipynb`.



Pour plus d'informations sur le démarrage, passez à la section Étape 5 : lire la JupyterLab documentation de ce tutoriel.

Étape 5 : lire la JupyterLab documentation

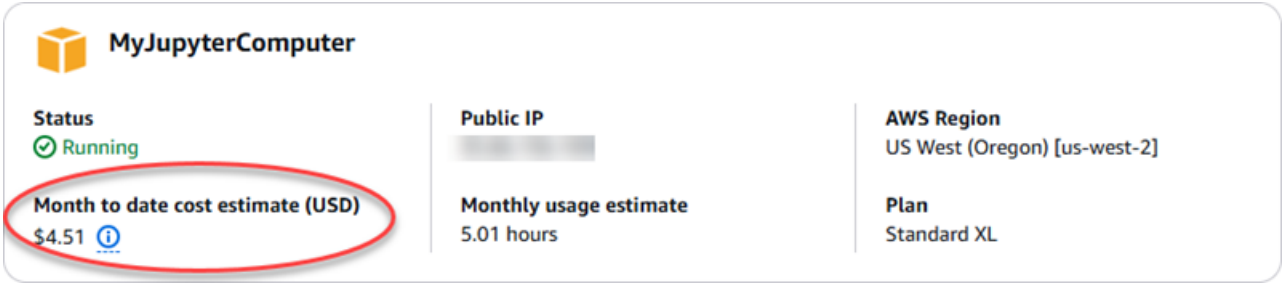
Si vous ne les connaissez pas JupyterLab, nous vous recommandons de lire leur documentation officielle. Les ressources JupyterLab en ligne suivantes sont disponibles :

- Documentation JupyterLab
- Forum Jupyter Discourse (français non garanti)
- JupyterLab sur StackOverflow
- JupyterLab sur GitHub

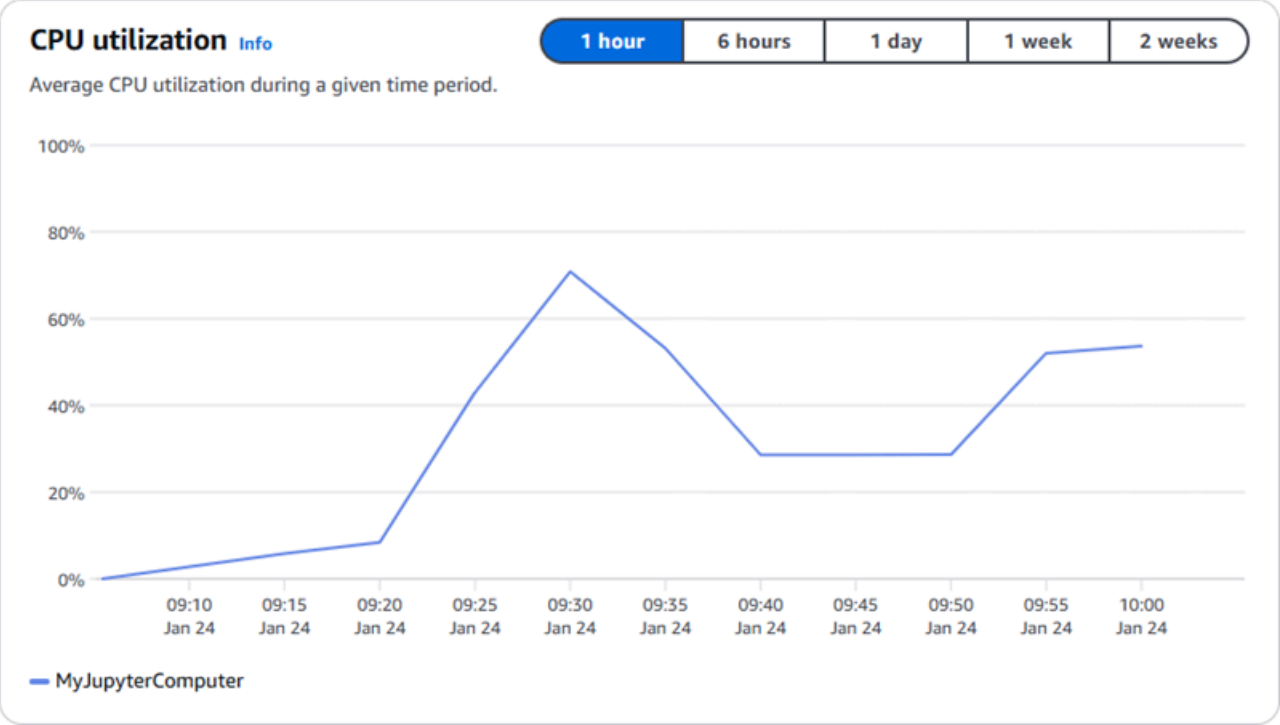
Étape 6 : (Facultatif) surveiller l'utilisation et les coûts

Les estimations du coût mensuel et de l'utilisation de vos ressources Lightsail for Research sont affichées dans les zones suivantes de la console Lightsail for Research.

1. Choisissez Ordinateurs virtuels dans le volet de navigation de la console Lightsail for Research. L'estimation des coûts mensuels cumulés de vos ordinateurs virtuels est répertoriée sous chaque ordinateur virtuel en cours d'exécution.



2. Pour afficher l'utilisation du CPU d'un ordinateur virtuel, choisissez le nom de l'ordinateur virtuel, puis cliquez sur l'onglet Tableau de bord.



3. Pour consulter le coût mensuel cumulé et les estimations d'utilisation de toutes vos ressources Lightsail for Research, sélectionnez Utilisation dans le volet de navigation.

Étape 7 : (Facultatif) créer une règle de contrôle des coûts

Gérez l'utilisation et les coûts de vos ordinateurs virtuels en créant des règles de contrôle des coûts. Vous pouvez créer une règle d'Arrêter l'ordinateur virtuel en veille qui arrête un ordinateur en cours d'exécution lorsqu'il atteint un pourcentage spécifié de son utilisation du CPU au cours d'une période donnée. Par exemple, une règle peut arrêter automatiquement un ordinateur spécifique lorsque son utilisation du CPU est égale ou inférieure à 5 % pendant une période de 30 minutes. Cela peut signifier que l'ordinateur est inactif et que Lightsail for Research arrête l'ordinateur afin que vous n'ayez pas à payer de frais pour une ressource inactive.

> **Important**
>
> Avant de créer une règle pour arrêter votre ordinateur virtuel en mode veille, nous vous recommandons de surveiller l'utilisation de son CPU pendant quelques jours. Prenez note de l'utilisation du CPU lorsque votre ordinateur virtuel est soumis à des charges différentes. Par exemple, lorsqu'il compile du code, traite une opération et tourne au ralenti. Cela vous aidera à déterminer un seuil précis pour la règle. Pour plus d'informations, veuillez consulter la section Étape 6 : (Facultatif) surveiller l'utilisation et les coûts de ce tutoriel.
> Si vous créez une règle avec un seuil d'utilisation du CPU supérieur à votre charge de travail, la règle peut arrêter consécutivement votre ordinateur virtuel. Par exemple, si vous démarrez votre ordinateur virtuel immédiatement après qu'une règle l'ait arrêté, la règle se réactive et l'ordinateur s'arrête à nouveau.

Les instructions détaillées relatives à la création et à la gestion des règles de contrôle des coûts sont disponibles dans les guides suivants :

- Gérez les règles de contrôle des coûts dans Lightsail for Research
- Créez des règles de contrôle des coûts pour vos ordinateurs virtuels Lightsail for Research
- Supprimer les règles de contrôle des coûts pour vos ordinateurs virtuels Lightsail for Research

Étape 8 : (Facultatif) créer un instantané

Les instantanés sont une point-in-time copie de vos données. Vous pouvez créer des instantanés de vos ordinateurs virtuels et les utiliser comme base de référence pour créer de nouveaux ordinateurs ou pour sauvegarder des données. Un instantané contient toutes les données nécessaires pour restaurer votre ordinateur (au moment où l'instantané a été pris).

Vous trouverez des instructions détaillées sur la création et la gestion des instantanés dans les guides suivants :

- Créez des instantanés d'ordinateurs ou de disques virtuels Lightsail for Research
- Afficher et gérer des instantanés d'ordinateurs virtuels et de disques dans Lightsail for Research
- Créer un ordinateur ou un disque virtuel à partir d'un instantané
- Supprimer un instantané dans la console Lightsail for Research

Étape 9 : (Facultatif) arrêter ou supprimer votre ordinateur virtuel

Une fois que vous avez fini avec l'ordinateur virtuel que vous avez créé dans le cadre de ce tutoriel, vous pouvez le supprimer. Cela permet de ne plus facturer de frais pour l'ordinateur virtuel si vous n'en avez pas besoin.

La suppression d'un ordinateur virtuel ne supprime pas les instantanés ou les disques attachés qui lui sont associés. Si vous avez créé des instantanés et des disques, vous devez les supprimer manuellement pour ne plus vous facturer de frais.

Pour enregistrer votre ordinateur virtuel pour plus tard, mais pour éviter de payer des frais aux prix horaires standard, vous pouvez arrêter l'ordinateur virtuel au lieu de le supprimer. Ensuite, vous pourrez le redémarrer plus tard. Pour de plus amples informations, veuillez consulter Afficher les détails de l'ordinateur virtuel Lightsail for Research. Pour plus d'informations sur les tarifs, consultez la section Tarification de Lightsail for Research.

> **Important**
>
> La suppression d'une ressource Lightsail for Research est une action permanente. Les données supprimées ne peuvent pas être récupérées. Si vous avez besoin des données ultérieurement, créez un instantané de votre ordinateur virtuel avant de le supprimer. Pour plus d'informations, consultez Création d'un instantané (français non garanti).

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, sélectionnez Ordinateurs virtuels.
3. Choisissez l'ordinateur virtuel à supprimer.
4. Choisissez Actions, puis sélectionnez Supprimer l'ordinateur virtuel.
5. Tapez confirmer dans le bloc de texte. Choisissez ensuite Supprimer l'ordinateur virtuel.

Lancement et utilisation RStudio sur Lightsail for Research

Dans ce didacticiel, nous vous expliquons comment commencer à gérer et à utiliser votre ordinateur RStudio virtuel dans Amazon Lightsail for Research.

> **Note**
>
> Un didacticiel détaillé pour démarrer avec Lightsail for Research est publié sur le RStudio blog AWS du secteur public. Pour plus d'informations, consultez Getting started with Amazon Lightsail for Research : A tutorial using. RStudio

Rubriques

Étape 1 : Exécuter les prérequis

Créez un ordinateur virtuel à l'aide de l' RStudio application si ce n'est pas déjà fait. Pour de plus amples informations, veuillez consulter Création d'un ordinateur virtuel Lightsail for Research.

Étape 2 : (Facultatif) ajouter de l'espace de stockage

Votre ordinateur virtuel est fourni avec un disque système. Toutefois, à mesure que vos besoins de stockage évoluent, vous pouvez attacher des disques supplémentaires à votre ordinateur virtuel pour augmenter son espace de stockage.

Vous pouvez également stocker vos fichiers de travail sur un disque attaché. Vous pouvez ensuite détacher le disque et l'attacher à un autre ordinateur virtuel pour déplacer rapidement vos fichiers d'un ordinateur à un autre.

Vous pouvez également créer un instantané d'un disque attaché sur lequel se trouvent vos fichiers de travail, puis créer une copie de disque à partir de l'instantané. Vous pouvez ensuite attacher le nouveau disque dupliqué à un autre ordinateur pour copier votre travail sur différents ordinateurs virtuels. Pour plus d'informations, consultez Création d'un disque de stockage dans la console Lightsail for Research et Ajouter de l'espace de stockage à un ordinateur virtuel dans Lightsail for Research.

> **Note**
>
> Lorsque vous connectez un disque à votre ordinateur virtuel à l'aide de la console, Lightsail for Research formate et monte automatiquement le disque. Ce processus prend quelques minutes. Vous devez donc vérifier que le disque a atteint l'état de montage Monté avant de commencer à l'utiliser. Par défaut, Lightsail for Research monte les disques dans le *<disk-name>* répertoire dont `/home/lightsail-user/`*<disk-name>* le nom est celui que vous avez attribué à votre disque.

Étape 3 : charger et télécharger des fichiers

Vous pouvez télécharger des fichiers sur votre ordinateur RStudio virtuel et télécharger des fichiers à partir de celui-ci. Pour ce faire, exécutez les étapes suivantes :

1. Procurez-vous une paire de clés auprès d'Amazon Lightsail. Pour de plus amples informations, veuillez consulter Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research.
2. Une fois que vous avez la paire de clés, vous pouvez l'utiliser pour établir une connexion à l'aide de l'utilitaire Secure Copy (SCP). Le SCP vous permet de charger et de télécharger des fichiers à l'aide d'une invite de commande ou d'un terminal. Pour de plus amples informations, veuillez consulter Transférez des fichiers vers des ordinateurs virtuels Lightsail for Research à l'aide de Secure Copy.
3. (Facultatif) Vous pouvez également utiliser la paire de clés pour vous connecter à votre ordinateur virtuel via SSH. Pour de plus amples informations, veuillez consulter Connectez-vous à un ordinateur virtuel Lightsail for Research à l'aide de Secure Shell.

> **Note**
>
> Vous pouvez également accéder à l'interface de ligne de commande de votre ordinateur virtuel et transférer des fichiers à l'aide du client Amazon DCV basé sur un navigateur. Amazon DCV est disponible dans la console Lightsail for Research. Pour plus d'informations, consultez Accédez à une application informatique virtuelle Lightsail for Research et Accédez au système d'exploitation de votre ordinateur virtuel Lightsail for Research.

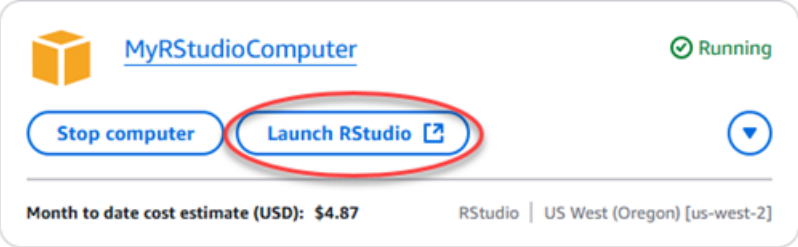
Étape 4 : Lancez l' RStudioapplication

Procédez comme suit pour lancer l' RStudio application sur votre nouvel ordinateur virtuel.

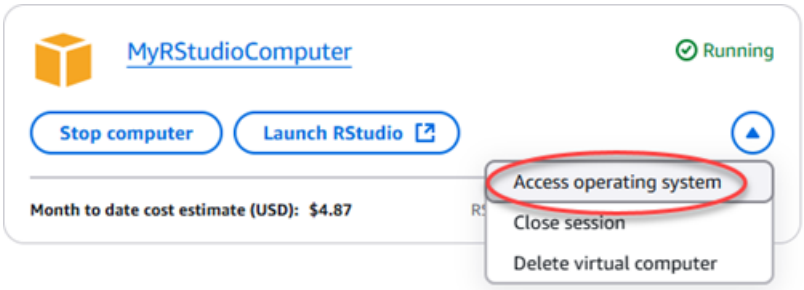
> **Important**
>
> Ne mettez pas à jour le système d'exploitation ou RStudio l'application même si vous y êtes invité. Choisissez plutôt l'option permettant de fermer ou d'ignorer ces invites. De plus, ne modifiez aucun des fichiers qui se trouvent dans le répertoire /home/lightsail-admin/. Ces actions peuvent rendre l'ordinateur virtuel inutilisable.

1. Connectez-vous à la console Lightsail for Research.
2. Choisissez Ordinateurs virtuels dans le panneau de navigation pour afficher les ordinateurs virtuels disponibles dans votre compte.
3. Sur la page Ordinateurs virtuels, recherchez votre ordinateur virtuel et choisissez l'une des options suivantes pour vous y connecter :

   a. (Recommandé) Choisissez Lancer RStudio pour lancer l' RStudio application en mode ciblé. Si vous ne vous êtes pas connecté récemment à votre ordinateur virtuel, vous devrez peut-être attendre quelques minutes pendant que Lightsail for Research prépare votre session.



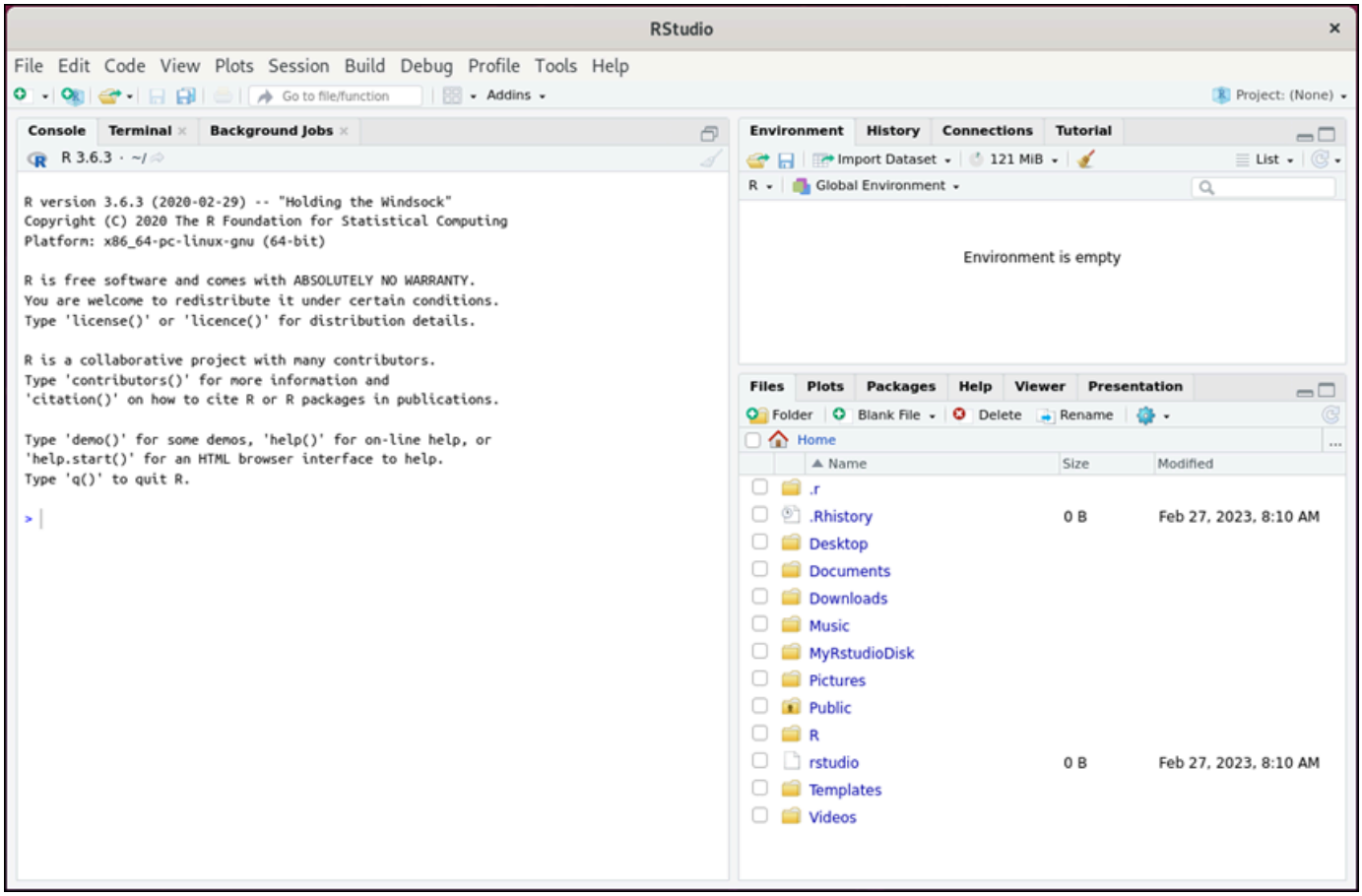
b. Choisissez le menu déroulant de l'ordinateur, puis sélectionnez Accéder au système d'exploitation pour accéder au bureau de votre ordinateur virtuel. Procédez ainsi si vous souhaitez installer une autre application sur le système d'exploitation.



Lightsail for Research exécute quelques commandes pour établir la connexion au protocole d'affichage à distance. Après quelques instants, un nouvel onglet de navigateur s'ouvre avec une connexion de bureau virtuel établie avec votre ordinateur virtuel. Si vous avez choisi l'option Lancer l'application, passez à l'étape suivante de cette procédure pour ouvrir un fichier dans l' RStudio application. Si vous avez choisi l'option Accéder au système d'exploitation, vous pouvez ouvrir d'autres applications via le bureau Ubuntu.

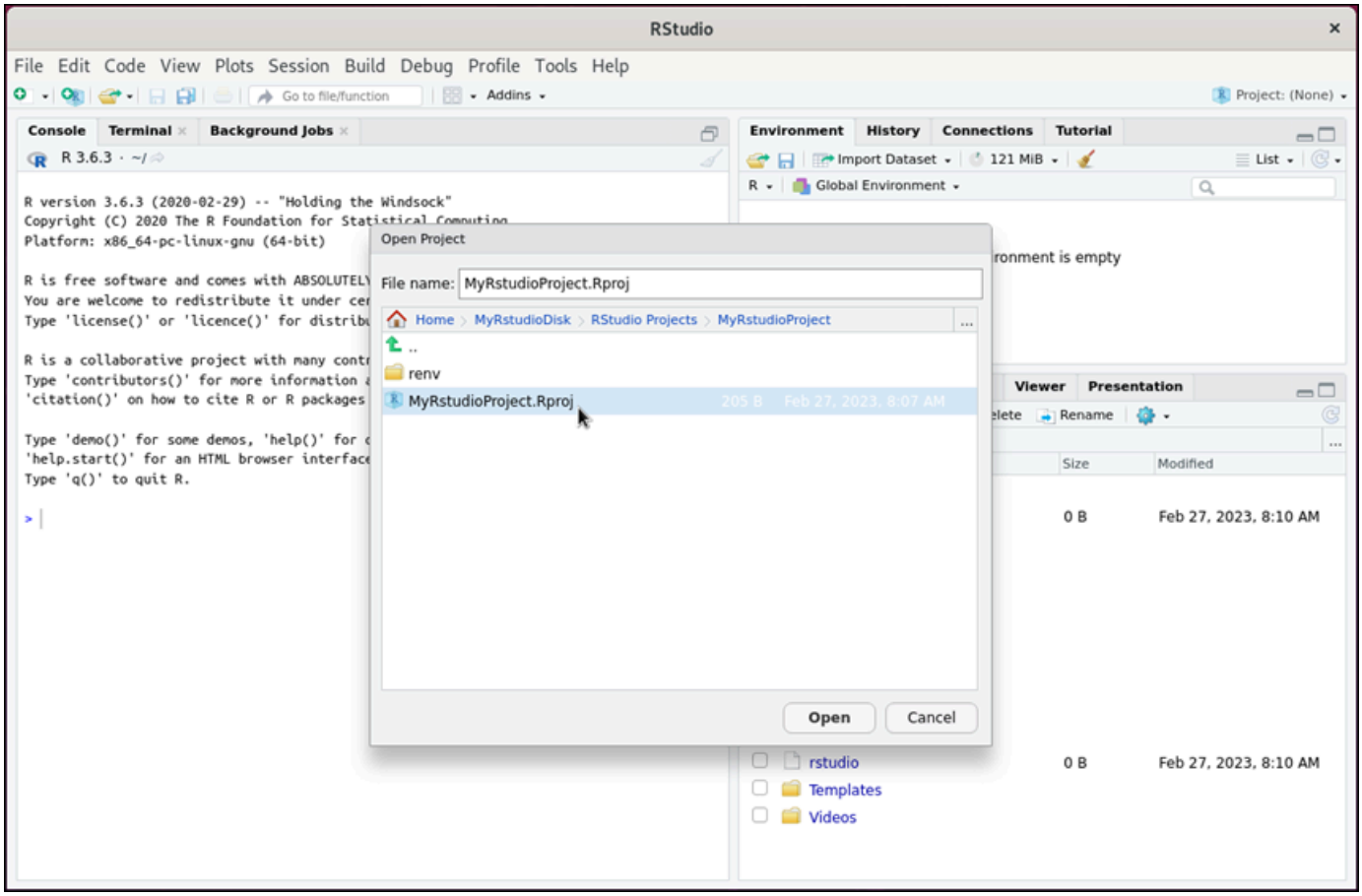
> **Note**
>
> Votre navigateur peut vous demander d'autoriser le partage de votre presse-papiers. Cette option vous permet de copier-coller entre votre ordinateur local et votre ordinateur virtuel.
>
> Ubuntu peut également vous demander une configuration initiale. Suivez les invites jusqu'à ce que vous ayez terminé la configuration et que vous puissiez utiliser le système d'exploitation.

4. L' RStudio application s'ouvre.

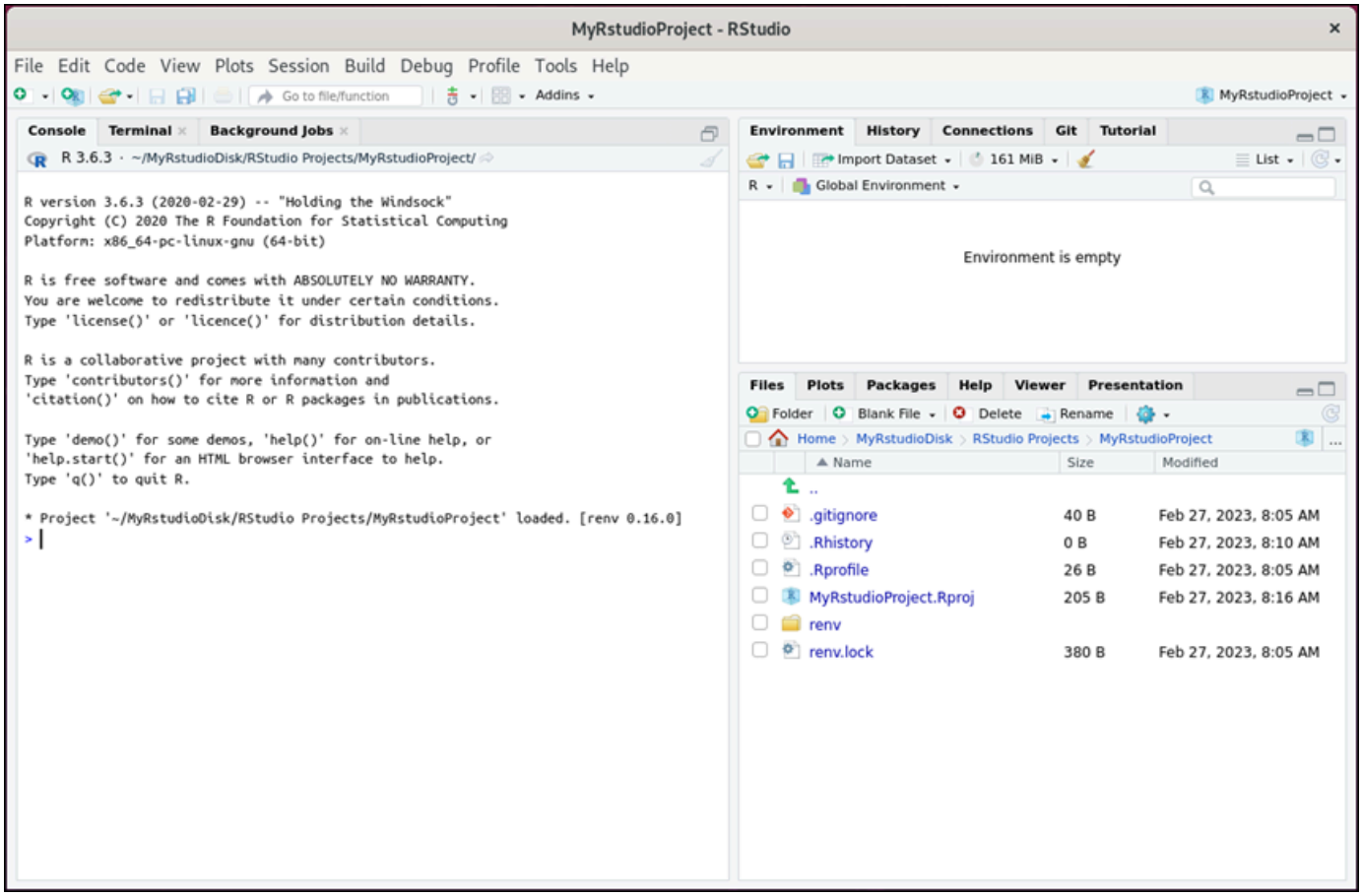


5. Pour ouvrir un projet dans RStudio, choisissez le menu Fichier, puis sélectionnez Ouvrir un projet. Naviguez jusqu'au répertoire ou dossier dans lequel les fichiers de votre projet sont stockés. Puis choisissez le fichier à ouvrir.

   Si vous avez chargé les fichiers de votre projet sur un disque attaché, recherchez le répertoire dans lequel le disque est monté. Par défaut, Lightsail for Research monte les disques dans le répertoire. `/home/lightsail-user/<disk-name>` `<disk-name>`est le nom que vous avez donné à votre disque. Dans l'exemple suivant, le `MyRstudioDisk` répertoire représente le disque monté et le `Projects` sous-répertoire contient nos fichiers de RStudio projet.



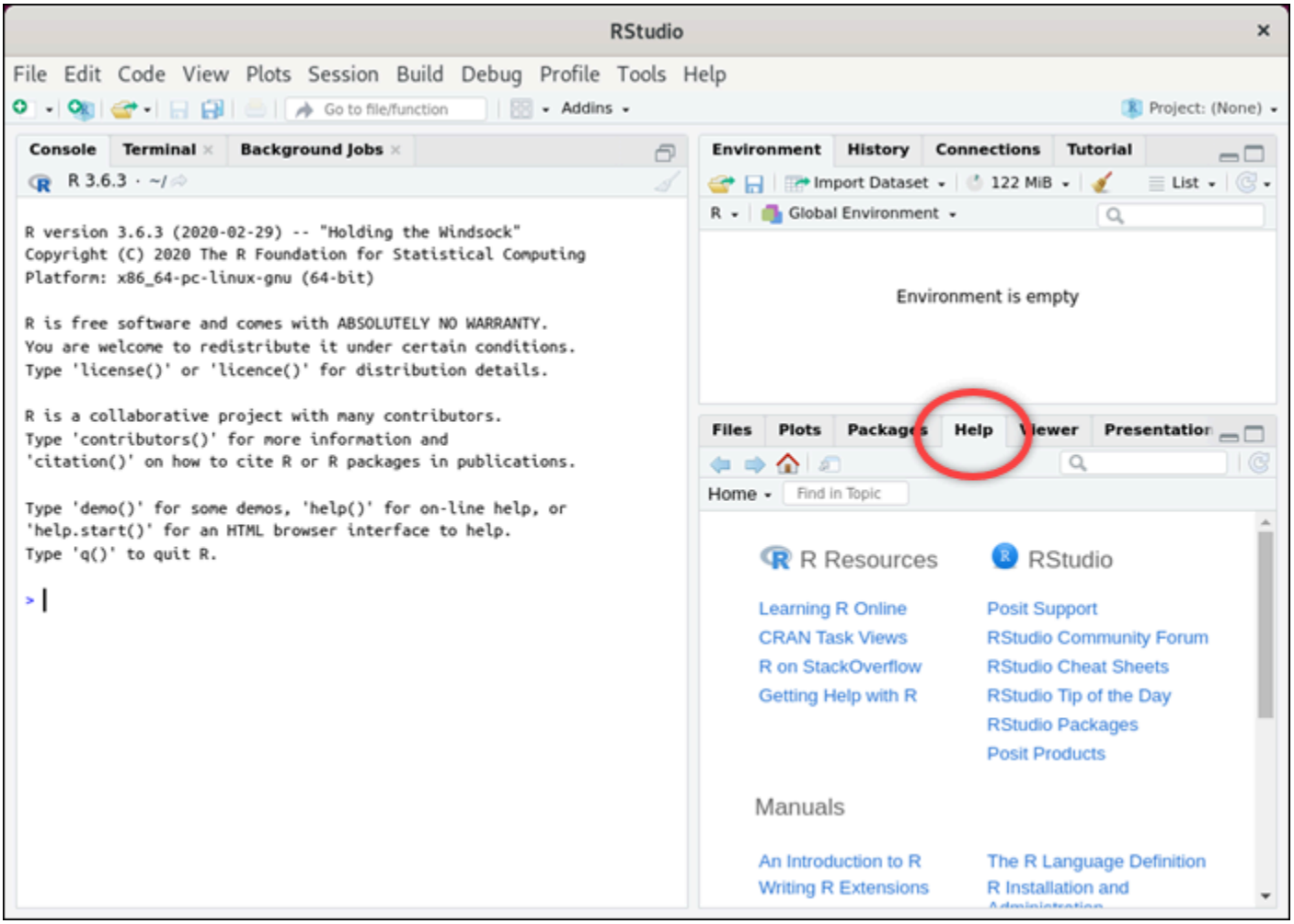
Dans l'exemple suivant, nous avons ouvert le fichier de projet `MyRstudioProject.Rproj`.



Pour plus d'informations sur la façon de démarrer RStudio, passez à la Étape 5 : lire la RStudio documentation section de ce didacticiel.

Étape 5 : lire la RStudio documentation

L' RStudio application est fournie avec un package de documentation complet. Pour commencer à apprendre RStudio, nous vous recommandons d'accéder à l'onglet Aide RStudio comme indiqué dans l'exemple suivant.



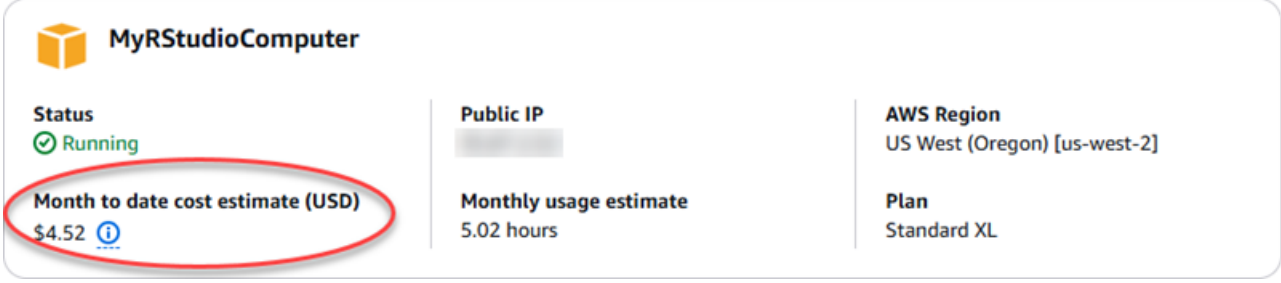
Les ressources RStudio en ligne suivantes sont également disponibles :

- Apprentissage R en ligne (français non garanti)
- R sur StackOverflow
- Obtenir de l'aide avec R (français non garanti)
- Support Posit (français non garanti)
- RStudioForum communautaire
- RStudio Feuilles de triche
- RStudio Conseil du jour (Twitter)
- RStudioForfaits

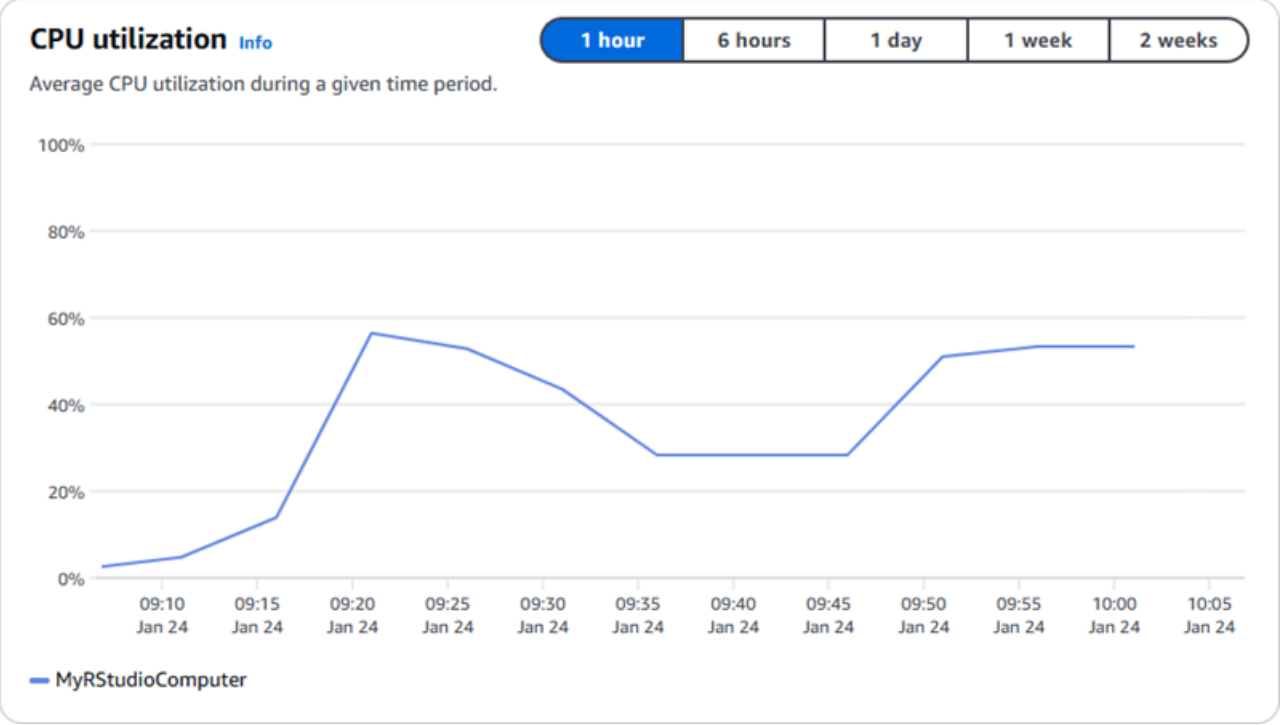
Étape 6 : (Facultatif) surveiller l'utilisation et les coûts

Les estimations du coût mensuel et de l'utilisation de vos ressources Lightsail for Research sont affichées dans les zones suivantes de la console Lightsail for Research.

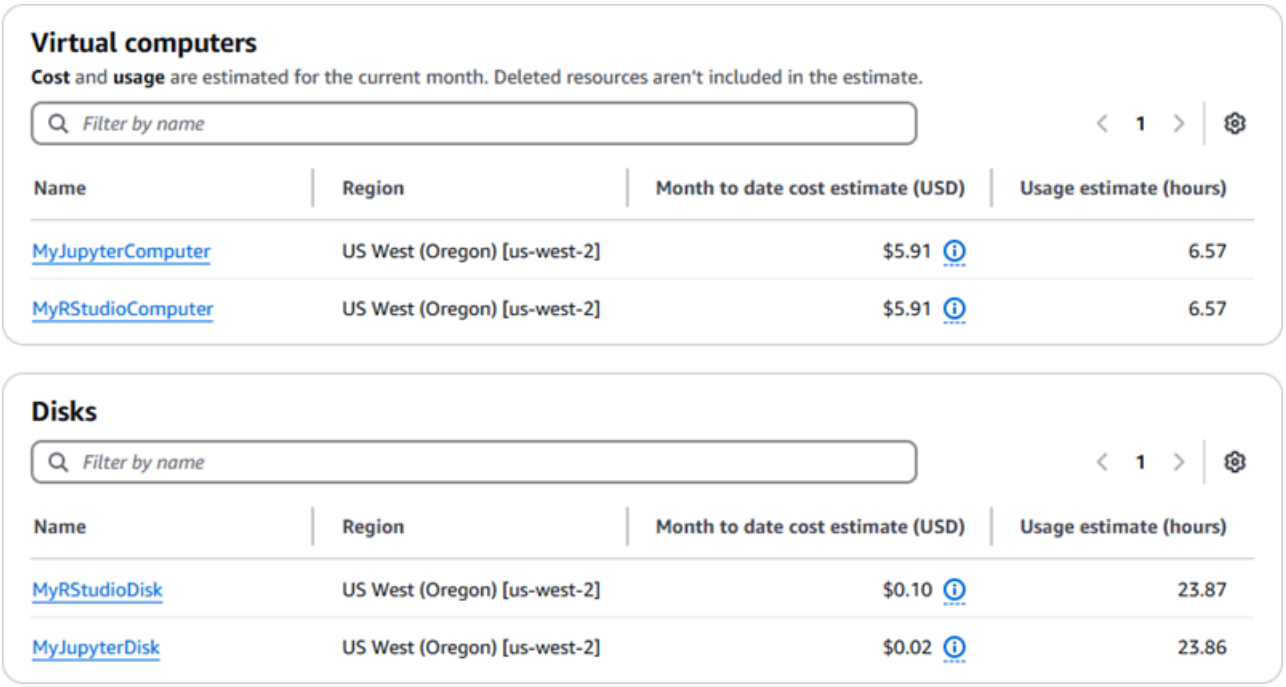
1. Choisissez Ordinateurs virtuels dans le volet de navigation de la console Lightsail for Research. L'estimation des coûts mensuels cumulés de vos ordinateurs virtuels est répertoriée sous chaque ordinateur virtuel en cours d'exécution.



2. Pour afficher l'utilisation du CPU d'un ordinateur virtuel, choisissez le nom de l'ordinateur virtuel, puis cliquez sur l'onglet Tableau de bord.



3. Pour consulter le coût mensuel cumulé et les estimations d'utilisation de toutes vos ressources Lightsail for Research, sélectionnez Utilisation dans le volet de navigation.



Étape 7 : (Facultatif) créer une règle de contrôle des coûts

Gérez l'utilisation et les coûts de vos ordinateurs virtuels en créant des règles de contrôle des coûts. Vous pouvez créer une règle d'Arrêter l'ordinateur virtuel en veille qui arrête un ordinateur en cours d'exécution lorsqu'il atteint un pourcentage spécifié de son utilisation du CPU au cours d'une période donnée. Par exemple, une règle peut arrêter automatiquement un ordinateur spécifique lorsque son utilisation du CPU est égale ou inférieure à 5 % pendant une période de 30 minutes. Cela peut signifier que l'ordinateur est inactif et que Lightsail for Research arrête l'ordinateur afin que vous n'ayez pas à payer de frais pour une ressource inactive.

Important

Avant de créer une règle pour arrêter votre ordinateur virtuel en mode veille, nous vous recommandons de surveiller l'utilisation de son CPU pendant quelques jours. Prenez note de l'utilisation du CPU lorsque votre ordinateur virtuel est soumis à des charges différentes. Par exemple, lorsqu'il compile du code, traite une opération et tourne au ralenti. Cela vous aidera à déterminer un seuil précis pour la règle. Pour plus d'informations, veuillez consulter la section Étape 6 : (Facultatif) surveiller l'utilisation et les coûts de ce tutoriel.

Si vous créez une règle avec un seuil d'utilisation du CPU supérieur à votre charge de travail, la règle peut arrêter consécutivement votre ordinateur virtuel. Par exemple, si vous démarrez

votre ordinateur virtuel immédiatement après qu'une règle l'ait arrêté, la règle se réactive et l'ordinateur s'arrête à nouveau.

Les instructions détaillées relatives à la création et à la gestion des règles de contrôle des coûts sont disponibles dans les guides suivants :

- Gérez les règles de contrôle des coûts dans Lightsail for Research
- Créez des règles de contrôle des coûts pour vos ordinateurs virtuels Lightsail for Research
- Supprimer les règles de contrôle des coûts pour vos ordinateurs virtuels Lightsail for Research

Étape 8 : (Facultatif) créer un instantané

Les instantanés sont une point-in-time copie de vos données. Vous pouvez créer des instantanés de vos ordinateurs virtuels et les utiliser comme base de référence pour créer de nouveaux ordinateurs ou pour sauvegarder des données. Un instantané contient toutes les données nécessaires pour restaurer votre ordinateur (au moment où l'instantané a été pris).

Vous trouverez des instructions détaillées sur la création et la gestion des instantanés dans les guides suivants :

- Créez des instantanés d'ordinateurs ou de disques virtuels Lightsail for Research
- Afficher et gérer des instantanés d'ordinateurs virtuels et de disques dans Lightsail for Research
- Créer un ordinateur ou un disque virtuel à partir d'un instantané
- Supprimer un instantané dans la console Lightsail for Research

Étape 9 : (Facultatif) arrêter ou supprimer votre ordinateur virtuel

Une fois que vous avez fini avec l'ordinateur virtuel que vous avez créé dans le cadre de ce tutoriel, vous pouvez le supprimer. Cela permet de ne plus facturer de frais pour l'ordinateur virtuel si vous n'en avez pas besoin.

La suppression d'un ordinateur virtuel ne supprime pas les instantanés ou les disques attachés qui lui sont associés. Si vous avez créé des instantanés et des disques, vous devez les supprimer manuellement pour ne plus vous facturer de frais.

Pour enregistrer votre ordinateur virtuel pour plus tard, mais pour éviter de payer des frais aux prix horaires standard, vous pouvez arrêter l'ordinateur virtuel au lieu de le supprimer. Ensuite, vous pourrez le redémarrer plus tard. Pour de plus amples informations, veuillez consulter Afficher les détails de l'ordinateur virtuel Lightsail for Research. Pour plus d'informations sur les tarifs, consultez la section Tarification de Lightsail for Research.

> **Important**
>
> La suppression d'une ressource Lightsail for Research est une action permanente. Les données supprimées ne peuvent pas être récupérées. Si vous avez besoin des données ultérieurement, créez un instantané de votre ordinateur virtuel avant de le supprimer. Pour plus d'informations, consultez Création d'un instantané (français non garanti).

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, sélectionnez Ordinateurs virtuels.
3. Choisissez l'ordinateur virtuel à supprimer.
4. Choisissez Actions, puis sélectionnez Supprimer l'ordinateur virtuel.
5. Tapez confirmer dans le bloc de texte. Choisissez ensuite Supprimer l'ordinateur virtuel.

Création et gestion d'ordinateurs virtuels sur Lightsail for Research

Avec Amazon Lightsail for Research, vous pouvez créer des ordinateurs virtuels dans le. AWS Cloud

Lorsque vous créez un ordinateur virtuel, vous choisissez l'application et le plan matériel à utiliser. Vous pouvez définir une limite de dépenses pour votre ordinateur virtuel et choisir ce qui se passe lorsque l'ordinateur virtuel atteint cette limite. Par exemple, vous pouvez choisir d'arrêter automatiquement l'ordinateur virtuel afin de ne pas vous facturer plus que le budget que vous avez configuré.

> **Important**
>
> À compter du 22 mars 2024, les ordinateurs virtuels Lightsail for Research seront IMDSv2 appliqués par défaut.

Rubriques

Choisissez les images des applications et les forfaits matériels pour Lightsail for Research

Lorsque vous créez un ordinateur virtuel Amazon Lightsail for Research, vous sélectionnez une application et un plan matériel (plan) pour celui-ci.

Une application fournit une configuration logicielle (par exemple, une application et un système d'exploitation). Un plan fournit le matériel de l'ordinateur virtuel, tel que le nombre de vCPUs, la mémoire, l'espace de stockage et l'allocation mensuelle de transfert de données. Ensemble, l'application et le plan constituent la configuration de l'ordinateur virtuel.

> **Note**
>
> Vous ne pouvez pas modifier l'application ou le plan de votre ordinateur virtuel après sa création. Toutefois, vous pouvez créer un instantané de l'ordinateur virtuel, puis choisir un nouveau plan lors de la création d'un nouvel ordinateur virtuel à partir de l'instantané. Pour plus d'informations sur les instantanés, consultez Backup des ordinateurs virtuels et des disques avec des instantanés de Lightsail for Research.

Rubriques

Applications

Amazon Lightsail for Research fournit et gère des images de machine contenant l'application et le système d'exploitation nécessaires au lancement d'un ordinateur virtuel. Vous choisissez parmi une liste d'applications lorsque vous créez un ordinateur virtuel dans Lightsail for Research. Toutes les images de l'application Lightsail for Research utilisent le système d'exploitation Ubuntu (Linux).

Les applications suivantes sont disponibles dans Lightsail for Research :

- JupyterLab— JupyterLab est un environnement de développement intégré (IDE) basé sur le Web pour les ordinateurs portables, le code et les données. Grâce à son interface flexible, vous pouvez configurer et organiser des flux de travail dans les domaines de la science des données, du

calcul scientifique, du journalisme informatique et du machine learning. Pour plus d'informations, consultez la Documentation du projet Jupyter (français non garanti).

- RStudio— RStudio est un environnement de développement intégré (IDE) open source pour R, un langage de programmation pour le calcul statistique et les graphiques, et Python. Il combine un éditeur de code source, des outils d'automatisation et un débogueur, ainsi que des outils de traçage et de gestion de l'espace de travail. Pour plus d'informations, consultez l'RStudioIDE.
- VSCodium— VSCodium est une distribution binaire dirigée par la communauté de l'éditeur VS Code de Microsoft. Pour de plus amples informations, veuillez consulter VSCodium.
- Scilab : Scilab est un progiciel de calcul numérique open source et un langage de programmation numérique de haut niveau. Pour de plus d'informations, consultez Scilab (français non garanti).
- Ubuntu 20.04 LTS : Ubuntu est une distribution Linux open source basée sur Debian. Simple, rapide et puissant, Ubuntu Server fournit des services fiables, prévisibles et économiques. C'est une excellente base sur laquelle construire vos ordinateurs virtuels. Pour plus d'informations, consultez Versions Ubuntu (français non garanti).

Plans

Un plan fournit les spécifications matérielles et détermine le prix de votre ordinateur virtuel Lightsail for Research. Un plan inclut une quantité fixe de mémoire (RAM), de calcul (vCPUs), un volume de stockage (disque) sur SSD et une allocation mensuelle de transfert de données. Les plans sont facturés sur une base horaire et à la demande. Vous ne payez donc que pour le temps de fonctionnement de votre ordinateur virtuel.

Le plan que vous choisissez peut dépendre des ressources requises par votre charge de travail. Lightsail for Research propose les types de forfaits suivants :

- Standard : les plans standard sont optimisés pour les calculs et idéaux pour les applications liées aux calculs qui bénéficient de processeurs haute performance.
- GPU : les plans GPU offrent une plateforme économique à hautes performances pour le calcul GPU à usage général. Vous pouvez utiliser ces plans pour accélérer de nombreuses applications scientifiques, d'ingénierie et de rendu et des charges de travail.

Plans standard

Vous trouverez ci-dessous les spécifications matérielles des plans standard disponibles dans Lightsail for Research.

Le nom du plan	v CPUs	Mémoire	Espace de stockage	Allocation mensuelle de transfert de données
Standard XL	4	8 Go	50 Go	512 Go
Standard 2XL	8	16 Go	50 Go	512 Go
Standard 4XL	16	32 GO	50 Go	512 Go

Plans GPU

Vous trouverez ci-dessous les spécifications matérielles des forfaits GPU disponibles dans Lightsail for Research.

Le nom du plan	v CPUs	Mémoire	Espace de stockage	Allocation mensuelle de transfert de données
GPU XL	4	16 Go	50 Go	1 To
GPU 2XL	8	32 GO	50 Go	1 To
GPU 4XL	16	64 Go	50 Go	1 To

Création d'un ordinateur virtuel Lightsail for Research

Procédez comme suit pour créer un ordinateur virtuel Lightsail for Research exécutant une application.

1. Connectez-vous à la console Lightsail for Research.
2. Sur la page d'accueil, choisissez Créer un ordinateur virtuel.
3. Sélectionnez un Région AWS pour votre ordinateur virtuel situé à proximité de votre emplacement physique.

4. Choisissez un plan d'applications et de matériel. Pour de plus amples informations, veuillez consulter Choisissez les images des applications et les forfaits matériels pour Lightsail for Research.
5. Saisissez un nom pour votre ordinateur virtuel. Les caractères valables incluent les caractères alphanumériques, les chiffres, les points, les traits d'union et les traits de soulignement.

   Les noms d'ordinateurs virtuels doivent également respecter les critères suivants :

   - Soyez unique Région AWS dans chaque élément de votre compte Lightsail for Research.
   - Contiennent de 2 à 255 caractères.
   - Doivent commencer et se terminer par un caractère alphanumérique ou un chiffre.
6. Choisissez Créer un ordinateur virtuel dans le panneau Résumé.

En quelques minutes, votre ordinateur virtuel Lightsail for Research est prêt et vous pouvez vous y connecter via une session d'interface utilisateur graphique (GUI). Pour plus d'informations sur la connexion à votre ordinateur virtuel Lightsail for Research, consultez. Accédez à une application informatique virtuelle Lightsail for Research

> **Important**
>
> Les ordinateurs virtuels nouvellement créés disposent d'un ensemble de ports de pare-feu ouverts par défaut. Pour plus d'informations sur ces ports, consultez Gestion des ports de pare-feu pour les ordinateurs virtuels Lightsail for Research.

Afficher les détails de l'ordinateur virtuel Lightsail for Research

Procédez comme suit pour afficher la liste des ordinateurs virtuels et leurs informations dans votre compte Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research.
2. Choisissez Ordinateurs virtuels dans le panneau de navigation pour afficher la liste des ordinateurs virtuels de votre compte.

Choisissez un nom d'ordinateur virtuel pour accéder à sa page de gestion. Voici les informations fournies par la page de gestion :

- Nom de l'ordinateur virtuel : le nom de votre ordinateur virtuel.
- Statut : votre ordinateur virtuel peut avoir l'un des codes de statut suivants :
  - Création
  - En cours d'exécution
  - Arrêt en cours
  - Arrêté(e)
  - Je ne sais pas
- Région AWS— Région AWS Votre ordinateur virtuel a été créé dans.
- Application et matériel : le plan d'application et de matériel de l'ordinateur virtuel.
- Estimation d'utilisation mensuelle : l'utilisation horaire estimée de cet ordinateur virtuel, pour le cycle de facturation en cours.
- Estimation des coûts depuis le début du mois : le coût estimé (en USD) de l'ordinateur virtuel, pour ce cycle de facturation.
- Tableau de bord : depuis l'onglet Tableau de bord, vous pouvez lancer une session pour accéder à l'application de l'ordinateur virtuel. Vous pouvez également consulter l'utilisation du CPU. L'utilisation du CPU identifie la puissance de traitement utilisée par les applications de l'ordinateur virtuel. Chaque point de données indiqué dans le graphique représente l'utilisation moyenne du CPU sur une période donnée.
- Règles de contrôle des coûts : règles que vous définissez pour vous aider à gérer l'utilisation et les coûts de votre ordinateur virtuel.
- Utilisation de l'ordinateur virtuel : une estimation des coûts et de l'utilisation pour le cycle de facturation donné. Vous pouvez filtrer par date et heure.
- Stockage : créez, attachez et détachez des disques d'ordinateurs virtuels à partir de l'onglet Stockage. Un disque est un volume de stockage que vous pouvez attacher à un ordinateur virtuel et monter en tant que disque dur.
- Balises : gérez les balises de votre ordinateur virtuel à partir de l'onglet balises. Une étiquette est une étiquette que vous attribuez à une AWS ressource. Chaque balise est constituée d’une clé et d’une valeur facultative. Vous pouvez utiliser des balises pour rechercher et filtrer vos ressources, ou pour suivre vos AWS coûts.

Accédez à une application informatique virtuelle Lightsail for Research

Procédez comme suit pour lancer l'application qui s'exécute sur votre ordinateur virtuel Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, sélectionnez Ordinateurs virtuels.
3. Recherchez le nom de l'ordinateur virtuel à partir duquel vous souhaitez lancer l'application.

> **Note**
>
> Si l'ordinateur virtuel est arrêté, cliquez d'abord sur le bouton Démarrer l'ordinateur pour l'activer.

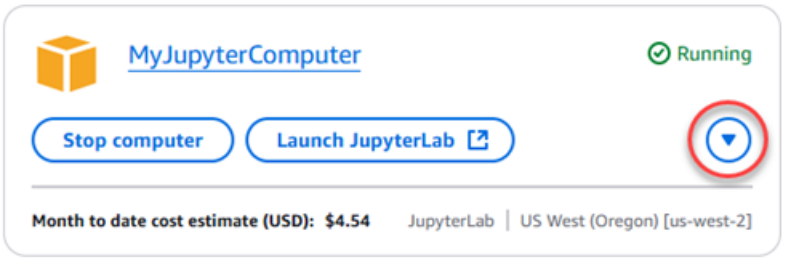
4. Choisissez Lancer l'application. Par exemple, Launch JupyterLab. Une session d'application s'ouvre dans une nouvelle fenêtre de navigateur Web.

> **Important**
>
> Si un bloqueur de fenêtres contextuelles est installé sur votre navigateur Web, vous devrez peut-être autoriser les fenêtres contextuelles provenant du domaine aws.amazon.com avant d'ouvrir votre session.

Accédez au système d'exploitation de votre ordinateur virtuel Lightsail for Research

Procédez comme suit pour accéder au système d'exploitation de votre ordinateur virtuel Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, sélectionnez Ordinateurs virtuels.
3. Recherchez le nom de votre ordinateur virtuel, puis cliquez sur le menu déroulant du bouton d'actions situé sous l'état de l'ordinateur.



> **Note**
>
> Si l'ordinateur virtuel est arrêté, cliquez d'abord sur le bouton Démarrer pour l'activer.

4. Choisissez Accéder au système d'exploitation. Une session du système d'exploitation s'ouvre dans une nouvelle fenêtre du navigateur.

> **Important**
>
> Si un bloqueur de fenêtres contextuelles est installé sur votre navigateur Web, vous devrez peut-être autoriser les fenêtres contextuelles provenant du domaine aws.amazon.com avant d'ouvrir votre session.

Gestion des ports de pare-feu pour les ordinateurs virtuels Lightsail for Research

Un pare-feu dans Amazon Lightsail for Research contrôle le trafic autorisé à se connecter à votre ordinateur virtuel. Vous ajoutez des règles au pare-feu de votre ordinateur virtuel qui spécifient le protocole, les ports, ainsi que la source IPv4 ou les IPv6 adresses autorisées à s'y connecter. Les règles de pare-feu sont toujours permissives ; vous ne pouvez pas créer de règles qui refusent l'accès. Vous ajoutez des règles au pare-feu de votre ordinateur virtuel pour autoriser le trafic à atteindre votre ordinateur virtuel. Chaque ordinateur virtuel possède deux pare-feux, l'un pour les IPv4 adresses et l'autre pour les IPv6 adresses. Les deux pare-feux sont indépendants l'un de l'autre et contiennent un ensemble préconfiguré de règles qui filtrent le trafic entrant dans l'instance.

Protocoles

Un protocole est le format dans lequel les données sont transmises entre deux ordinateurs. Vous pouvez spécifier les protocoles suivants dans une règle de pare-feu :

- Le protocole TCP (Transmission Control Protocol) est principalement utilisé pour établir et maintenir une connexion entre des clients et l'application en cours d'exécution sur votre ordinateur virtuel. Il s'agit d'un protocole largement utilisé, que vous pouvez souvent spécifier dans vos règles de pare-feu.
- Le protocole UDP (User Datagram Protocol) est principalement utilisé pour établir des connexions à faible latence et à tolérance de pertes entre les clients et l'application en cours d'exécution sur votre ordinateur virtuel. Son utilisation idéale est pour les applications de réseau dans lesquelles la latence perçue est essentielle, comme les jeux, les communications vocales et vidéo.
- Leprotocole ICMP (Internet Control Message Protocol) est principalement utilisé pour diagnostiquer les problèmes de communication réseau ; par exemple, pour déterminer si les données atteignent leur destination prévue en temps opportun. Son utilisation idéale est pour l'utilitaire Ping, que vous pouvez utiliser pour tester la vitesse de connexion entre votre ordinateur local et votre ordinateur virtuel. Il indique le temps nécessaire pour que les données atteignent votre ordinateur virtuel et reviennent sur votre ordinateur local.
- Tout est utilisé pour permettre à tout le trafic de protocole de circuler dans votre ordinateur virtuel. Spécifiez ce paramètre lorsque vous n'êtes pas sûr du protocole à spécifier. Cela inclut tous les protocoles Internet, pas seulement ceux spécifiés ici. Pour de plus amples informations, veuillez consulter les numéros des protocoles sur le site Internet de l'IANA (Internet Assigned Numbers Authority).

Ports

Comme les ports physiques de votre ordinateur, qui permettent à celui-ci de communiquer avec des périphériques comme votre clavier et votre pointeur, les ports pare-feu servent de points de terminaison de communication Internet pour votre ordinateur virtuel. Lorsqu'un client cherche à se connecter avec votre ordinateur virtuel, il expose un port pour établir la communication.

Les ports que vous pouvez spécifier dans une règle de pare-feu peuvent aller de 0 à 65535. Lorsque vous créez une règle de pare-feu pour permettre à un client d'établir une connexion avec votre ordinateur virtuel, vous spécifiez le protocole à utiliser. Vous spécifiez également les numéros de port par lesquels la connexion peut être établie et les adresses IP qui sont autorisées à établir une connexion.

Les ports suivants sont ouverts par défaut pour les ordinateurs virtuels nouvellement créés.

- TCP
  - 22 : utilisé pour Secure Shell (SSH).

- 80 : utilisé pour le protocole de transfert hypertexte (HTTP).
- 443 : utilisé pour le protocole de transfert hypertexte sécurisé (HTTPS).
- 8 443 : utilisé pour le protocole de transfert hypertexte sécurisé (HTTPS).

Pourquoi ouvrir et fermer des ports

Lorsque vous ouvrez des ports, vous autorisez un client à établir une connexion avec votre ordinateur virtuel. Lorsque vous fermez des ports, vous bloquez les connexions à votre ordinateur virtuel. Par exemple, pour autoriser un client SSH à se connecter à votre ordinateur virtuel, vous configurez une règle de pare-feu qui autorise le protocole TCP sur le port 22 uniquement à partir de l'adresse IP de l'ordinateur qui doit établir une connexion. Dans ce cas, vous ne souhaitez autoriser aucune adresse IP à établir une connexion SSH avec votre ordinateur virtuel. Cela pourrait entraîner un risque de sécurité. Si cette règle est déjà configurée sur le pare-feu de votre instance, vous pouvez la supprimer pour empêcher le client SSH de se connecter à votre ordinateur virtuel.

Les procédures suivantes vous montrent comment obtenir les ports actuellement ouverts sur votre ordinateur virtuel, ouvrir de nouveaux ports et fermer des ports.

Rubriques

Remplir les conditions préalables

Remplissez les conditions préalables suivantes avant de démarrer.

- Créez un ordinateur virtuel dans Lightsail for Research. Pour de plus amples informations, veuillez consulter Création d'un ordinateur virtuel Lightsail for Research.
- Téléchargez et installez le AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente d' AWS CLI (français non garanti) dans le Guide de l'utilisateur AWS Command Line Interface pour la version 2.

- Configurez le AWS CLI pour accéder à votre Compte AWS. Pour plus d'informations, consultez Principes de base de la configuration (français non garanti) dans le Guide de l'utilisateur AWS Command Line Interface pour la version 2.

Obtenir l'état des ports d'un ordinateur virtuel

Suivez la procédure ci-dessous pour obtenir l'état du port d'un ordinateur virtuel. Cette procédure utilise la `get-instance-port-states` AWS CLI commande pour obtenir l'état des ports de pare-feu d'un ordinateur virtuel Lightsail for Research spécifique, les adresses IP autorisées à se connecter à l'ordinateur virtuel via les ports et le protocole. Pour plus d'informations, consultez get-instance-port-states dans la Référence des commandes de l'AWS CLI .

1. Cette étape dépend du système d'exploitation de votre ordinateur local.

   - Si votre ordinateur local utilise un système d'exploitation Windows, ouvrez une fenêtre d'invite de commande.
   - Si votre ordinateur local utilise un système d'exploitation basé sur Linux ou Unix (y compris macOS), ouvrez une fenêtre de terminal.

2. Saisissez la commande suivante pour obtenir les états des ports du pare-feu ainsi que les adresses IP et les protocoles autorisés. Dans la commande, remplacez *REGION* par le code de la région AWS dans laquelle l'ordinateur virtuel a été créé, tel que `us-east-2`. Remplacez *NAME* par le nom de votre ordinateur virtuel.

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

   Exemple

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

   La réponse affichera les ports et protocoles ouverts, ainsi que les plages d'adresses IP au format CIDR autorisées à se connecter à votre ordinateur virtuel.

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

Pour plus d'informations sur l'ouverture des ports, passez à la section suivante.

Ouvrir des ports pour un ordinateur virtuel

Suivez la procédure suivante pour ouvrir les ports d'un ordinateur virtuel. Cette procédure utilise la `open-instance-public-ports` AWS CLI commande. Ouvrez des ports de pare-feu pour permettre l'établissement de connexions à partir d'une adresse IP fiable ou d'une plage d'adresses IP. Par exemple, pour autoriser l'adresse IP `192.0.2.44`, spécifiez `192.0.2.44` ou `192.0.2.44/32`. Pour autoriser les adresses IP `192.0.2.0` à `192.0.2.255`, spécifiez `192.0.2.0/24`. Pour plus d'informations, consultez open-instance-public-ports dans la Référence des commandes de l'AWS CLI .

1. Cette étape dépend du système d'exploitation de votre ordinateur local.

   - Si votre ordinateur local utilise un système d'exploitation Windows, ouvrez une fenêtre d'invite de commande.
   - Si votre ordinateur local utilise un système d'exploitation basé sur Linux ou Unix (y compris macOS), ouvrez une fenêtre de terminal.

2. Saisissez la commande suivante pour ouvrir les ports.

   Dans la commande, remplacer les éléments suivants :

   - *`REGION`*Remplacez-le par le code de la AWS région dans laquelle l'ordinateur virtuel a été créé, tel que`us-east-2`.
   - Remplacez *`NAME`* par le nom de votre ordinateur virtuel.
   - Remplacez *`FROM-PORT`* par le premier port d'une série de ports que vous souhaitez ouvrir.
   - Remplacez *`PROTOCOL`* par le nom du protocole IP. Par exemple, TCP.
   - Remplacez *`TO-PORT`* par le dernier port d'une série de ports que vous souhaitez ouvrir.

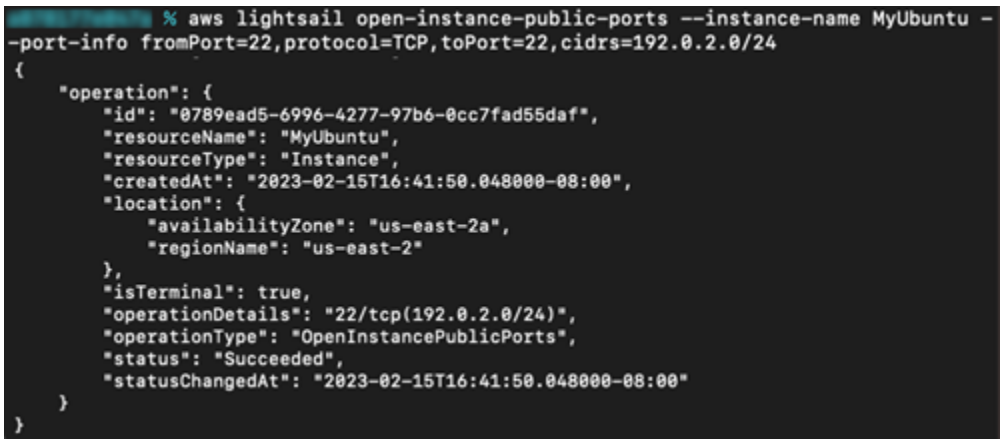
- Remplacez *IP* par l'adresse IP ou la plage d'adresses IP que vous souhaitez autoriser à vous connecter à votre ordinateur virtuel.

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

Exemple

```
aws lightsail open-instance-public-ports --region us-east-2 --instance-
name MyUbuntu --port-info fromPort=22, protocol=TCP, toPort=22,cidrs=192.0.2.0/24
```

La réponse affichera les ports, protocoles et plages d'adresses IP sur le format CIDR récemment ajoutés qui sont autorisés à se connecter à votre ordinateur virtuel.



Pour plus d'informations sur la fermeture des ports, passez à la section suivante.

Fermer les ports d'un ordinateur virtuel

Suivez la procédure suivante pour fermer les ports d'un ordinateur virtuel. Cette procédure utilise la `close-instance-public-ports` AWS CLI commande. Pour plus d'informations, consultez close-instance-public-ports dans la Référence des commandes de l'AWS CLI .

1. Cette étape dépend du système d'exploitation de votre ordinateur local.

   - Si votre ordinateur local utilise un système d'exploitation Windows, ouvrez une fenêtre d'invite de commande.

- Si votre ordinateur local utilise un système d'exploitation basé sur Linux ou Unix (y compris macOS), ouvrez une fenêtre de terminal.

2. Saisissez la commande suivante pour fermer les ports.

   Dans la commande, remplacer les éléments suivants :

   - *REGION*Remplacez-le par le code de la AWS région dans laquelle l'ordinateur virtuel a été créé, tel que`us-east-2`.
   - Remplacez *NAME* par le nom de votre ordinateur virtuel.
   - Remplacez *FROM-PORT* par le premier port d'une série de ports que vous souhaitez fermer.
   - Remplacez *PROTOCOL* par le nom du protocole IP. Par exemple, TCP.
   - Remplacez *TO-PORT* par le dernier port d'une série de ports que vous souhaitez fermer.
   - Remplacez *IP* par l'adresse IP ou la plage d'adresses IP que vous souhaitez supprimer.

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

   Exemple

   ```
   aws lightsail close-instance-public-ports --region us-east-2 --instance-
   name MyUbuntu --port-info fromPort=22, protocol=TCP, toPort=22,cidrs=192.0.2.0/24
   ```

   La réponse affichera les ports, les protocoles et les plages d'adresses IP sur format CIDR qui ont été fermés et ne sont plus autorisés à se connecter à votre ordinateur virtuel.

Passer aux étapes suivantes

Vous pouvez effectuer les étapes supplémentaires suivantes après avoir géré avec succès les ports de pare-feu de votre ordinateur virtuel :

- Obtenez la paire de clés de votre ordinateur virtuel. Avec la paire de clés, vous pouvez établir une connexion à l'aide de nombreux clients SSH, tels qu'OpenSSH, PuTTY et Windows Subsystem for Linux. Pour de plus amples informations, veuillez consulter Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research.
- Connectez-vous à votre ordinateur virtuel via SSH pour le gérer à l'aide de la ligne de commande. Pour de plus amples informations, veuillez consulter Transférez des fichiers vers des ordinateurs virtuels Lightsail for Research à l'aide de Secure Copy.
- Connectez-vous à votre ordinateur virtuel à l'aide de SCP pour transférer des fichiers en toute sécurité. Pour de plus amples informations, veuillez consulter Transférez des fichiers vers des ordinateurs virtuels Lightsail for Research à l'aide de Secure Copy.

Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research

Une paire de clés, composée d'une clé publique et d'une clé privée, est un ensemble d'informations de sécurité que vous utilisez pour prouver votre identité lorsque vous vous connectez à un ordinateur virtuel Amazon Lightsail for Research. La clé publique est stockée sur chaque ordinateur virtuel dans Lightsail for Research, et vous conservez la clé privée sur votre ordinateur local. La clé privée vous permet d'établir en toute sécurité un protocole Secure Shell (SSH) avec votre ordinateur virtuel. Toute personne détentrice de votre clé privée peut se connecter à votre ordinateur virtuel, il est donc important que vous stockiez celle-ci en lieu sûr.

Une paire de clés par défaut (DKP) Amazon Lightsail est automatiquement créée la première fois que vous créez une instance Lightsail ou un ordinateur virtuel Lightsail for Research. Le DKP est spécifique à chaque AWS région dans laquelle vous créez une instance ou un ordinateur virtuel. Par exemple, le DKP Lightsail pour la région USA Est (Ohio) (us-east-2) s'applique à tous les ordinateurs que vous créez dans l'est des États-Unis (Ohio) dans Lightsail et Lightsail for Research qui ont été configurés pour utiliser le DKP lors de leur création. Lightsail for Research stocke automatiquement la clé publique du DKP sur les ordinateurs virtuels que vous créez. Vous pouvez télécharger la clé privée du DKP à tout moment en appelant le service Lightsail via l'API.

Dans ce document, nous vous expliquons comment obtenir la DKP pour un ordinateur virtuel. Une fois que vous avez la DKP, vous pouvez établir une connexion à l'aide de nombreux clients SSH, tels qu'OpenSSH, PuTTY et Windows Subsystem for Linux. Vous pouvez également utiliser Secure Copy (SCP) pour transférer en toute sécurité des fichiers de votre ordinateur local vers votre ordinateur virtuel.

> **Note**
>
> Vous pouvez également établir une connexion au protocole d'affichage à distance avec votre ordinateur virtuel à l'aide du client Amazon DCV basé sur un navigateur. Amazon DCV est disponible dans la console Lightsail for Research. Ce client RDP ne nécessite pas que vous obteniez une paire de clés pour votre ordinateur. Pour plus d'informations, consultez Accédez à une application informatique virtuelle Lightsail for Research et Accédez au système d'exploitation de votre ordinateur virtuel Lightsail for Research.

Rubriques

Remplir les conditions préalables

Remplissez les conditions préalables suivantes avant de démarrer.

- Créez un ordinateur virtuel dans Lightsail for Research. Pour de plus amples informations, veuillez consulter Création d'un ordinateur virtuel Lightsail for Research.
- Téléchargez et installez le AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente d' AWS CLI (français non garanti) dans le Guide de l'utilisateur AWS Command Line Interface pour la version 2.
- Configurez le AWS CLI pour accéder à votre Compte AWS. Pour plus d'informations, consultez Principes de base de la configuration (français non garanti) dans le Guide de l'utilisateur AWS Command Line Interface pour la version 2.
- Téléchargez et installez jq. Il s'agit d'un processeur JSON en ligne de commande léger et flexible utilisé dans les procédures suivantes pour extraire les détails des paires de clés à partir des sorties

JSON d' AWS CLI. Pour plus d'informations sur le téléchargement et l'installation de jq, consultez la section Télécharger jq (français non garanti) sur le site Web de jq.

Obtenir une paire de clés pour un ordinateur virtuel

Effectuez l'une des procédures suivantes pour obtenir le Lightsail DKP pour un ordinateur virtuel dans Lightsail for Research.

Obtenir une paire de clés pour un ordinateur virtuel à l'aide d'un ordinateur local Windows

Cette procédure s'applique à vous si votre ordinateur local utilise un système d'exploitation Windows. Cette procédure utilise la `download-default-key-pair` AWS CLI commande pour obtenir le DKP Lightsail pour une région. AWS Pour plus d'informations, consultez download-default-key-pair dans la Référence des commandes de l'AWS CLI .

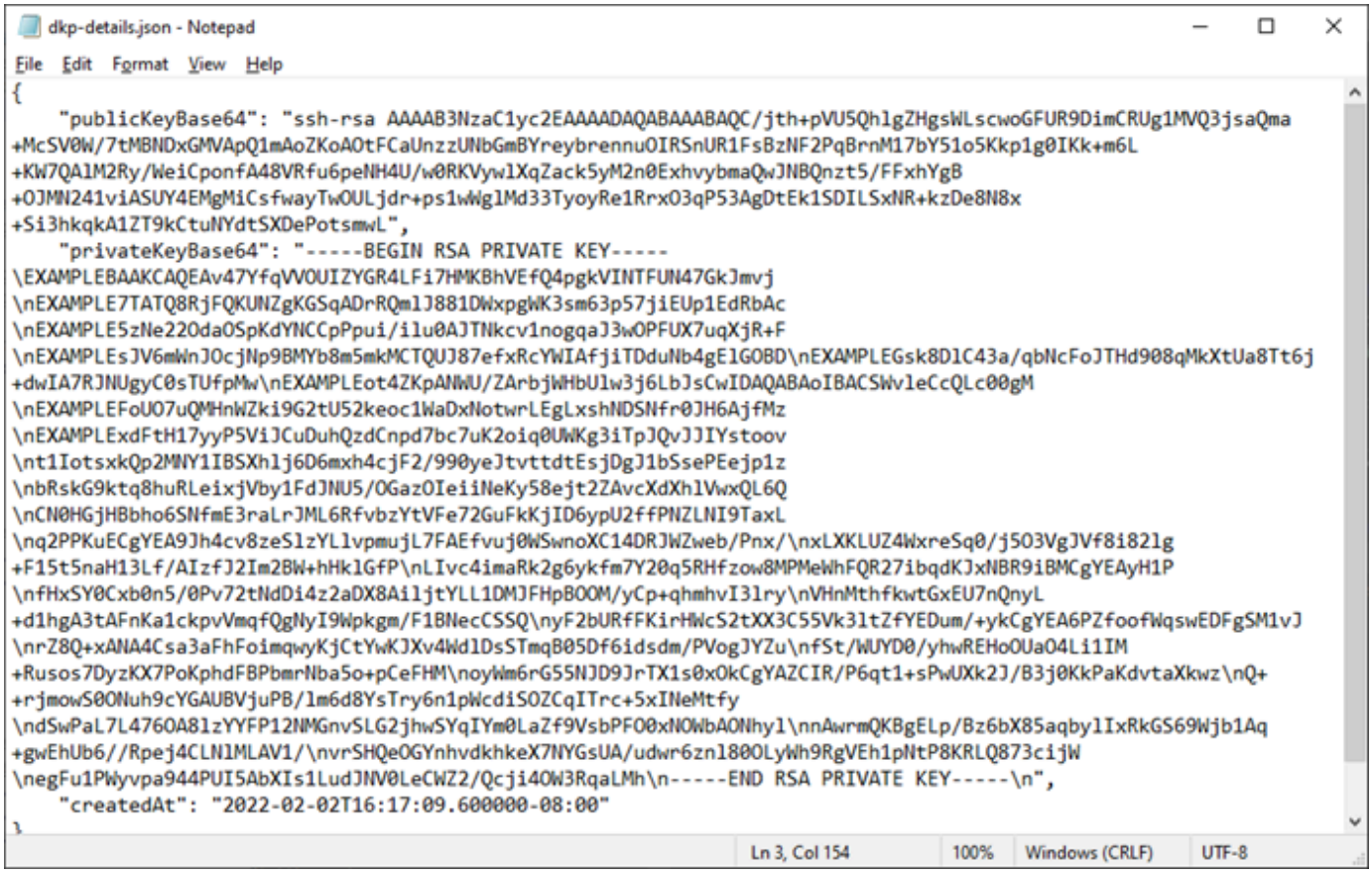
1. Ouvrez une fenêtre d'invite de commande.
2. Entrez la commande suivante pour obtenir le DKP Lightsail pour une région spécifique. AWS Cette commande enregistre les informations dans un fichier `dkp-details.json`. Dans la commande, remplacez *`region-code`* par le code de la AWS région dans laquelle l'ordinateur virtuel a été créé, tel que`us-east-2`.

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

   Exemple

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

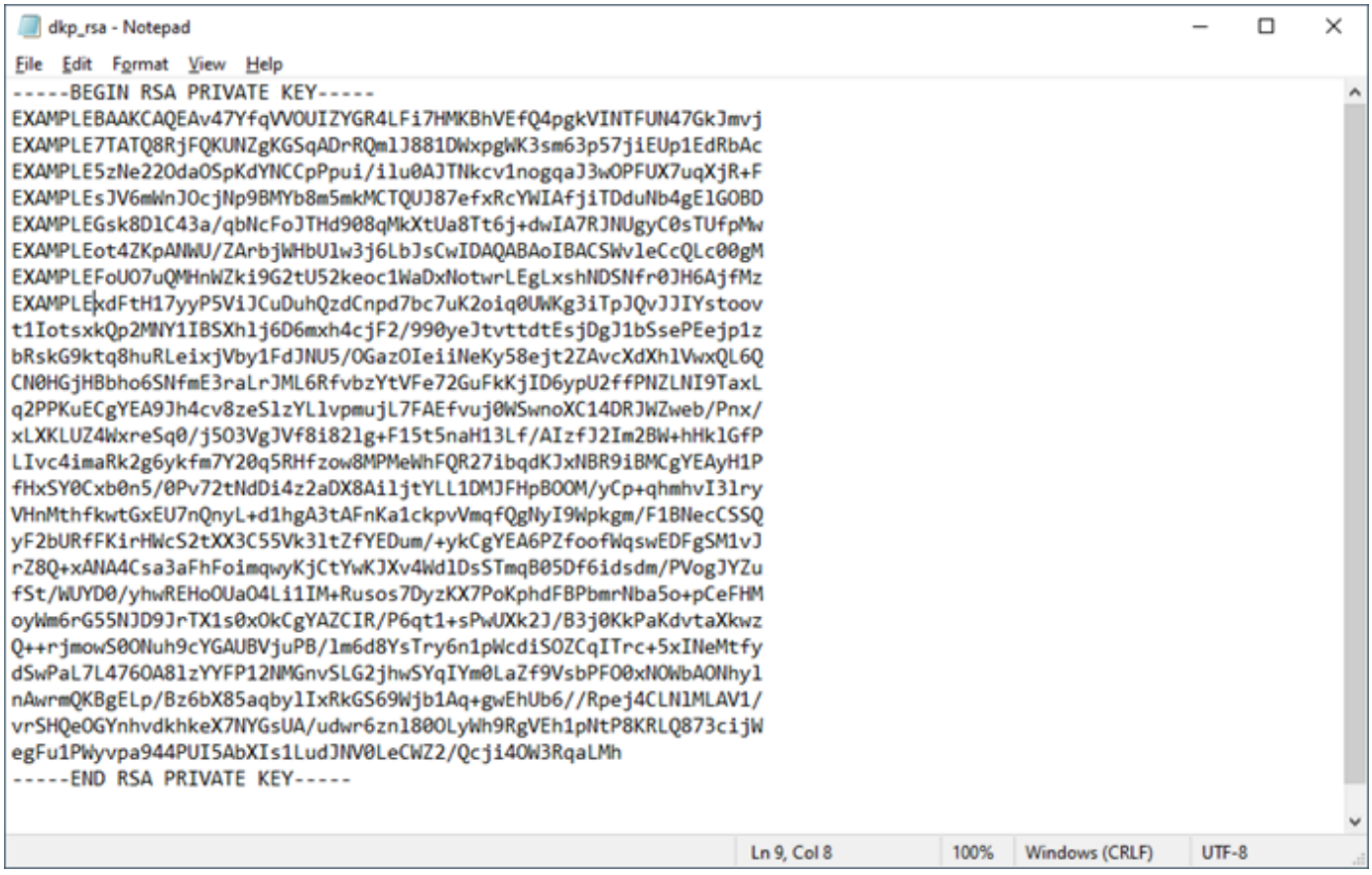
   Il n'y a aucune réponse à la commande. Vous pouvez confirmer le succès de la commande en ouvrant le `dkp-details.json` fichier et en vérifiant si les informations DKP de Lightsail ont été enregistrées. Le contenu du fichier `dkp-details.json` peut ressembler à l'exemple suivant. La commande a échoué si le fichier est vide.



3. Saisissez la commande suivante pour extraire les informations de clé privée du fichier `dkp-details.json` et les ajouter à un nouveau fichier de clé privée `dkp_rsa`.

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

Il n'y a aucune réponse à la commande. Vous pouvez confirmer le succès de la commande en ouvrant les fichiers `dkp_rsa` et en vérifiant s'ils contiennent des informations. Le contenu du fichier `dkp_rsa` peut ressembler à l'exemple suivant. La commande a échoué si le fichier est vide.



Vous disposez désormais de la clé privée requise pour établir une connexion SSH ou SCP avec votre ordinateur virtuel. Passez à la section suivante pour les prochaines étapes supplémentaires.

Obtenir une paire de clés pour un ordinateur virtuel utilisant un ordinateur local Linux, Unix ou macOS

Cette procédure s'applique à vous si votre ordinateur local utilise un système d'exploitation Linux, Unix ou macOS. Cette procédure utilise la `download-default-key-pair` AWS CLI commande pour obtenir le DKP Lightsail pour une région. AWS Pour plus d'informations, consultez download-default-key-pair dans la Référence des commandes de l'AWS CLI .

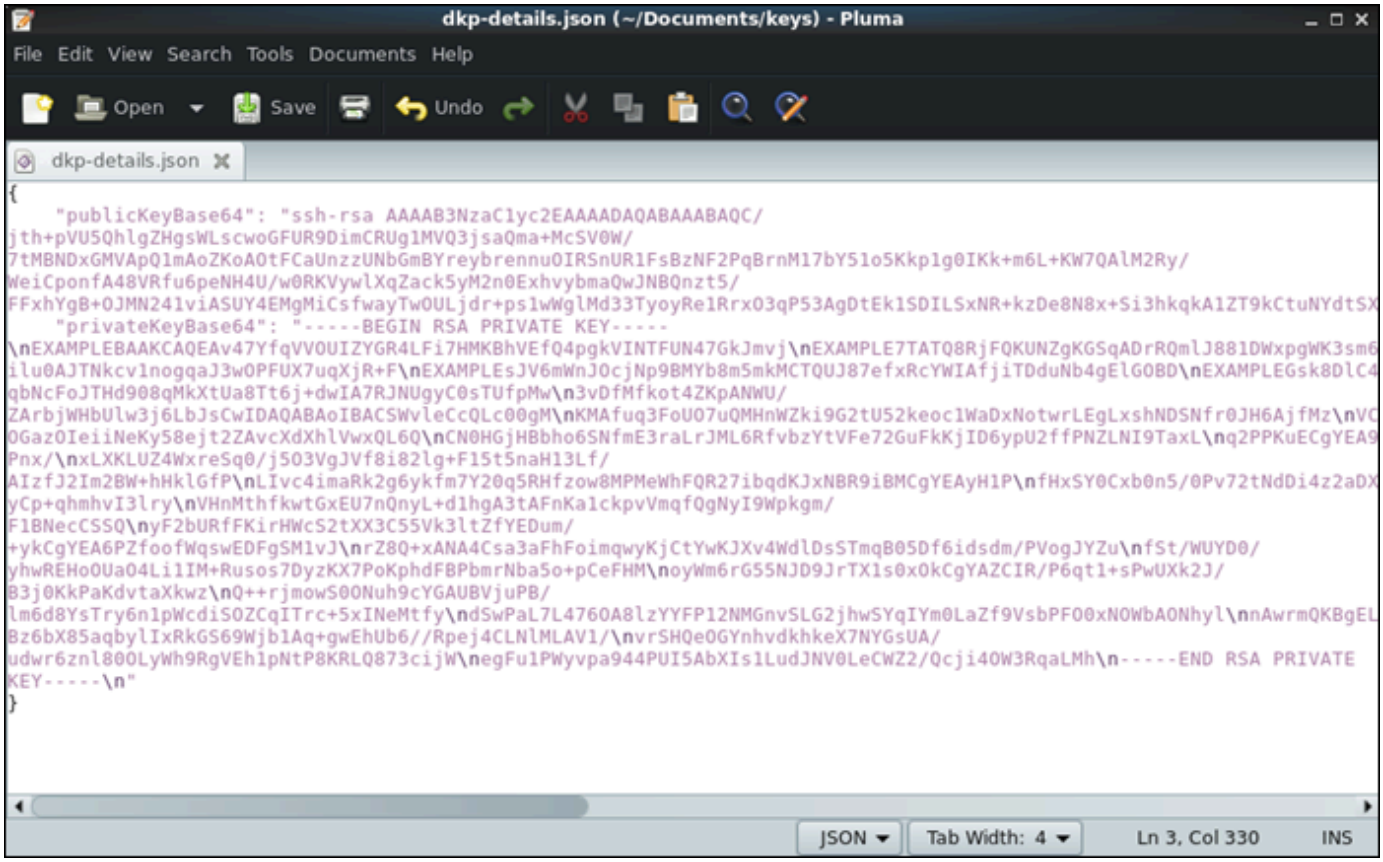
1. Ouvrez une fenêtre de terminal.
2. Entrez la commande suivante pour obtenir le DKP Lightsail pour une région spécifique. AWS Cette commande enregistre les informations dans un fichier `dkp-details.json`. Dans la commande, remplacez *`region-code`* par le code de la AWS région dans laquelle l'ordinateur virtuel a été créé, tel que`us-east-2`.

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

Exemple

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

Il n'y a aucune réponse à la commande. Vous pouvez confirmer le succès de la commande en ouvrant le `dkp-details.json` fichier et en vérifiant si les informations DKP de Lightsail ont été enregistrées. Le contenu du fichier `dkp-details.json` peut ressembler à l'exemple suivant. La commande a échoué si le fichier est vide.

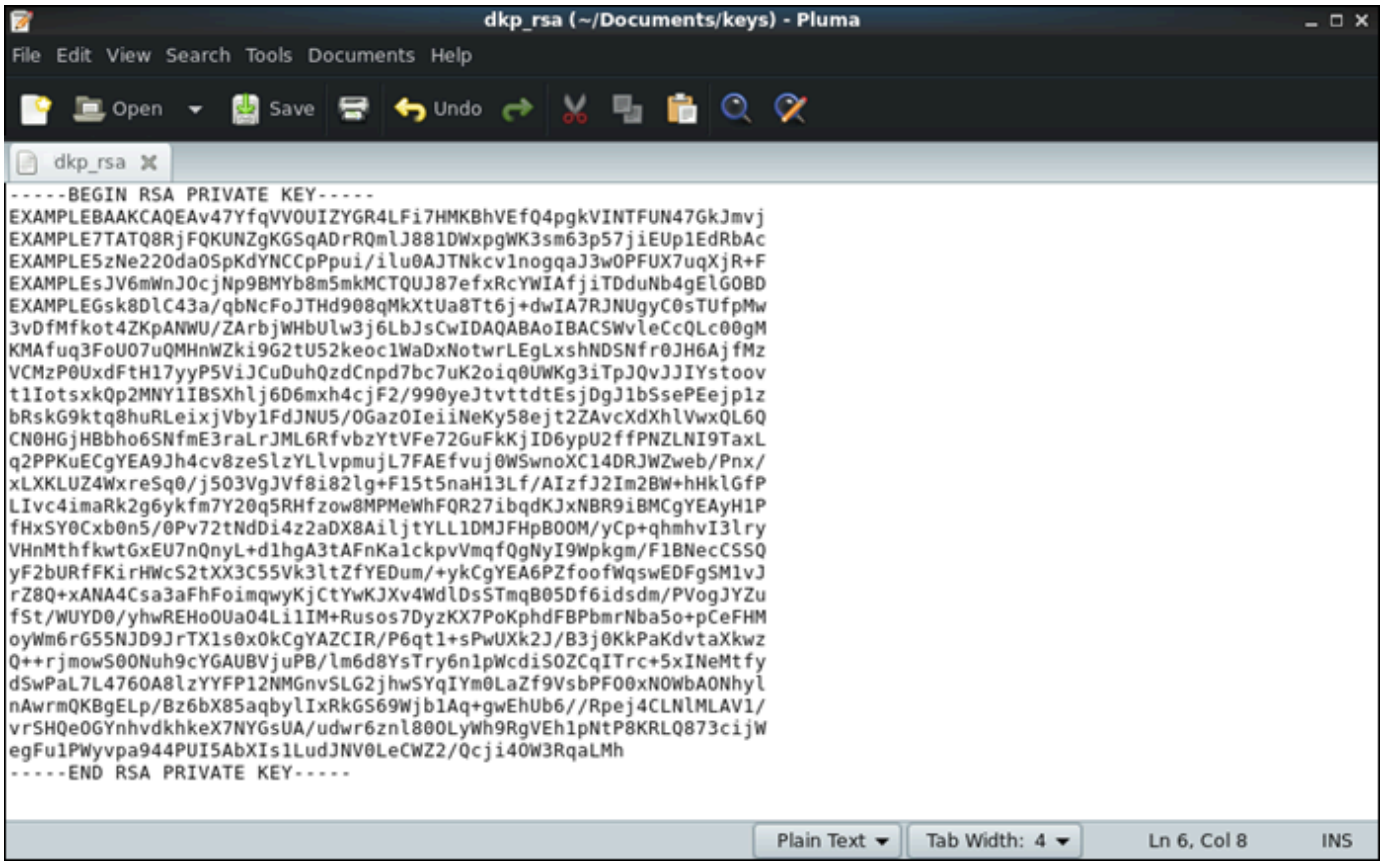


3. Saisissez la commande suivante pour extraire les informations de clé privée du fichier `dkp-details.json` et les ajouter à un nouveau fichier de clé privée `dkp_rsa`.

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

Il n'y a aucune réponse à la commande. Vous pouvez confirmer le succès de la commande en ouvrant les fichiers `dkp_rsa` et en vérifiant s'ils contiennent des informations. Le contenu du

fichier `dkp_rsa` peut ressembler à l'exemple suivant. La commande a échoué si le fichier est vide.



4. Saisissez la commande suivante pour définir les autorisations du fichier `dkp_rsa`.

```
chmod 600 dkp_rsa
```

Vous disposez désormais de la clé privée requise pour établir une connexion SSH ou SCP avec votre ordinateur virtuel. Passez à la section suivante pour les prochaines étapes supplémentaires.

Passer aux étapes suivantes

Vous pouvez effectuer les étapes supplémentaires suivantes après avoir obtenu avec succès les paires de clés pour votre ordinateur virtuel :

- Connectez-vous à votre ordinateur virtuel via SSH pour le gérer à l'aide de la ligne de commande. Pour de plus amples informations, veuillez consulter Connectez-vous à un ordinateur virtuel Lightsail for Research à l'aide de Secure Shell.

- Connectez-vous à votre ordinateur virtuel à l'aide de SCP pour transférer des fichiers en toute sécurité. Pour de plus amples informations, veuillez consulter Transférez des fichiers vers des ordinateurs virtuels Lightsail for Research à l'aide de Secure Copy.

Connectez-vous à un ordinateur virtuel Lightsail for Research à l'aide de Secure Shell

Vous pouvez vous connecter à un ordinateur virtuel dans Amazon Lightsail for Research à l'aide du protocole Secure Shell (SSH). Vous pouvez utiliser SSH pour gérer votre ordinateur virtuel à distance afin de pouvoir vous connecter à votre ordinateur via Internet et exécuter des commandes.

> **Note**
>
> Vous pouvez également établir une connexion au protocole d'affichage à distance avec votre ordinateur virtuel à l'aide du client Amazon DCV basé sur un navigateur. Amazon DCV est disponible dans la console Lightsail for Research. Pour de plus amples informations, veuillez consulter Accédez au système d'exploitation de votre ordinateur virtuel Lightsail for Research.

Rubriques

Remplir les conditions préalables

Remplissez les conditions préalables suivantes avant de démarrer.

- Créez un ordinateur virtuel dans Lightsail for Research. Pour de plus amples informations, veuillez consulter Création d'un ordinateur virtuel Lightsail for Research.
- Assurez-vous que l'ordinateur virtuel auquel vous souhaitez vous connecter fonctionne. Notez également le nom de l'ordinateur virtuel et la AWS région dans laquelle il a été créé. Vous aurez besoin de ces informations plus tard dans le processus. Pour de plus amples informations, veuillez consulter Afficher les détails de l'ordinateur virtuel Lightsail for Research.

- Assurez-vous que le port 22 est ouvert sur l'ordinateur virtuel auquel vous souhaitez vous connecter. Il s'agit du port par défaut utilisé pour SSH. Il est ouvert par défaut. Mais si vous l'avez fermé, vous devez le rouvrir avant de continuer. Pour de plus amples informations, veuillez consulter Gestion des ports de pare-feu pour les ordinateurs virtuels Lightsail for Research.
- Obtenez la paire de clés par défaut (DKP) Lightsail pour votre ordinateur virtuel. Pour de plus amples informations, veuillez consulter Obtenir une paire de clés pour un ordinateur virtuel.

> **Tip**
>
> Si vous prévoyez de l'utiliser AWS CloudShell pour vous connecter à votre ordinateur virtuel, reportez-vous Connectez-vous à un ordinateur virtuel à l'aide de AWS CloudShell à la section suivante. Pour plus d'informations, consultez Qu'est-ce qu'AWS CloudShell ? Sinon, passez au prérequis suivant.

- Téléchargez et installez le AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente d' AWS CLI (français non garanti) dans le Guide de l'utilisateur AWS Command Line Interface pour la version 2.
- Configurez le AWS CLI pour accéder à votre Compte AWS. Pour plus d'informations, consultez Principes de base de la configuration (français non garanti) dans le Guide de l'utilisateur AWS Command Line Interface pour la version 2.
- Téléchargez et installez jq. Il s'agit d'un processeur JSON en ligne de commande, léger et flexible, utilisé dans les procédures suivantes pour extraire les détails des paires de clés. Pour plus d'informations sur le téléchargement et l'installation de jq, consultez la section Télécharger jq (français non garanti) sur le site Web de jq.

Connexion à un ordinateur virtuel à l'aide de SSH

Effectuez l'une des procédures suivantes pour établir une connexion SSH à votre ordinateur virtuel dans Lightsail for Research.

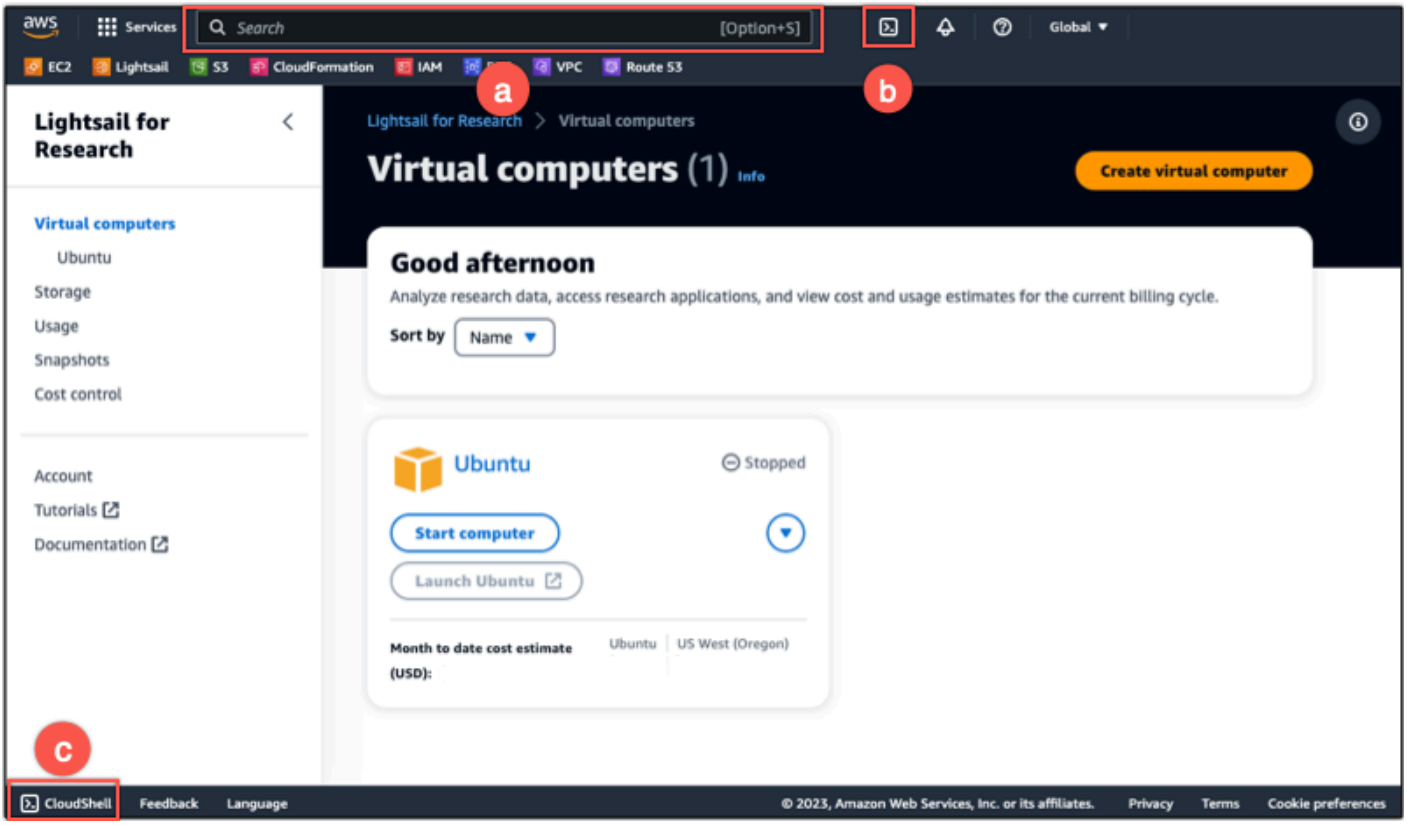
Connectez-vous à un ordinateur virtuel à l'aide de AWS CloudShell

Cette procédure s'applique si vous préférez une configuration minimale pour vous connecter à votre ordinateur virtuel. AWS CloudShell utilise un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Vous pouvez exécuter AWS CLI des commandes à l'aide de votre shell préféré PowerShell, tel que Bash ou Z. Vous pouvez le faire

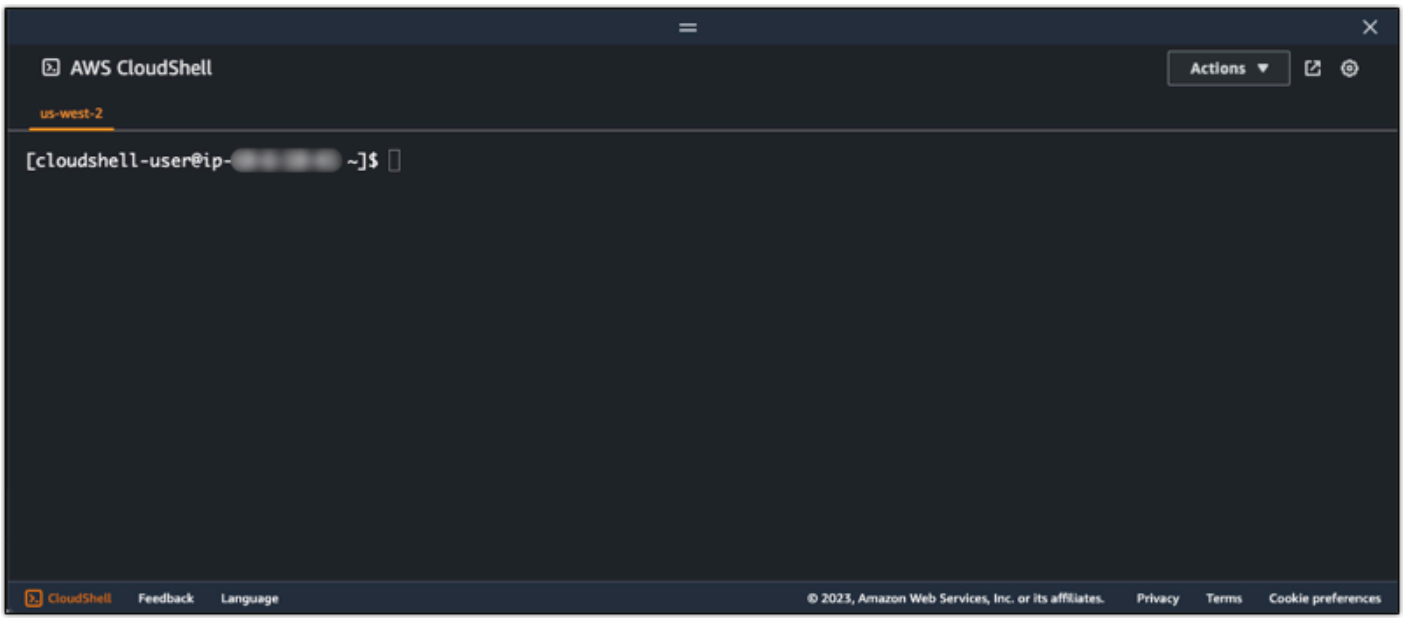
sans télécharger ou installer des outils de ligne de commande. Pour plus d'informations, consultez Démarrer avec AWS CloudShell dans le Guide de l'utilisateur AWS CloudShell .

> **Important**
>
> Avant de commencer, assurez-vous d'obtenir la paire de clés par défaut (DKP) Lightsail pour l'ordinateur virtuel auquel vous vous connectez. Pour de plus amples informations, veuillez consulter Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research.

1. Depuis la console Lightsail for Research, CloudShell lancez-le en choisissant l'une des options suivantes :
   a. Dans la zone de recherche, tapez CloudShell « », puis choisissez CloudShell.
   b. Dans la barre de navigation, choisissez l'CloudShellicône.
   c. Choisissez dans CloudShellla barre d'outils de la console en bas à gauche de la console.



Lorsque l'invite de commandes s'affiche, le shell est prêt pour l'interaction.



2. Choisissez un shell préinstallé avec lequel travailler. Pour modifier le shell par défaut, entrez l'un des noms de programme suivants à l'invite de la ligne de commande. Bash est le shell par défaut qui s'exécute lors du lancement AWS CloudShell.

   Bash

   ```
   bash
   ```

   Si vous passez à Bash, le symbole affiché à l'invite de commande prend la valeur$.

   PowerShell

   ```
   pwsh
   ```

   Si vous passez à PowerShell, le symbole affiché à l'invite de commande prend la valeurPS>.

   Z shell

   ```
   zsh
   ```

   Si vous passez à Z shell, le symbole affiché à l'invite de commande prend la valeur%.

3. Pour vous connecter à un ordinateur virtuel depuis la fenêtre du CloudShell terminal, reportez-vous àConnexion à un ordinateur virtuel à l'aide de SSH sur un ordinateur local Linux, Unix ou macOS.

Pour plus d'informations sur le logiciel préinstallé dans l' CloudShellenvironnement, voir environnement de AWS CloudShell calcul dans le guide de l'AWS CloudShell utilisateur.

Connexion à un ordinateur virtuel à l'aide de SSH sur un ordinateur local Windows

Cette procédure s'applique si votre ordinateur local utilise un système d'exploitation Windows. Cette procédure utilise la `get-instance` AWS CLI commande pour obtenir le nom d'utilisateur et l'adresse IP publique de l'instance à laquelle vous souhaitez vous connecter. Pour plus d'informations, consultez get-instance (français non garanti) dans la Référence des commandes AWS CLI .

> **Important**
>
> Assurez-vous d'obtenir la paire de clés par défaut (DKP) Lightsail pour l'ordinateur virtuel auquel vous essayez de vous connecter avant de commencer cette procédure. Pour de plus amples informations, veuillez consulter Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research. Cette procédure génère la clé privée du Lightsail DKP dans `dkp_rsa` un fichier utilisé dans l'une des commandes suivantes.

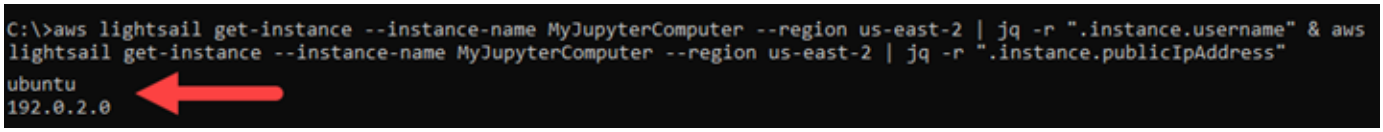
1. Ouvrez une fenêtre d'invite de commande.
2. Saisissez la commande suivante pour afficher l'adresse IP publique et le nom d'utilisateur de votre ordinateur virtuel. Dans la commande, remplacez *`region-code`* par le code Région AWS dans lequel l'ordinateur virtuel a été créé, tel que`us-east-2`. Remplacez *`computer-name`* par le nom de l'ordinateur virtuel auquel vous souhaitez vous connecter.

   ```
   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"
   ```

   Exemple

   ```
   aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
    | jq -r ".instance.username" & aws lightsail get-instance --region us-east-2 --
   instance-name MyJupyterComputer | jq -r ".instance.publicIpAddress"
   ```

   La réponse affichera le nom d'utilisateur et l'adresse IP publique de l'ordinateur virtuel, comme illustré dans l'exemple suivant. Notez ces valeurs, car vous en aurez besoin à l'étape suivante de cette procédure.



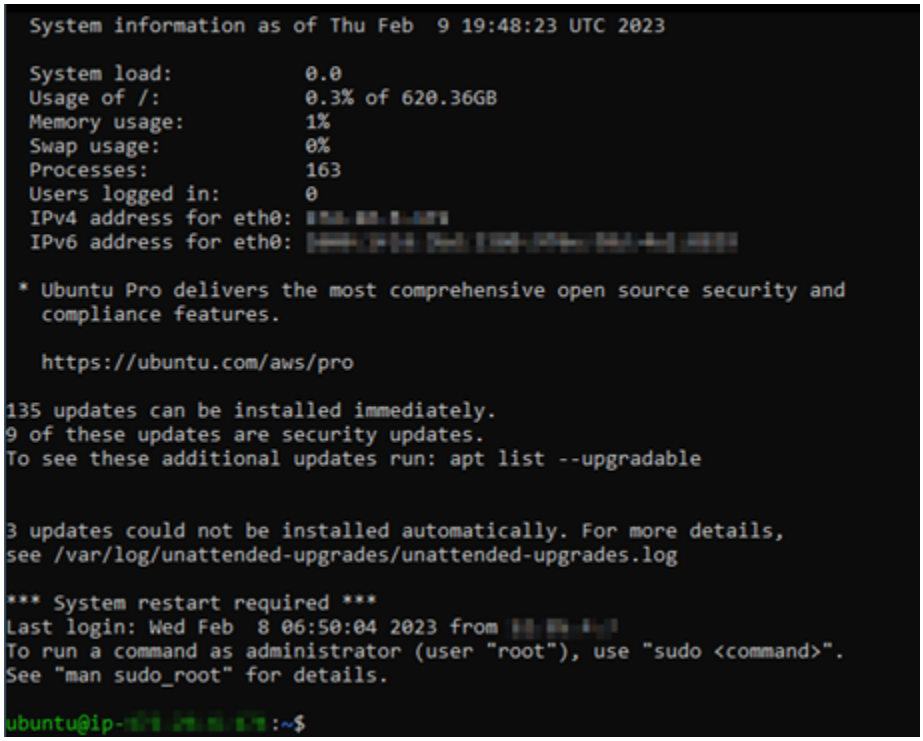
3. Saisissez la commande suivante pour établir une connexion SSH avec votre ordinateur virtuel. Dans la commande, remplacez *user-name* par le nom d'utilisateur de connexion et remplacez *public-ip-address* par l'adresse IP publique de votre ordinateur virtuel.

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

Exemple

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

Vous devriez voir une réponse similaire à l'exemple suivant, qui montre une connexion SSH établie avec un ordinateur virtuel Ubuntu dans Lightsail for Research.



Maintenant que vous avez réussi à établir une connexion SSH à votre ordinateur virtuel, passez à la section suivante pour les étapes supplémentaires suivantes.

Connexion à un ordinateur virtuel à l'aide de SSH sur un ordinateur local Linux, Unix ou macOS

Cette procédure s'applique si votre ordinateur local utilise un système d'exploitation Linux, Unix ou macOS. Cette procédure utilise la `get-instance` AWS CLI commande pour obtenir le nom d'utilisateur et l'adresse IP publique de l'instance à laquelle vous souhaitez vous connecter. Pour plus d'informations, consultez get-instance (français non garanti) dans la Référence des commandes AWS CLI .

> **Important**
>
> Assurez-vous d'obtenir la paire de clés par défaut (DKP) Lightsail pour l'ordinateur virtuel auquel vous essayez de vous connecter avant de commencer cette procédure. Pour de plus amples informations, veuillez consulter Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research. Cette procédure génère la clé privée du Lightsail DKP dans `dkp_rsa` un fichier utilisé dans l'une des commandes suivantes.

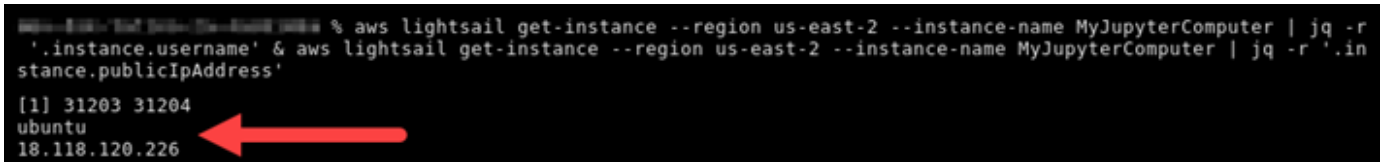
1. Ouvrez une fenêtre de terminal.
2. Saisissez la commande suivante pour afficher l'adresse IP publique et le nom d'utilisateur de votre ordinateur virtuel. Dans la commande, remplacez *`region-code`* par le code de la AWS région dans laquelle l'ordinateur virtuel a été créé, tel que`us-east-2`. Remplacez *`computer-name`* par le nom de l'ordinateur virtuel auquel vous souhaitez vous connecter.

   ```
   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'
   ```

   Exemple

   ```
   aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
    | jq -r '.instance.username' && aws lightsail get-instance --region us-east-2 --
   instance-name MyJupyterComputer | jq -r '.instance.publicIpAddress'
   ```

   La réponse affichera le nom d'utilisateur et l'adresse IP publique de l'ordinateur virtuel, comme illustré dans l'exemple suivant. Notez ces valeurs, car vous en aurez besoin à l'étape suivante de cette procédure.



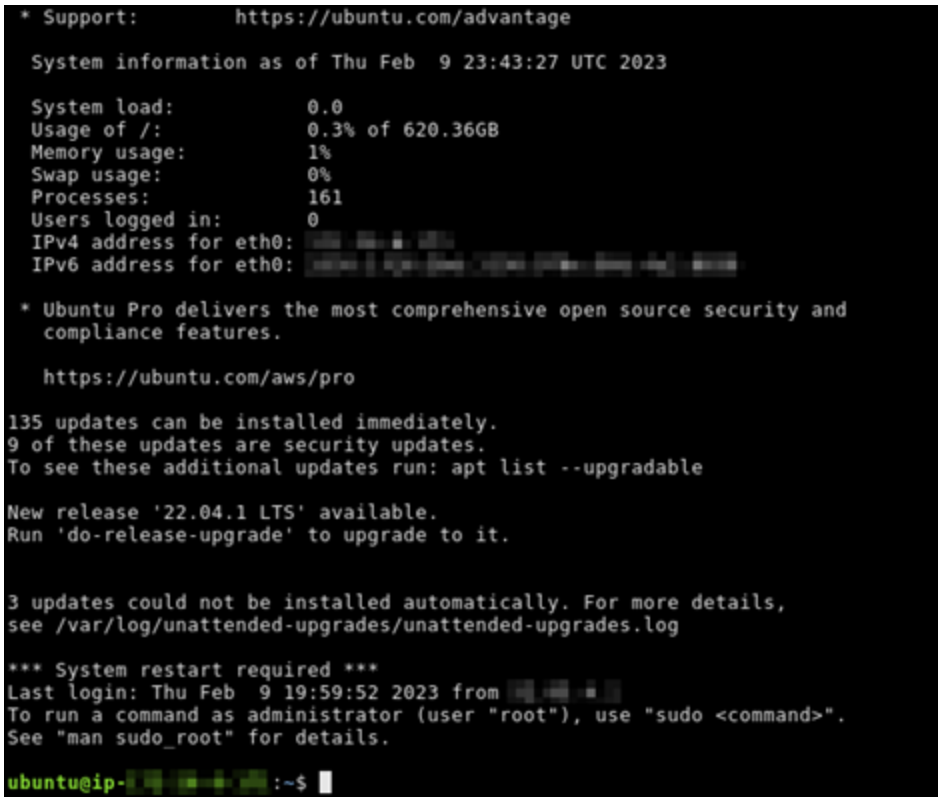
3. Saisissez la commande suivante pour établir une connexion SSH avec votre ordinateur virtuel. Dans la commande, remplacez *user-name* par le nom d'utilisateur de connexion, puis *public-ip-address* par l'adresse IP publique de votre ordinateur virtuel.

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

Exemple

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

Vous devriez voir une réponse similaire à l'exemple suivant, qui montre une connexion SSH établie avec un ordinateur virtuel Ubuntu dans Lightsail for Research.



Maintenant que vous avez réussi à établir une connexion SSH à votre ordinateur virtuel, passez à la section suivante pour les étapes supplémentaires suivantes.

Passer aux étapes suivantes

Vous pouvez effectuer les étapes supplémentaires suivantes après avoir établi avec succès une connexion SSH à votre ordinateur virtuel :

- Connectez-vous à votre ordinateur virtuel à l'aide de SCP pour transférer des fichiers en toute sécurité. Pour de plus amples informations, veuillez consulter Transférez des fichiers vers des ordinateurs virtuels Lightsail for Research à l'aide de Secure Copy.

Transférez des fichiers vers des ordinateurs virtuels Lightsail for Research à l'aide de Secure Copy

Vous pouvez transférer des fichiers de votre ordinateur local vers un ordinateur virtuel dans Amazon Lightsail for Research à l'aide de Secure Copy (SCP). Avec ce processus, vous pouvez transférer plusieurs fichiers ou des répertoires entiers à la fois.

> **Note**
>
> Vous pouvez également établir une connexion par protocole d'affichage à distance avec votre ordinateur virtuel à l'aide du client Amazon DCV basé sur un navigateur disponible dans la console Lightsail for Research. Avec le client Amazon DCV, vous pouvez transférer rapidement des fichiers individuels. Pour de plus amples informations, veuillez consulter Accédez au système d'exploitation de votre ordinateur virtuel Lightsail for Research.

Rubriques

Remplir les conditions préalables

Remplissez les conditions préalables suivantes avant de démarrer.

- Créez un ordinateur virtuel dans Lightsail for Research. Pour de plus amples informations, veuillez consulter Création d'un ordinateur virtuel Lightsail for Research.

- Assurez-vous que l'ordinateur virtuel auquel vous souhaitez vous connecter fonctionne. Notez également le nom de l'ordinateur virtuel et la région AWS dans laquelle il a été créé. Vous aurez besoin de ces informations ultérieurement lors de cette procédure. Pour de plus amples informations, veuillez consulter Afficher les détails de l'ordinateur virtuel Lightsail for Research.
- Téléchargez et installez le AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente d' AWS CLI (français non garanti) dans le Guide de l'utilisateur AWS Command Line Interface pour la version 2.
- Configurez le AWS CLI pour accéder à votre Compte AWS. Pour plus d'informations, consultez Principes de base de la configuration (français non garanti) dans le Guide de l'utilisateur AWS Command Line Interface pour la version 2.
- Téléchargez et installez jq. Il s'agit d'un processeur JSON en ligne de commande, léger et flexible, utilisé dans les procédures suivantes pour extraire les détails des paires de clés. Pour plus d'informations sur le téléchargement et l'installation de jq, consultez la section Télécharger jq (français non garanti) sur le site Web de jq.
- Assurez-vous que le port 22 est ouvert sur l'ordinateur virtuel auquel vous souhaitez vous connecter. Il s'agit du port par défaut utilisé pour SSH. Il est ouvert par défaut. Mais si vous l'avez fermé, vous devez le rouvrir avant de continuer. Pour de plus amples informations, veuillez consulter Gestion des ports de pare-feu pour les ordinateurs virtuels Lightsail for Research.
- Obtenez la paire de clés par défaut (DKP) Lightsail pour votre ordinateur virtuel. Pour de plus amples informations, veuillez consulter Création d'un ordinateur virtuel Lightsail for Research.

Connexion à un ordinateur virtuel à l'aide de SCP

Effectuez l'une des procédures suivantes pour vous connecter à votre ordinateur virtuel dans Lightsail for Research à l'aide de SCP.

Connexion à un ordinateur virtuel à l'aide de SCP sur un ordinateur local Windows

Cette procédure s'applique à vous si votre ordinateur local utilise un système d'exploitation Windows. Cette procédure utilise la `get-instance` AWS CLI commande pour obtenir le nom d'utilisateur et l'adresse IP publique de l'instance à laquelle vous souhaitez vous connecter. Pour plus d'informations, consultez get-instance (français non garanti) dans la Référence des commandes AWS CLI .

> **Important**
>
> Assurez-vous d'obtenir la paire de clés par défaut (DKP) Lightsail pour l'ordinateur virtuel auquel vous essayez de vous connecter avant de commencer cette procédure. Pour de plus amples informations, veuillez consulter Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research. Cette procédure génère la clé privée du Lightsail DKP dans `dkp_rsa` un fichier utilisé dans l'une des commandes suivantes.

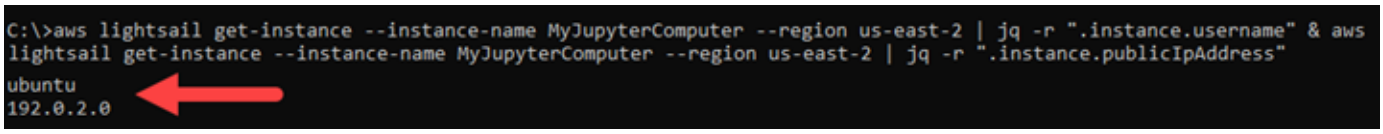
1. Ouvrez une fenêtre d'invite de commande.
2. Saisissez la commande suivante pour afficher l'adresse IP publique et le nom d'utilisateur de votre ordinateur virtuel. Dans la commande, remplacez *`region-code`* par le code de la AWS région dans laquelle l'ordinateur virtuel a été créé, tel que`us-east-2`. Remplacez *`computer-name`* par le nom de l'ordinateur virtuel auquel vous souhaitez vous connecter.

   ```
   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"
   ```

   Exemple

   ```
   aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
    | jq -r ".instance.username" & aws lightsail get-instance --region us-east-2 --
   instance-name MyJupyterComputer | jq -r ".instance.publicIpAddress"
   ```

   La réponse affichera le nom d'utilisateur et l'adresse IP publique de l'ordinateur virtuel, comme illustré dans l'exemple suivant. Notez ces valeurs, car vous en aurez besoin à l'étape suivante de cette procédure.

3. Saisissez la commande suivante pour établir une connexion SCP avec votre ordinateur virtuel et y transférer des fichiers.

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

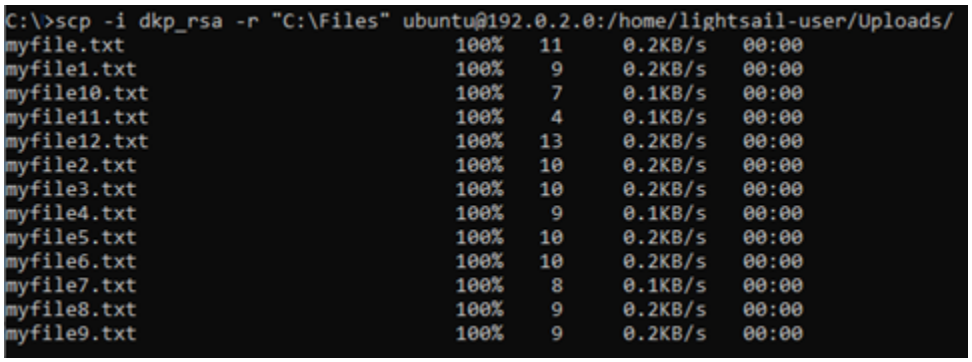
   Dans la commande, remplacez :

- *source-folder* avec le dossier sur votre ordinateur local qui contient les fichiers que vous souhaitez transférer.
- *user-name* avec le nom d'utilisateur de l'étape précédente de cette procédure (par exemple ubuntu).
- *public-ip-address* avec l'adresse IP publique de votre ordinateur virtuel indiquée à l'étape précédente de cette procédure.
- *destination-directory* avec le chemin du répertoire sur l'ordinateur virtuel où vous souhaitez copier vos fichiers.

L'exemple suivant copie tous les fichiers du dossier `C:\Files` sur l'ordinateur local vers le répertoire `/home/lightsail-user/Uploads/` de l'ordinateur virtuel distant.

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

Vous devriez voir une réponse similaire à l'exemple suivant. Il montre chaque fichier transféré du dossier d'origine vers le répertoire de destination. Vous devriez maintenant être en mesure d'accéder à ces fichiers sur votre ordinateur virtuel.



Connexion à un ordinateur virtuel à l'aide de SCP sur un ordinateur local Linux, Unix ou macOS

Cette procédure s'applique à vous si votre ordinateur local utilise un système d'exploitation Linux, Unix ou macOS. Cette procédure utilise la `get-instance` AWS CLI commande pour obtenir le nom d'utilisateur et l'adresse IP publique de l'instance à laquelle vous souhaitez vous connecter. Pour plus d'informations, consultez get-instance (français non garanti) dans la Référence des commandes AWS CLI .

> **Important**
>
> Assurez-vous d'obtenir la paire de clés par défaut (DKP) Lightsail pour l'ordinateur virtuel auquel vous essayez de vous connecter avant de commencer cette procédure. Pour de plus amples informations, veuillez consulter Obtenez une paire de clés pour un ordinateur virtuel Lightsail for Research. Cette procédure génère la clé privée du Lightsail DKP dans `dkp_rsa` un fichier utilisé dans l'une des commandes suivantes.

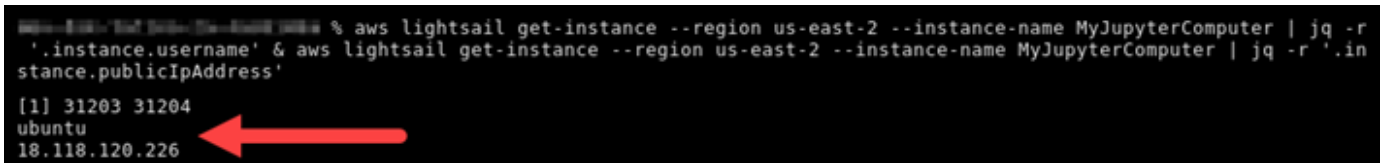
1. Ouvrez une fenêtre de terminal.
2. Saisissez la commande suivante pour afficher l'adresse IP publique et le nom d'utilisateur de votre ordinateur virtuel. Dans la commande, remplacez *`region-code`* par le code de la AWS région dans laquelle l'ordinateur virtuel a été créé, tel que`us-east-2`. Remplacez *`computer-name`* par le nom de l'ordinateur virtuel auquel vous souhaitez vous connecter.

   ```
   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'
   ```

   Exemple

   ```
   aws lightsail get-instance --region us-east-2 --instance-name MyJupyterComputer
    | jq -r '.instance.username' & aws lightsail get-instance --region us-east-2 --
   instance-name MyJupyterComputer | jq -r '.instance.publicIpAddress'
   ```

   La réponse affichera le nom d'utilisateur et l'adresse IP publique de l'ordinateur virtuel, comme illustré dans l'exemple suivant. Notez ces valeurs, car vous en aurez besoin à l'étape suivante de cette procédure.

3. Saisissez la commande suivante pour établir une connexion SCP avec votre ordinateur virtuel et y transférer des fichiers.

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

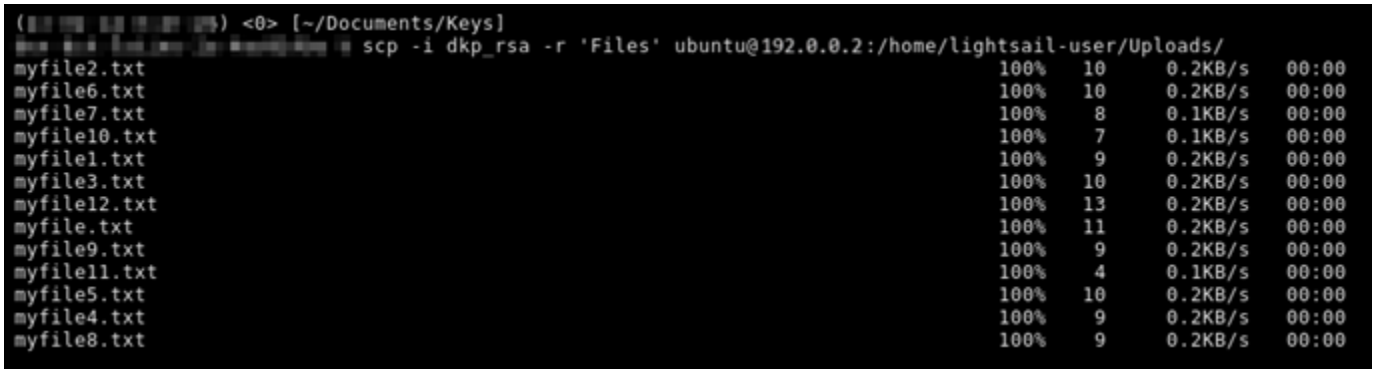
Dans la commande, remplacez :

- *source-folder* avec le dossier sur votre ordinateur local qui contient les fichiers que vous souhaitez transférer.
- *user-name* avec le nom d'utilisateur de l'étape précédente de cette procédure (par exemple ubuntu).
- *public-ip-address* avec l'adresse IP publique de votre ordinateur virtuel indiquée à l'étape précédente de cette procédure.
- *destination-directory* avec le chemin du répertoire sur l'ordinateur virtuel où vous souhaitez copier vos fichiers.

L'exemple suivant copie tous les fichiers du dossier `C:\Files` sur l'ordinateur local vers le répertoire `/home/lightsail-user/Uploads/` de l'ordinateur virtuel distant.

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

Vous devriez voir une réponse similaire à l'exemple suivant. Il montre chaque fichier transféré du dossier d'origine vers le répertoire de destination. Vous devriez maintenant être en mesure d'accéder à ces fichiers sur votre ordinateur virtuel.



Supprimer un ordinateur virtuel Lightsail for Research

Procédez comme suit pour supprimer votre ordinateur virtuel Lightsail for Research lorsque vous n'en avez plus besoin. Vous ne payez plus de frais pour l'ordinateur virtuel dès qu'il est supprimé. Les ressources attachées à l'ordinateur supprimé, telles que les instantanés, continuent d'être facturées jusqu'à ce que vous les supprimiez.

> **Important**
>
> La suppression d'un ordinateur virtuel est une action permanente et l'ordinateur ne peut pas être restauré. Si vous avez besoin de vos données ultérieurement, créez un instantané de votre ordinateur virtuel avant de le supprimer. Pour plus d'informations, consultez Création d'un instantané (français non garanti).

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, sélectionnez Ordinateurs virtuels.
3. Choisissez l'ordinateur virtuel à supprimer.
4. Choisissez Actions, puis sélectionnez Supprimer l'ordinateur virtuel.
5. Tapez confirmer dans le bloc de texte. Choisissez ensuite Supprimer l'ordinateur virtuel.

Sécurisez et stockez les données avec les volumes Lightsail for Research

Amazon Lightsail for Research fournit des volumes de stockage par blocs (disques) que vous pouvez associer à un ordinateur virtuel Lightsail for Research en cours d'exécution. Vous pouvez utiliser un disque comme périphérique de stockage principal pour les données nécessitant des mises à jour fréquentes et précises. Par exemple, les disques constituent l'option de stockage recommandée lorsque vous exécutez une base de données sur un ordinateur virtuel Lightsail for Research.

Un disque se comporte comme un périphérique de stockage en mode bloc externe non formaté que vous pouvez attacher à un ordinateur virtuel unique. Le volume persiste indépendamment de la durée d'exécution d'un ordinateur. Après avoir attaché un disque à un ordinateur, vous pouvez l'utiliser comme n'importe quel autre disque dur physique.

Vous pouvez attacher plusieurs disques à un ordinateur. Vous pouvez également détacher un disque d'un ordinateur et l'attacher à un autre ordinateur.

Pour conserver une copie de sauvegarde de vos données, créez un instantané du disque. Vous pouvez créer un nouveau disque à partir d'un instantané, puis l'attacher à un autre ordinateur.

Rubriques

Création d'un disque de stockage dans la console Lightsail for Research

Procédez comme suit pour créer un disque pour votre ordinateur virtuel Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, choisissez Stockage.

3. Choisissez Créer un disque.
4. Entrez un nom pour votre disque. Les caractères valables incluent les caractères alphanumériques, les chiffres, les points, les traits d'union et les traits de soulignement.

   Les noms de disques doivent respecter les critères suivants :

   - Soyez unique au sein de chaque Région AWS élément de votre compte Lightsail for Research.
   - Contiennent de 2 à 255 caractères.
   - Doivent commencer et se terminer par un caractère alphanumérique ou un chiffre.
5. Choisissez un Région AWS pour votre disque.

   Le disque doit se trouver dans la même région que l'ordinateur virtuel auquel vous allez l'attacher.
6. Choisissez la taille de votre disque en Go.
7. Passez à la section Attacher un disque pour obtenir des informations sur l'attachement de disques à votre ordinateur virtuel.

Afficher les détails du disque de stockage dans la console Lightsail for Research

Procédez comme suit pour afficher les disques de votre compte Lightsail for Research et leurs détails.

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, choisissez Stockage.

   La page Stockage fournit une vue complète des disques de votre compte Lightsail for Research.

   Les informations suivantes sont affichées sur la page :

   - Nom : le nom de votre disque de stockage.
   - Taille : la taille de votre disque (en Go).
   - Région AWS : l' Région AWS dans laquelle votre disque a été créée.
   - Connecté à : ordinateur Lightsail auquel votre disque est connecté.
   - Date de création : la date à laquelle votre disque a été créé.

Ajouter de l'espace de stockage à un ordinateur virtuel dans Lightsail for Research

Procédez comme suit pour connecter un disque à un ordinateur virtuel dans Lightsail for Research. Vous pouvez attacher jusqu'à 15 disques à un ordinateur virtuel. Lorsque vous connectez un disque à votre ordinateur virtuel à l'aide de la console Lightsail for Research, il est automatiquement formaté et monté par le service. Ce processus prend quelques minutes. Vous devez donc vérifier que le disque a atteint l'état de montage Monté avant de commencer à l'utiliser. Par défaut, Lightsail for Research monte les disques dans `/home/lightsail-user/<disk-name>` le répertoire ; `<disk-name>` où est le nom que vous avez donné à votre disque.

> **Important**
>
> Avant de pouvoir attacher un disque à un ordinateur virtuel, ce dernier doit être en cours d'exécution. Si vous attachez un disque à un ordinateur virtuel alors qu'il est à l'état Arrêté, le disque sera attaché mais ne pourra pas être monté. Si l'état de montage du disque est Échec, vous devez le détacher puis le rattacher lorsque l'ordinateur virtuel est en cours d'exécution.

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, sélectionnez Ordinateurs virtuels.
3. Choisissez l'ordinateur auquel attacher le disque.
4. Choisissez l'onglet Stockage.
5. Choisissez Attacher un disque.
6. Sélectionnez le nom du disque à attacher à l'ordinateur.
7. Choisissez Attacher.

Détacher un disque d'un ordinateur virtuel dans Lightsail for Research

Procédez comme suit pour détacher un disque d'un ordinateur.

1. Connectez-vous à la console Lightsail for Research.

2. Dans le panneau de navigation, choisissez Stockage.
3. Trouvez le disque à détacher. Dans la colonne Attaché à, choisissez le nom de l'ordinateur auquel le disque est attaché.
4. Choisissez Arrêter pour arrêter l'ordinateur. Vous devez arrêter l'ordinateur avant de pouvoir détacher le disque.
5. Confirmez que vous souhaitez arrêter l'ordinateur, puis choisissez Arrêter l'ordinateur.
6. Choisissez l'onglet Stockage.
7. Sélectionnez le disque à détacher, puis choisissez Détacher.
8. Confirmez que vous souhaitez détacher le disque de l'ordinateur, puis choisissez Détacher.

Supprimer les disques de stockage inutilisés dans Lightsail for Research

Procédez comme suit pour supprimer un disque de stockage lorsque vous n'en avez plus besoin. Vous ne payez plus de frais pour le disque dès qu'il est supprimé.

Si le disque est attaché à un ordinateur, vous devez d'abord le détacher avant de pouvoir le supprimer. Pour de plus amples informations, veuillez consulter Détacher un disque d'un ordinateur virtuel dans Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, choisissez Stockage.
3. Recherchez et sélectionnez le disque à supprimer.
4. Choisissez Supprimer le disque.
5. Confirmez que vous souhaitez supprimer votre disque. Ensuite, choisissez Supprimer.

Backup des ordinateurs virtuels et des disques avec des instantanés de Lightsail for Research

Les instantanés sont une point-in-time copie de vos données. Vous pouvez créer des instantanés de vos ordinateurs virtuels et disques de stockage Amazon Lightsail for Research, et les utiliser comme référence pour créer de nouveaux ordinateurs ou pour sauvegarder des données.

Un instantané contient toutes les données nécessaires pour restaurer votre ordinateur (au moment où l'instantané a été pris). Lorsque vous créez un nouvel ordinateur virtuel à partir d'un instantané, il commence par être un réplica exact de l'ordinateur original qui a été utilisé pour créer l'instantané.

Vos ressources étant susceptibles de tomber en panne à tout moment, nous vous recommandons de créer des instantanés fréquents pour éviter toute perte de données permanente.

Rubriques

Créez des instantanés d'ordinateurs ou de disques virtuels Lightsail for Research

Procédez comme suit pour créer un instantané de votre ordinateur virtuel ou de votre disque Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research.
2. Choisissez Instantanés dans le panneau de navigation.
3. Effectuez l'une des étapes suivantes :

    - Sous Instantanés d'ordinateur virtuel, recherchez le nom de l'ordinateur que vous souhaitez capturer et choisissez Créer un instantané.
    - Sous Instantanés de disque, recherchez le nom du disque pour lequel vous souhaitez créer un instantané et sélectionnez Créer un instantané.

4. Saisissez un nom pour votre instantané. Les caractères valables incluent les caractères alphanumériques, les chiffres, les points, les traits d'union et les traits de soulignement.

   Les noms des instantanés doivent respecter les critères suivants :

   - Soyez unique Région AWS dans chaque élément de votre compte Lightsail for Research.
   - Contiennent de 2 à 255 caractères.
   - Doivent commencer et se terminer par un caractère alphanumérique ou un chiffre.
5. Choisissez Créer un instantané.

Afficher et gérer des instantanés d'ordinateurs virtuels et de disques dans Lightsail for Research

Procédez comme suit pour afficher les instantanés de vos ordinateurs virtuels et de vos disques.

1. Connectez-vous à la console Lightsail for Research.
2. Choisissez Instantanés dans le panneau de navigation.

   La page Instantanés affiche les instantanés d'ordinateur virtuel et de disque que vous avez créés.

   Les instantanés archivés se trouvent également sur cette page. Les instantanés archivés sont des instantanés des ressources qui ont été supprimées de votre compte.

Créer un ordinateur ou un disque virtuel à partir d'un instantané

Procédez comme suit pour créer un nouvel ordinateur virtuel ou un nouveau disque Lightsail for Research à partir d'un instantané.

Lorsque vous créez un ordinateur virtuel à partir d'un instantané, utilisez un plan de même taille ou supérieur à celui utilisé pour l'ordinateur d'origine. Vous ne pouvez pas utiliser un plan inférieur à celui de l'ordinateur virtuel d'origine.

Lorsque vous créez un disque à partir d'un instantané, choisissez une taille de disque supérieure à celle du disque d'origine. Vous ne pouvez pas utiliser un disque plus petit que l'original.

1. Connectez-vous à la console Lightsail for Research.

2. Choisissez Instantanés dans le panneau de navigation.
3. Sur la page Instantanés, recherchez le nom de l'instantané d'ordinateur ou de disque que vous utiliserez pour créer le nouvel ordinateur ou le nouveau disque. Choisissez le menu déroulant Instantanés pour afficher la liste des instantanés disponibles pour cette ressource.
4. Sélectionnez l'instantané que vous souhaitez utiliser pour créer l'ordinateur virtuel.
5. Choisissez le menu déroulant Actions. Choisissez ensuite Créer un ordinateur virtuel ou Créer un disque.

Supprimer un instantané dans la console Lightsail for Research

Pour supprimer un instantané, effectuez les opérations suivantes.

1. Connectez-vous à la console Lightsail for Research.
2. Choisissez Instantanés dans le panneau de navigation.
3. Sur la page Instantanés, recherchez le nom de l'instantané d'ordinateur ou de disque que vous souhaitez supprimer. Choisissez le menu déroulant Instantanés pour afficher la liste des instantanés disponibles pour cette ressource.
4. Choisissez l'instantané à supprimer.
5. Choisissez le menu déroulant Actions. Choisissez ensuite Supprimer l'instantané.
6. Vérifiez que le nom de l'instantané est correct. Choisissez ensuite Supprimer l'instantané.

Estimations des coûts et de l'utilisation dans Lightsail for Research

Amazon Lightsail for Research propose des estimations du coût et de l'utilisation de vos ressources. AWS Vous pouvez utiliser ces estimations pour vous aider à planifier vos dépenses, à identifier des opportunités de réduction des coûts et à prendre des décisions éclairées lorsque vous utilisez Lightsail for Research.

Lorsque vous créez un ordinateur ou un disque virtuel, les estimations de coût et d'utilisation sont affichées pour cette ressource. Une estimation des coûts et d'utilisation commence à être suivie dès qu'une ressource est créée et qu'elle est disponible ou en cours d'exécution. L'estimation apparaîtra dans la console de gestion AWS dans les 15 minutes suivant la création de la ressource. Les ressources supprimées ne sont pas incluses dans une estimation.

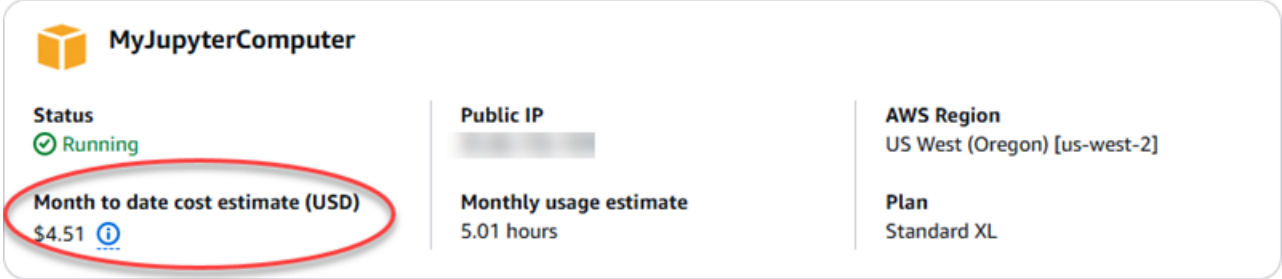
> **Important**
>
> Une estimation est un coût estimé basé sur l'utilisation de la ressource. Votre coût réel sera basé sur l'utilisation réelle de vos ressources, et non sur l'estimation affichée dans la console Lightsail for Research. Les coûts réels sont indiqués sur votre relevé de AWS Billing compte. Connectez-vous à la AWS Billing and Cost Management console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/costmanagement/.

Rubriques

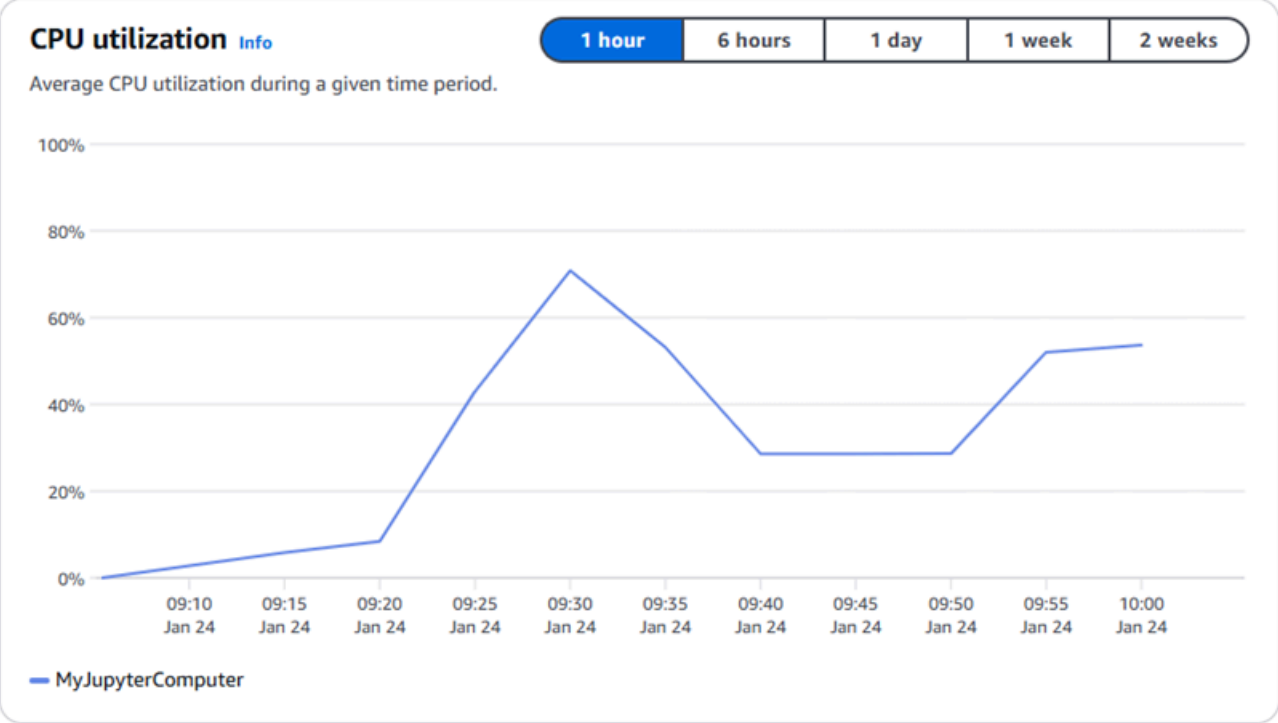
Afficher les estimations du coût et de l'utilisation de vos ressources dans Lightsail for Research

Les estimations du coût mensuel et de l'utilisation de vos ressources Lightsail for Research sont affichées dans les zones suivantes de la console Lightsail for Research.

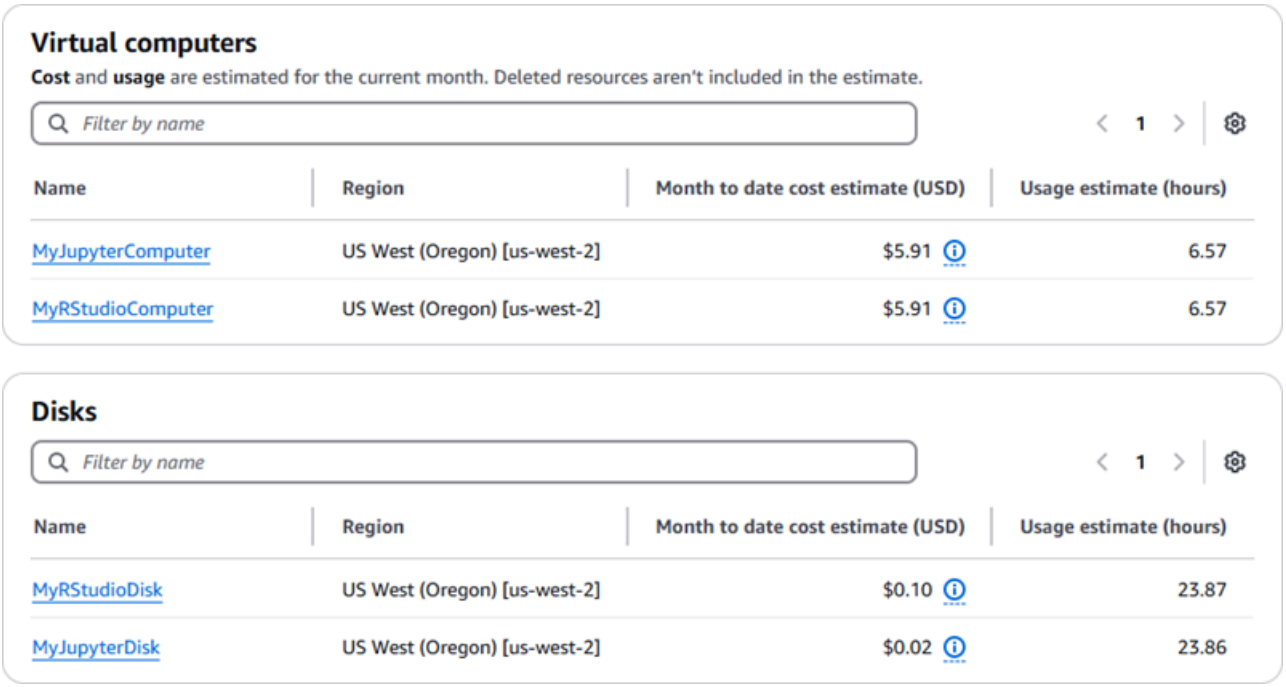
1. Choisissez Ordinateurs virtuels dans le volet de navigation de la console Lightsail for Research. L'estimation des coûts mensuels cumulés de vos ordinateurs virtuels est répertoriée sous chaque ordinateur virtuel en cours d'exécution.



2. Pour afficher l'utilisation du CPU d'un ordinateur virtuel, choisissez le nom de l'ordinateur virtuel, puis cliquez sur l'onglet Tableau de bord.



3. Pour consulter le coût mensuel cumulé et les estimations d'utilisation de toutes vos ressources Lightsail for Research, sélectionnez Utilisation dans le volet de navigation.



Virtual computers

Cost and **usage** are estimated for the current month. Deleted resources aren't included in the estimate.

Filter by name

1

Name	Region	Month to date cost estimate (USD)	Usage estimate (hours)
MyJupyterComputer	US West (Oregon) [us-west-2]	$5.91	6.57
MyRStudioComputer	US West (Oregon) [us-west-2]	$5.91	6.57

Disks

Filter by name

1

Name	Region	Month to date cost estimate (USD)	Usage estimate (hours)
MyRStudioDisk	US West (Oregon) [us-west-2]	$0.10	23.87
MyJupyterDisk	US West (Oregon) [us-west-2]	$0.02	23.86

Gérez les règles de contrôle des coûts dans Lightsail for Research

Le contrôle des coûts utilise des règles que vous définissez pour vous aider à gérer l'utilisation et le coût de vos ordinateurs virtuels Lightsail for Research.

Vous pouvez créer une règle d'Arrêter l'ordinateur virtuel en veille qui arrête un ordinateur en cours d'exécution lorsqu'il atteint un pourcentage spécifié de son utilisation du CPU au cours d'une période donnée. Par exemple, une règle peut arrêter automatiquement un ordinateur spécifique lorsque son utilisation du CPU est égale ou inférieure à 5 % pendant une période de 30 minutes. Cela signifie que l'ordinateur est inactif et que Lightsail for Research l'arrête. Vous n'avez plus à payer les frais horaires standard après l'arrêt de l'ordinateur virtuel.

Rubriques

Créez des règles de contrôle des coûts pour vos ordinateurs virtuels Lightsail for Research

Procédez comme suit pour créer une règle pour votre ordinateur virtuel Lightsail for Research.

> **Note**
>
> La seule action de règle prise en charge pour le moment consiste à arrêter un ordinateur virtuel. L'utilisation du CPU est la seule métrique actuellement surveillée par des règles, et la seule opération prise en charge est inférieure ou égale à.

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, choisissez Contrôle des coûts.
3. Choisissez Créer une règle.
4. Sélectionnez la ressource à laquelle appliquer la règle.

5. Spécifiez le pourcentage d'utilisation du CPU et la période pendant laquelle la règle doit s'exécuter.

   Par exemple, vous pouvez spécifier 5 % et 30 minutes. Lightsail for Research arrête automatiquement l'ordinateur lorsque le taux d'utilisation du processeur est inférieur ou égal à 5 % sur une période de 30 minutes.
6. Choisissez Créer une règle.
7. Vérifiez que les informations relatives à votre nouvelle règle sont correctes, puis choisissez Confirmer.

Supprimer les règles de contrôle des coûts pour vos ordinateurs virtuels Lightsail for Research

Procédez comme suit pour supprimer une règle pour votre ordinateur virtuel Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research.
2. Dans le panneau de navigation, choisissez Contrôle des coûts.
3. Sélectionnez la règle à supprimer.
4. Sélectionnez Delete (Supprimer).
5. Vérifiez que vous souhaitez supprimer la règle et choisissez Supprimer.

Organisez les ressources de Lightsail for Research à l'aide de balises

Avec Amazon Lightsail for Research, vous pouvez attribuer des balises à vos ressources. Chaque balise est une étiquette composée d'une clé et d'une valeur facultative, qui peut rendre efficace la gestion de vos ressources. Une clé sans valeur est appelée balise clé uniquement et une clé avec une valeur est appelée balise clé-valeur. Bien qu'il n'y ait pas de types de balises inhérents, ils vous permettent de classer vos ressources en fonction de leur objectif, de leur propriétaire, de leur environnement ou d'autres critères. Cela est utile lorsque vous avez de nombreuses ressources du même type. Vous pouvez identifier rapidement une ressource spécifique en fonction des étiquettes que vous lui avez attribuées. Par exemple, vous pouvez définir un ensemble de balises qui vous permettent de suivre le projet ou la priorité de chaque ressource.

Les ressources suivantes peuvent être balisées dans la console Amazon Lightsail for Research :

- Ordinateurs virtuels
- Disques de stockage
- Instantanés

Les restrictions suivantes s'appliquent aux balises :

- Le nombre maximum d'identifications par ressource est de 50.
- Pour chaque ressource, chaque clé de la balise doit être unique. Chaque clé de balise ne peut avoir qu'une seule valeur.
- La longueur maximale de la clé est de 128 caractères Unicode en UTF-8.
- La longueur maximale de la valeur est de 256 caractères Unicode en UTF-8.
- Si votre schéma de balisage est utilisé pour plusieurs services et ressources, n'oubliez pas que d'autres services peuvent avoir des restrictions concernant les caractères autorisés. Les caractères généralement autorisés sont : les lettres, les chiffres, les espaces et les caractères suivants : `+ - = . _ : / @`
- Les clés et valeurs d'étiquette sont sensibles à la casse.
- N'utilisez pas le préfixe `aws:` pour des clés ou des valeurs. Ce préfixe est réservé à l' AWS usage.

Rubriques

Tag : Lightsail pour les ressources de recherche

Procédez comme suit pour créer une balise pour votre ordinateur virtuel Lightsail for Research. Les étapes sont similaires pour les disques et les instantanés Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research sur la console Lightsail for Research.
2. Dans le panneau de navigation, sélectionnez Ordinateurs virtuels.
3. Sélectionnez l'ordinateur virtuel pour lequel vous souhaitez créer une balise.
4. Sélectionnez l'onglet Tags (Identifications).
5. Choisissez Gérer les balises.
6. Choisissez Add new tag (Ajouter une nouvelle balise).
7. Saisissez un nom de clé dans le champ Clé. Par exemple, Projet.
8. (Facultatif) Saisissez un nom de valeur dans le champ valeur. Par exemple, Blog.
9. Choisissez Enregistrer les modifications pour enregistrer la clé sur votre ordinateur virtuel.

Supprimer les tags des ressources de Lightsail for Research

Procédez comme suit pour supprimer une balise de votre ordinateur virtuel Lightsail for Research. Les étapes sont similaires pour les disques et les instantanés Lightsail for Research.

1. Connectez-vous à la console Lightsail for Research sur la console Lightsail for Research.
2. Dans le panneau de navigation, sélectionnez Ordinateurs virtuels.
3. Sélectionnez l'ordinateur virtuel dont vous souhaitez supprimer la balise.
4. Sélectionnez l'onglet Tags (Identifications).
5. Choisissez Gérer les balises.
6. Sélectionnez Supprimer pour supprimer la balise de la ressource.

> **Note**
>
> Si vous souhaitez uniquement supprimer la valeur de la balise, localisez la valeur, puis cliquez sur l'icône X située à côté.

7. Sélectionnez Enregistrer les modifications.

La sécurité dans Amazon Lightsail pour la recherche

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon Lightsail for Research, AWS consultez la section Services concernés par programme de conformité Services concernés par AWS
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Lightsail for Research. Les rubriques suivantes expliquent comment configurer Lightsail for Research afin d'atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Lightsail for Research.

Rubriques

Protection des données dans Amazon Lightsail for Research

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Lightsail for Research. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Lightsail for Research ou Services AWS autre

à l'aide de la console, de l'API AWS CLI ou. AWS SDKs Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Identity and Access Management pour Amazon Lightsail for Research

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de Lightsail for Research. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

> **Note**
>
> Amazon Lightsail et Lightsail for Research partagent les mêmes paramètres de politique IAM. Les modifications apportées aux politiques de Lightsail for Research affecteront également les politiques de Lightsail. Par exemple, si un utilisateur est autorisé à créer un disque dans Lightsail for Research, ce même utilisateur peut également créer un disque dans Lightsail.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Lightsail for Research.

Utilisateur du service : si vous utilisez le service Lightsail for Research pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de Lightsail for Research dans le cadre de votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité de Lightsail for Research, consultez. Résolution des problèmes d'identité et d'accès à Amazon Lightsail for Research

Administrateur du service — Si vous êtes responsable des ressources de Lightsail for Research au sein de votre entreprise, vous avez probablement un accès complet à Lightsail for Research. Il vous incombe de déterminer les fonctionnalités et ressources de Lightsail for Research auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser l'IAM avec Lightsail for Research, consultez. Comment Amazon Lightsail for Research fonctionne avec IAM

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Lightsail for Research. Pour consulter des exemples de politiques basées sur l'identité de Lightsail for Research que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour Amazon Lightsail for Research

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec

des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains

services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette

ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités

figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.

- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Amazon Lightsail for Research fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Lightsail for Research, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Lightsail for Research.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon Lightsail for Research

Fonctionnalité IAM	Lightsail pour le soutien à la recherche
Politiques basées sur l'identité	Oui

Fonctionnalité IAM	Lightsail pour le soutien à la recherche
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACLs	Non
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Autorisations de principals	Non
Fonctions du service	Non
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont Lightsail for Research et les AWS autres services fonctionnent avec la plupart des fonctionnalités IAM, AWS consultez la section Services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Lightsail for Research

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou

refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour Lightsail for Research

Pour consulter des exemples de politiques basées sur l'identité de Lightsail for Research, voir. Exemples de politiques basées sur l'identité pour Amazon Lightsail for Research

Politiques basées sur les ressources au sein de Lightsail for Research

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Actions politiques pour Lightsail for Research

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions de Lightsail for Research, consultez la section Actions définies par Amazon Lightsail for Research dans la référence d'autorisation du service.

Dans Lightsail for Research, les actions stratégiques utilisent le préfixe suivant avant l'action :

```
lightsail
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour consulter des exemples de politiques basées sur l'identité de Lightsail for Research, voir. Exemples de politiques basées sur l'identité pour Amazon Lightsail for Research

Ressources politiques pour Lightsail for Research

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources Lightsail for Research et ARNs leurs caractéristiques, consultez la section Ressources définies par Amazon Lightsail for Research dans le Guide d'autorisation du service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon Lightsail for Research.

Pour consulter des exemples de politiques basées sur l'identité de Lightsail for Research, voir. Exemples de politiques basées sur l'identité pour Amazon Lightsail for Research

Clés de conditions de politique pour Lightsail for Research

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition de Lightsail for Research, consultez la section Clés de condition pour Amazon Lightsail for Research dans le manuel de référence d'autorisation du service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon Lightsail for Research.

Pour consulter des exemples de politiques basées sur l'identité de Lightsail for Research, voir. Exemples de politiques basées sur l'identité pour Amazon Lightsail for Research

ACLs dans Lightsail for Research

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Lightsail pour la recherche

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Lightsail for Research

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Lightsail for Research

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Lightsail for Research

Prend en charge les rôles de service : Non

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut interrompre les fonctionnalités de Lightsail for Research. Modifiez les rôles de service uniquement lorsque Lightsail for Research fournit des instructions à cet effet.

Rôles liés aux services pour Lightsail for Research

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Amazon Lightsail for Research

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources Lightsail for Research. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Lightsail for Research, y compris le format de ARNs chaque type de ressource, consultez la section Actions, ressources et clés de condition pour Amazon Lightsail for Research dans la référence d'autorisation du service.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer les ressources Lightsail for Research de votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.

- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Lightsail for Research

Pour accéder à la console Amazon Lightsail for Research, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les informations relatives aux ressources Lightsail for Research présentes dans votre. Compte AWS Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum

d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Lightsail for Research, associez également la politique Lightsail for Research ou la politique gérée aux *ConsoleAccess* entités. *ReadOnly* AWS Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

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

```
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Résolution des problèmes d'identité et d'accès à Amazon Lightsail for Research

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de Lightsail for Research et d'IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Lightsail for Research
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Lightsail for Research

Je ne suis pas autorisé à effectuer une action dans Lightsail for Research

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `lightsail:`*`GetWidget`* fictives.

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

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `lightsail:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Lightsail for Research

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Lightsail for Research prend en charge ces fonctionnalités, consultez. Comment Amazon Lightsail for Research fonctionne avec IAM
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Validation de conformité pour Amazon Lightsail for Research

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

La résilience dans Amazon Lightsail pour la recherche

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, Lightsail for Research propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données. Pour plus d'informations, consultez Backup des ordinateurs virtuels et des disques avec des instantanés de Lightsail for Research et Créez des instantanés d'ordinateurs ou de disques virtuels Lightsail for Research.

Sécurité de l'infrastructure dans Amazon Lightsail for Research

En tant que service géré, Amazon Lightsail for Research est protégé par la sécurité AWS du réseau mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Lightsail for Research via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.

- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Analyse de configuration et de vulnérabilité dans Amazon Lightsail for Research

La configuration et les contrôles informatiques sont une responsabilité partagée entre vous AWS et vous, notre client. Pour plus d'informations, consultez le modèle de responsabilité AWS partagée.

Bonnes pratiques de sécurité pour Amazon Lightsail for Research

Lightsail for Research propose un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Pour éviter les événements de sécurité potentiels associés à votre utilisation de Lightsail for Research, suivez les meilleures pratiques suivantes :

- Accédez à la console Lightsail for Research en vous authentifiant auprès de la première console. AWS Management Console Ne partagez pas vos informations d'identification personnelles de console. Tous les utilisateurs d'Internet peuvent accéder à la console, mais ils ne peuvent pas se connecter ou démarrer une session s'ils n'ont pas d'informations d'identification valides pour la console.

Historique du document relatif au guide de l'utilisateur de Lightsail for Research

Le tableau suivant décrit les versions de documentation de Lightsail for Research.

Modification	Description	Date
Première version	Première publication du guide de l'utilisateur de Lightsail for Research.	28 février 2023

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.