aws

Panduan Pengguna

Amazon Lightsail untuk Penelitian

Amazon Lightsail untuk Penelitian: Panduan Pengguna

Table of Contents

Apa itu Amazon Lightsail untuk Penelitian?

Dengan Amazon Lightsail for Research, akademisi dan peneliti dapat membuat komputer virtual yang kuat di Amazon Web Services () Cloud.AWS Komputer virtual ini dilengkapi dengan aplikasi penelitian pra-instal, seperti RStudio dan Scilab.

Dengan Lightsail for Research, Anda dapat mengunggah data langsung dari browser web untuk memulai pekerjaan Anda. Anda dapat membuat dan menghapus komputer virtual Anda kapan saja, yang memberi Anda akses sesuai permintaan ke sumber daya komputasi yang kuat.

Anda hanya membayar selama Anda membutuhkan komputer virtual. Lightsail for Research menawarkan kontrol penganggaran yang dapat secara otomatis menghentikan komputer Anda ketika mencapai batas biaya yang telah dikonfigurasi sebelumnya, jadi Anda tidak perlu khawatir tentang biaya kelebihan biaya.

Semua yang Anda lakukan di konsol Lightsail for Research didukung oleh API yang tersedia untuk umum. Pelajari cara menginstal dan menggunakan API AWS CLIdan untuk Amazon Lightsail.

Harga

Dengan Lightsail for Research, Anda hanya membayar untuk sumber daya yang Anda buat dan gunakan. Untuk informasi selengkapnya, lihat harga Lightsail for Research.

Ketersediaan

Lightsail for Research tersedia di Wilayah AWS yang sama dengan Amazon Lightsail, dengan pengecualian Wilayah AS Timur (Virginia N.). Lightsail for Research juga menggunakan titik akhir yang sama dengan Lightsail. Untuk melihat AWS Wilayah dan titik akhir Lightsail yang saat ini didukung, lihat Titik Akhir Lightsail dan Kuota di Referensi Umum.AWS

Menyiapkan Amazon Lightsail untuk Penelitian

Jika Anda AWS pelanggan baru, selesaikan prasyarat penyiapan yang tercantum di halaman ini sebelum Anda mulai menggunakan Amazon Lightsail for Research.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan menerima panggilan telepon atau pesan teks dan memasukkan kode verifikasi pada keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke Konsol Manajemen AWSsebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.

2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Tutorial: Memulai dengan Lightsail for Research komputer virtual

Gunakan tutorial ini untuk memulai dengan Amazon Lightsail for Research komputer virtual. Anda akan belajar cara membuat, terhubung ke, dan menggunakan komputer virtual. Dalam Lightsail for Research, komputer virtual adalah workstation penelitian yang Anda buat dan kelola di. AWS Cloud Komputer virtual didasarkan pada instance Lightsail Linux dengan sistem operasi Ubuntu. Di komputer virtual Anda, Anda dapat mengkonfigurasi aplikasi penelitian seperti JupyterLab,, Scilab RStudio, dan banyak lagi.

Komputer virtual yang Anda buat dalam tutorial ini akan dikenakan biaya penggunaan dari saat Anda membuat komputer virtual hingga Anda menghapusnya. Penghapusan adalah langkah terakhir dari tutorial ini. Untuk informasi selengkapnya tentang harga, lihat harga Lightsail for Research.

Topik

Langkah 1: Selesaikan prasyarat

Jika Anda AWS pelanggan baru, selesaikan prasyarat penyiapan sebelum Anda mulai menggunakan Amazon Lightsail for Research. Untuk informasi selengkapnya, lihat Menyiapkan Amazon Lightsail untuk Penelitian.

Langkah 2: Buat komputer virtual

Anda dapat membuat komputer virtual dengan menggunakan konsol Lightsail for Research seperti yang dijelaskan dalam prosedur berikut. Tutorial ini dimaksudkan untuk membantu Anda dengan

cepat meluncurkan komputer virtual pertama Anda. Kami juga merekomendasikan untuk menjelajahi aplikasi dan paket perangkat keras yang tersedia. Untuk informasi selengkapnya, silakan lihat Pilih gambar aplikasi dan paket perangkat keras untuk Lightsail for Research dan Buat Lightsail untuk Penelitian komputer virtual.

1. Masuk ke konsol Lightsail for Research.
2. Di halaman beranda, pilih Buat komputer virtual.
3. Pilih Wilayah AWS untuk komputer virtual Anda.

   Pilih Wilayah AWS yang paling dekat dengan lokasi fisik Anda untuk mengurangi latensi.
4. Pilih aplikasi, juga dikenal sebagai cetak biru di Lightsail API.

   Aplikasi yang Anda pilih diinstal dan dikonfigurasi di komputer virtual Anda saat Anda membuatnya.
5. Pilih paket perangkat keras, juga dikenal sebagai bundel di Lightsail API.

   Paket perangkat keras menawarkan jumlah daya pemrosesan yang berbeda termasuk inti vCPU, memori, penyimpanan, dan transfer data bulanan. Lightsail for Research menawarkan paket standar dan paket GPU untuk komputer virtual. Pilih paket standar ketika persyaratan komputasi pekerjaan Anda rendah. Pilih paket GPU saat persyaratan itu tinggi, seperti saat menjalankan model pembelajaran mesin atau tugas intensif komputasi lainnya.
6. Masukkan nama untuk komputer virtual Anda.
7. Pilih Buat komputer virtual di panel Ringkasan.

Setelah komputer virtual baru Anda aktif dan berjalan, lanjutkan ke langkah berikutnya dari tutorial ini untuk mempelajari cara meluncurkan aplikasi komputer.

Langkah 3: Luncurkan aplikasi komputer virtual

Setelah Anda membuat komputer virtual dan dalam keadaan Running, Anda dapat meluncurkan sesi virtual di browser web Anda. Dengan sesi ini, Anda dapat berinteraksi dengan dan mengelola aplikasi yang diinstal pada komputer virtual Anda.

1. Pilih Komputer virtual di panel navigasi konsol Lightsail for Research.
2. Temukan nama komputer virtual yang Anda buat di Langkah 1, dan pilih Luncurkan aplikasi. Misalnya, Luncurkan JupyterLab. Sesi aplikasi terbuka di jendela browser web baru.

> **Important**
>
> Jika browser web Anda memiliki pemblokir pop-up yang diinstal, Anda mungkin perlu mengizinkan pop-up dari domain aws.amazon.com sebelum membuka sesi Anda.

Untuk mempelajari cara terhubung ke komputer virtual Anda, lanjutkan ke langkah berikutnya dari tutorial ini.

Langkah 4: Connect ke komputer virtual Anda

Anda dapat terhubung ke komputer virtual Anda menggunakan metode berikut:

- Gunakan klien Amazon DCV berbasis browser yang tersedia di konsol Lightsail for Research. Dengan Amazon DCV, Anda dapat menggunakan antarmuka pengguna grafis (GUI) untuk berinteraksi dengan aplikasi penelitian dan sistem operasi komputer virtual Anda.

  Anda juga dapat mengakses antarmuka baris perintah komputer virtual Anda dan mentransfer file dengan menggunakan klien Amazon DCV berbasis browser.
- Gunakan klien shell aman (SSH) seperti OpenSSH, Putty, atau Windows Subsystem untuk Linux untuk mengakses antarmuka baris perintah komputer virtual Anda. Dengan klien SSH, Anda dapat mengedit skrip dan file konfigurasi.
- Gunakan Secure Copy (SCP) untuk mentransfer file dengan aman antara komputer lokal dan komputer virtual Anda. Dengan SCP, Anda dapat memulai pekerjaan Anda secara lokal dan melanjutkannya di komputer virtual Anda. Anda juga dapat mengunduh file dari komputer virtual Anda untuk menyalin pekerjaan Anda ke komputer lokal Anda.

Anda harus menyediakan key pair komputer virtual Anda untuk menghubungkannya menggunakan SSH atau untuk mentransfer file menggunakan SCP. Key pair adalah seperangkat kredensyal keamanan yang Anda gunakan untuk membuktikan identitas Anda saat menghubungkan ke komputer virtual Lightsail for Research. Sebuah key pair terdiri dari public key dan private key.

Untuk informasi selengkapnya tentang menghubungkan ke komputer virtual Anda, lihat dokumentasi berikut:

- Buat koneksi protokol tampilan jarak jauh:

  - Akses Lightsail for Research aplikasi komputer virtual
  - Akses Lightsail for Research sistem operasi komputer virtual
- Buat koneksi SSH atau transfer file menggunakan SCP:
  - Dapatkan key pair untuk komputer virtual Lightsail for Research
  - Connect ke komputer virtual Lightsail for Research menggunakan Secure Shell
  - Transfer file ke Lightsail untuk Penelitian komputer virtual menggunakan Secure Copy

Untuk mempelajari tentang penyimpanan untuk komputer virtual Anda, lanjutkan ke langkah berikutnya dari tutorial ini.

Langkah 5: Tambahkan penyimpanan ke komputer virtual Anda

Lightsail for Research menyediakan volume penyimpanan tingkat blok (disk) yang dapat Anda lampirkan ke komputer virtual. Meskipun komputer virtual Anda dilengkapi dengan disk sistem, Anda dapat melampirkan disk tambahan ke komputer virtual Anda karena kebutuhan penyimpanan Anda berubah. Anda juga dapat melepaskan disk dari komputer virtual dan memasangnya ke komputer virtual lain.

Saat Anda memasang disk ke komputer virtual Anda menggunakan konsol, Lightsail for Research secara otomatis memformat dan memasang disk di sistem operasi Anda. Proses ini memakan waktu beberapa menit, jadi Anda harus mengonfirmasi bahwa disk dalam status Mounted sebelum Anda mulai menggunakannya.

Untuk informasi selengkapnya tentang membuat, melampirkan, dan mengelola disk, lihat dokumentasi berikut:

- Buat disk penyimpanan di konsol Lightsail for Research
- Lihat detail disk penyimpanan di konsol Lightsail for Research
- Tambahkan penyimpanan ke komputer virtual di Lightsail for Research
- Lepaskan disk dari komputer virtual di Lightsail for Research
- Hapus disk penyimpanan yang tidak digunakan di Lightsail for Research

Untuk mempelajari tentang mencadangkan komputer virtual Anda, lanjutkan ke langkah berikutnya dari tutorial ini.

Langkah 6: Buat snapshot

Snapshot adalah point-in-time salinan data Anda. Anda dapat membuat snapshot dari komputer virtual Anda dan menggunakannya sebagai garis dasar untuk membuat komputer baru atau untuk cadangan data. Snapshot berisi semua data yang diperlukan untuk memulihkan komputer Anda (dari saat snapshot diambil).

Untuk informasi selengkapnya tentang membuat dan mengelola snapshot, lihat dokumentasi berikut:

- Buat snapshot dari Lightsail for Research komputer virtual atau disk
- Lihat dan kelola snapshot komputer dan disk virtual di Lightsail for Research
- Buat komputer virtual atau disk dari snapshot
- Menghapus snapshot di konsol Lightsail for Research

Untuk mempelajari tentang membersihkan sumber daya komputer virtual Anda, lanjutkan ke langkah berikutnya dari tutorial ini.

Langkah 7: Bersihkan

Setelah Anda selesai dengan komputer virtual yang Anda buat untuk tutorial ini, Anda dapat menghapusnya. Ini berhenti menimbulkan biaya untuk komputer virtual jika Anda tidak membutuhkannya.

Menghapus komputer virtual tidak menghapus snapshot terkait atau disk terlampir. Jika Anda membuat snapshot dan disk, Anda harus menghapusnya secara manual untuk menghentikan biaya untuk mereka.

Untuk menyimpan komputer virtual Anda untuk nanti, tetapi untuk menghindari dikenakan biaya dengan harga per jam standar, Anda dapat menghentikan komputer virtual alih-alih menghapusnya. Kemudian Anda bisa memulainya lagi nanti. Untuk informasi selengkapnya, lihat Lihat Lightsail for Research detail komputer virtual. Untuk informasi selengkapnya tentang harga, lihat harga Lightsail for Research.

> **Important**
>
> Menghapus sumber daya Lightsail for Research adalah tindakan permanen. Data yang dihapus tidak dapat dipulihkan. Jika Anda mungkin memerlukan data nanti, buat snapshot

komputer virtual Anda sebelum Anda menghapusnya. Untuk informasi selengkapnya, lihat Membuat snapshot.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi.
3. Pilih komputer virtual yang akan dihapus.
4. Pilih Tindakan, lalu pilih Hapus komputer virtual.
5. Ketik konfirmasi di blok teks. Kemudian, pilih Hapus komputer virtual.

Memulai aplikasi ilmu data di Lightsail for Research

Tutorial berikut memberikan informasi tambahan tentang cara memulai dengan aplikasi tertentu yang tersedia di Lightsail for Research.

Topik

> **Note**
>
> Tutorial mendalam untuk memulai dengan Lightsail for Research RStudio dan dipublikasikan ke AWS Blog Sektor Publik. Untuk informasi selengkapnya, lihat Memulai Amazon Lightsail for Research: Tutorial menggunakan. RStudio

Luncurkan dan gunakan JupyterLab pada Lightsail untuk Penelitian

Dalam tutorial ini, kami menunjukkan kepada Anda cara memulai mengelola dan menggunakan komputer JupyterLab virtual Anda di Amazon Lightsail for Research.

Topik

Langkah 1: Selesaikan prasyarat

Buat komputer virtual menggunakan JupyterLab aplikasi jika Anda belum melakukannya. Untuk informasi selengkapnya, lihat Buat Lightsail untuk Penelitian komputer virtual.

Setelah komputer virtual baru Anda aktif dan berjalan, lanjutkan ke bagian peluncuran JupyterLab aplikasi tutorial ini.

Langkah 2: (Opsional) Tambahkan ruang penyimpanan

Komputer virtual Anda dilengkapi dengan disk sistem. Namun, karena kebutuhan penyimpanan Anda berubah, Anda dapat melampirkan disk tambahan ke komputer virtual Anda untuk menambah ruang penyimpanannya.

Anda juga dapat menyimpan file kerja Anda ke disk yang terpasang. Kemudian Anda dapat melepaskan disk dan melampirkannya ke komputer virtual yang berbeda untuk memindahkan file Anda dengan cepat dari satu komputer ke komputer lain.

Atau, Anda dapat membuat snapshot dari disk terlampir yang memiliki file kerja Anda, dan kemudian membuat disk duplikat dari snapshot. Kemudian Anda dapat melampirkan disk duplikat baru ke komputer lain untuk menduplikasi pekerjaan Anda di komputer virtual yang berbeda. Untuk informasi selengkapnya, lihat Buat disk penyimpanan di konsol Lightsail for Research dan Tambahkan penyimpanan ke komputer virtual di Lightsail for Research.

> **Note**
>
> Saat Anda memasang disk ke komputer virtual Anda menggunakan konsol, Lightsail for Research secara otomatis memformat dan memasang disk. Proses ini memakan waktu beberapa menit, jadi Anda harus mengonfirmasi bahwa disk telah mencapai status pemasangan yang dipasang sebelum Anda mulai menggunakannya. Secara default, Lightsail for Research memasang disk ke direktori. `/home/lightsail-user/<disk-name>` `<disk-name>`adalah nama yang Anda berikan pada disk Anda.

Langkah 3: Unggah dan unduh file

Anda dapat mengunggah file ke komputer JupyterLab virtual Anda, dan mengunduh file darinya. Untuk melakukannya, Anda harus menyelesaikan langkah-langkah berikut:

1. Dapatkan key pair dari Amazon Lightsail. Untuk informasi selengkapnya, lihat Dapatkan key pair untuk komputer virtual Lightsail for Research.
2. Setelah Anda memiliki key pair, Anda dapat menggunakannya untuk membuat koneksi menggunakan utilitas Secure Copy (SCP). SCP memungkinkan Anda mengunggah dan mengunduh file menggunakan Command Prompt atau Terminal. Untuk informasi selengkapnya, lihat Transfer file ke Lightsail untuk Penelitian komputer virtual menggunakan Secure Copy.
3. (Opsional) Anda juga dapat menggunakan key pair untuk terhubung ke komputer virtual Anda dengan SSH. Untuk informasi selengkapnya, lihat Connect ke komputer virtual Lightsail for Research menggunakan Secure Shell.

> **Note**
>
> Anda juga dapat mengakses antarmuka baris perintah komputer virtual Anda dan mentransfer file dengan menggunakan klien Amazon DCV berbasis browser. Amazon DCV tersedia di konsol Lightsail for Research. Untuk informasi selengkapnya, lihat Akses Lightsail for Research aplikasi komputer virtual dan Akses Lightsail for Research sistem operasi komputer virtual.

Untuk mengelola file proyek Anda dalam disk penyimpanan terlampir, pastikan untuk mengunggahnya ke direktori mount yang benar untuk disk yang terpasang. Saat Anda melampirkan disk ke komputer virtual Anda menggunakan konsol, Lightsail for Research secara otomatis memformat dan memasang disk ke direktori. `/home/lightsail-user/<disk-name>` *<disk-name>*adalah nama yang Anda berikan pada disk Anda.

Langkah 4: Luncurkan JupyterLab aplikasi

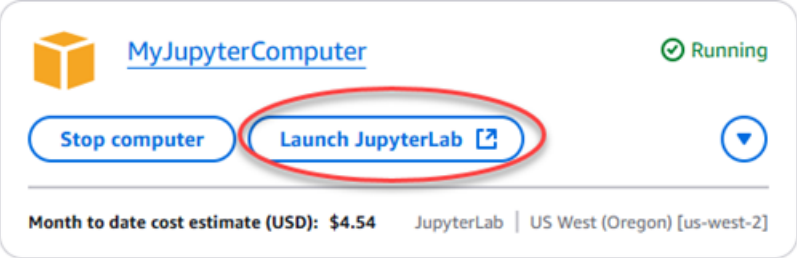
Selesaikan prosedur berikut untuk meluncurkan JupyterLab aplikasi di komputer virtual baru Anda.

> **Important**
>
> Jangan memperbarui sistem operasi atau JupyterLab aplikasi bahkan jika Anda diminta untuk melakukannya. Sebagai gantinya, pilih opsi untuk menutup atau mengabaikan petunjuk tersebut. Selain itu, jangan memodifikasi file apa pun yang ada di direktori /home/lightsail-admin/. Tindakan ini mungkin membuat komputer virtual tidak dapat digunakan.

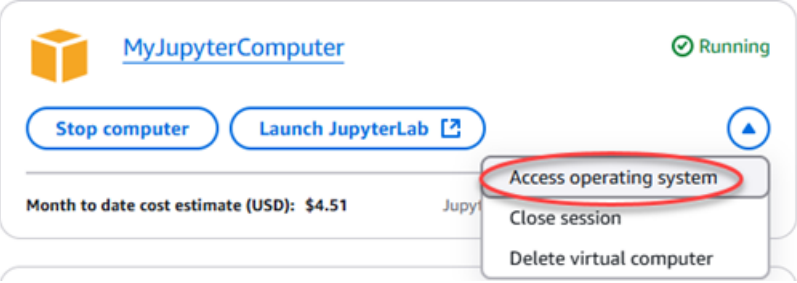
1. Masuk ke konsol Lightsail for Research.

2. Pilih Komputer virtual di panel navigasi untuk melihat komputer virtual yang tersedia di akun Anda.
3. Di halaman Komputer virtual, temukan komputer virtual Anda dan pilih salah satu opsi berikut untuk menghubungkannya:

   a. (Disarankan) Pilih Luncurkan JupyterLab untuk meluncurkan JupyterLab aplikasi dalam mode terfokus. Jika Anda belum terhubung ke komputer virtual Anda baru-baru ini, Anda mungkin harus menunggu beberapa menit sementara Lightsail for Research mempersiapkan sesi Anda.



   b. Pilih menu tarik-turun untuk komputer, lalu pilih Access sistem operasi untuk mengakses desktop komputer virtual Anda.

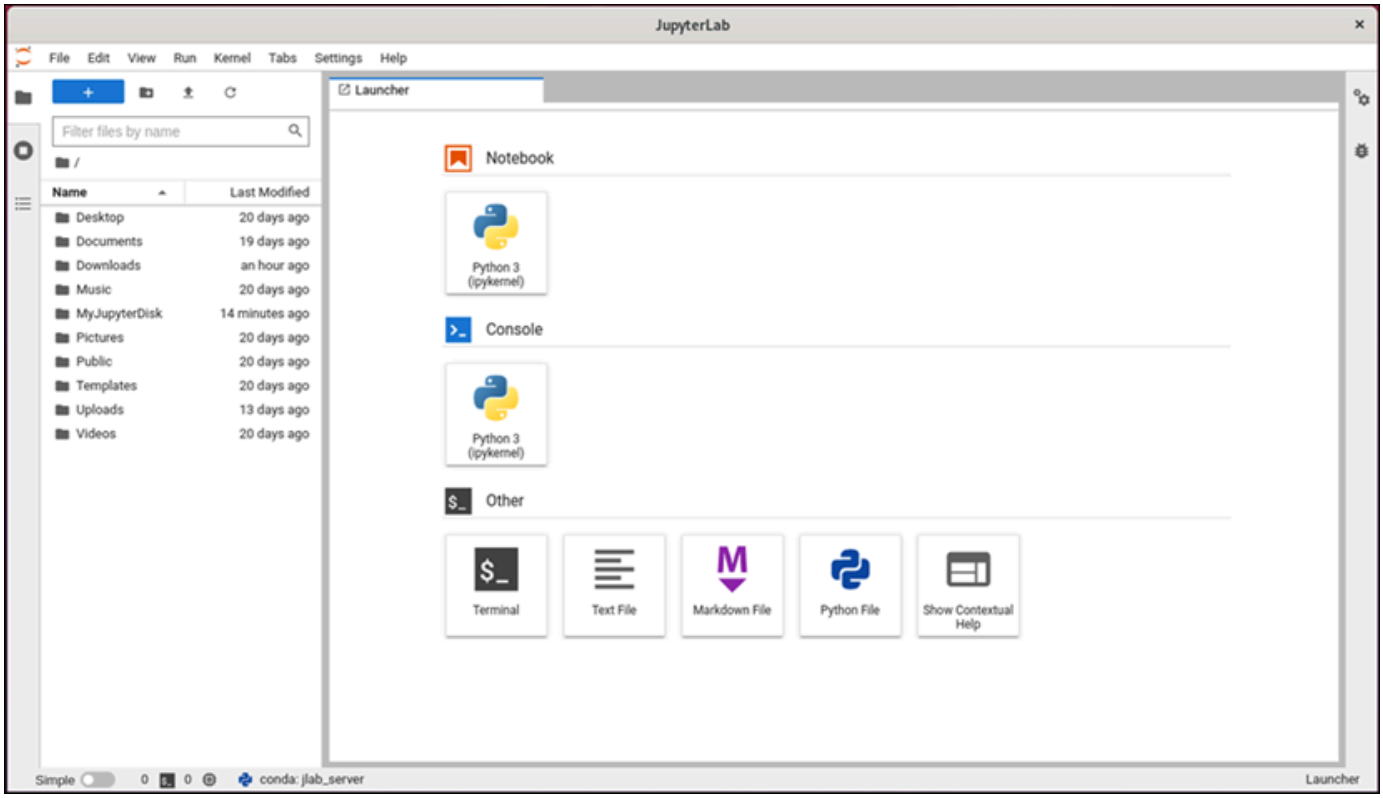


Lightsail for Research menjalankan beberapa perintah untuk memulai koneksi protokol tampilan jarak jauh. Setelah beberapa saat, jendela tab browser baru terbuka dengan koneksi desktop virtual yang dibuat ke komputer virtual Anda. Jika Anda memilih opsi Luncurkan aplikasi, lanjutkan ke langkah selanjutnya dari prosedur ini untuk membuka file di JupyterLab aplikasi. Jika Anda memilih opsi sistem operasi Access, Anda dapat membuka aplikasi lain melalui desktop Ubuntu.

> **Note**
>
> Browser Anda mungkin meminta Anda untuk mengotorisasi berbagi clipboard Anda. Memungkinkan ini memungkinkan Anda menyalin dan menempel antara komputer lokal Anda dan komputer virtual Anda.

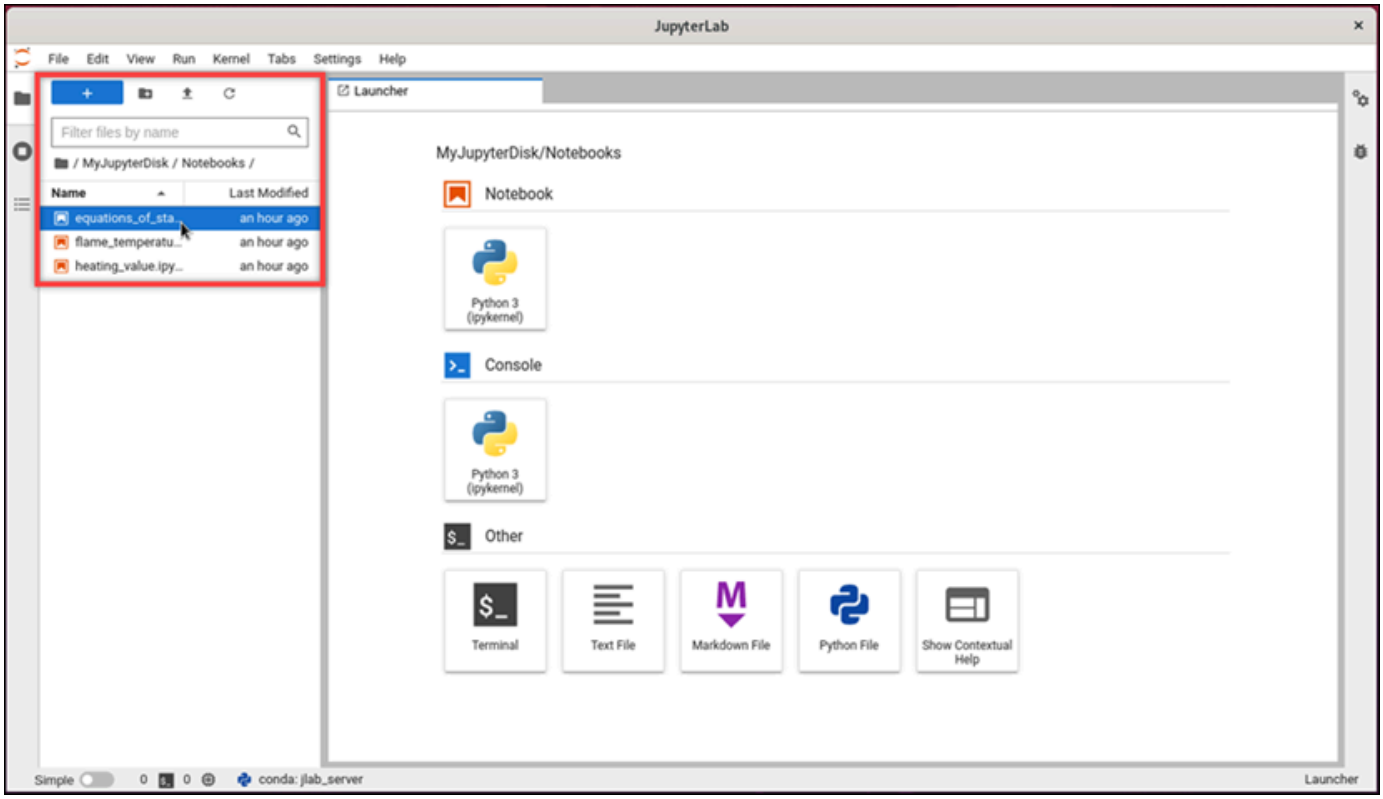
Ubuntu mungkin juga meminta Anda untuk pengaturan awal. Ikuti petunjuknya sampai Anda menyelesaikan pengaturan dan dapat menggunakan sistem operasi.

4. JupyterLab Aplikasi terbuka. Di menu peluncur, Anda dapat membuat notebook baru, meluncurkan konsol, meluncurkan terminal, dan membuat berbagai file.

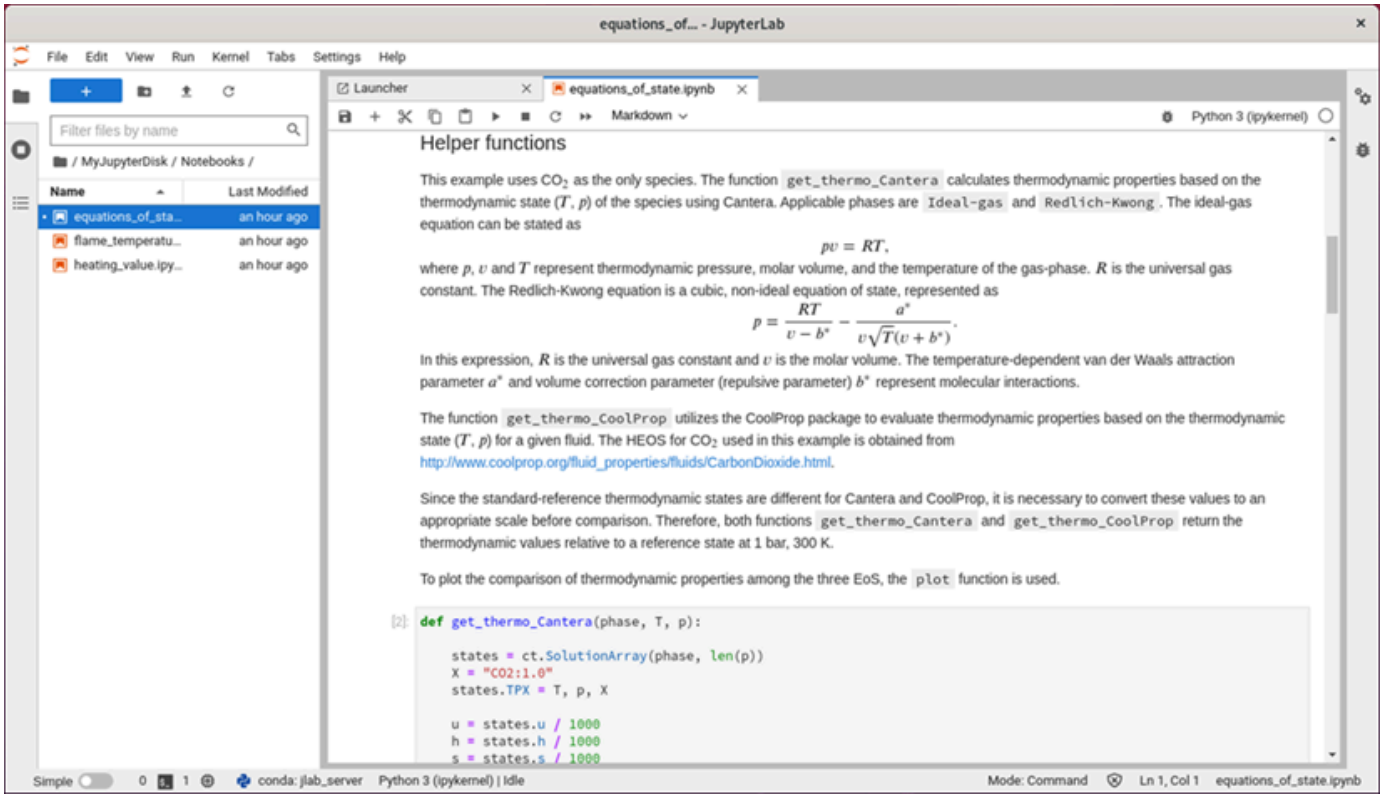


5. Untuk membuka file JupyterLab, di panel File Browser, pilih direktori atau folder tempat file proyek Anda disimpan. Kemudian pilih file yang akan dibuka.

   Jika Anda mengunggah file proyek Anda ke disk yang terpasang, cari direktori tempat disk dipasang. Secara default, Lightsail for Research memasang disk ke direktori. `/home/lightsail-user/<disk-name>` `<disk-name>`adalah nama yang Anda berikan pada disk Anda. Dalam contoh berikut, `MyJupyterDisk` direktori mewakili disk yang dipasang, dan `Notebooks` subdirektori berisi file notebook Jupyter kami.



Dalam contoh berikut, kami telah membuka file `equations_of_state.ipynb` notebook Jupyter.



Untuk informasi tentang cara memulai, lanjutkan ke Langkah 5: Baca JupyterLab dokumentasi bagian tutorial ini.

Langkah 5: Baca JupyterLab dokumentasi

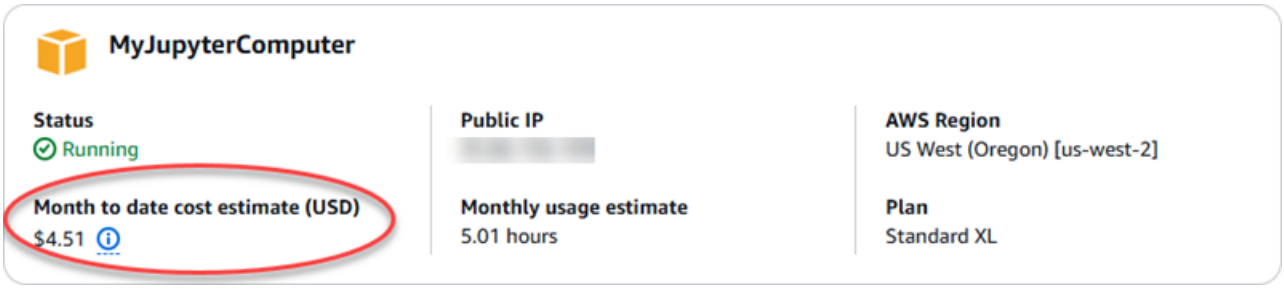
Jika Anda tidak terbiasa dengan JupyterLab, kami sarankan Anda membaca dokumentasi resmi mereka. Sumber daya JupyterLab online berikut tersedia:

- Dokumentasi JupyterLab
- Forum Wacana Jupyter
- JupyterLab pada StackOverflow
- JupyterLab pada GitHub

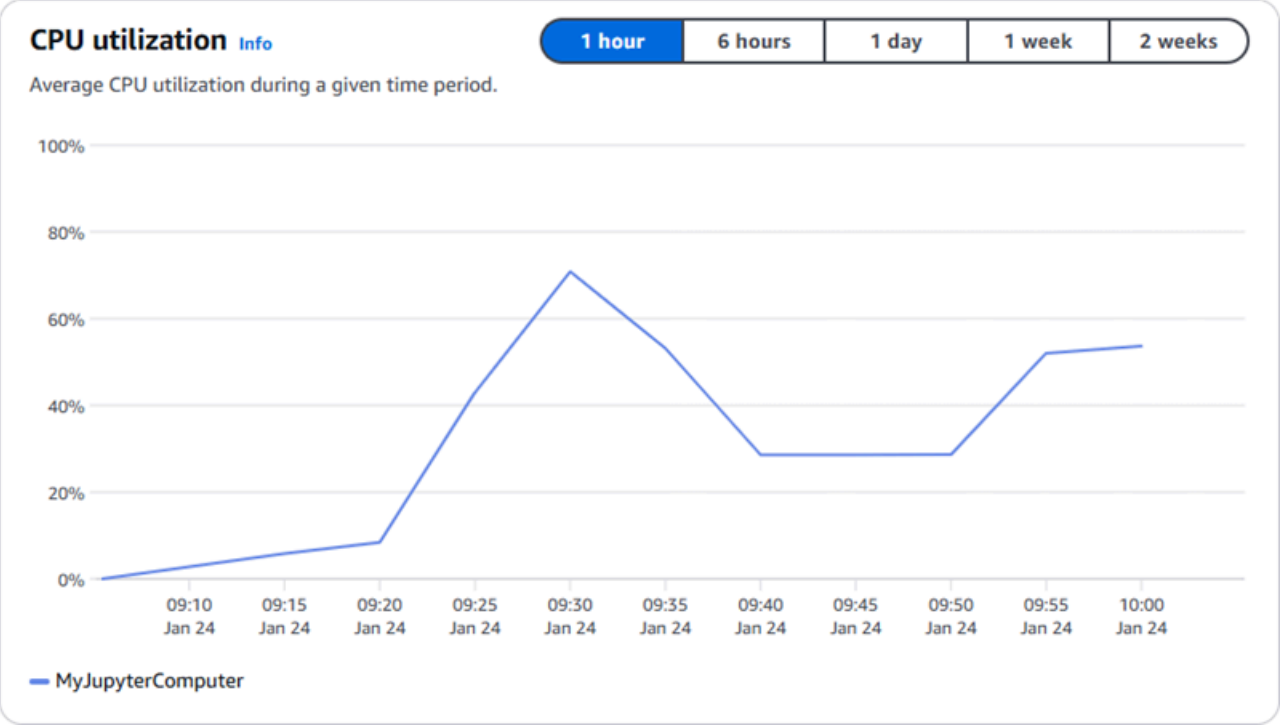
Langkah 6: (Opsional) Pantau penggunaan dan biaya

Perkiraan biaya dan penggunaan bulan hingga saat ini untuk sumber daya Lightsail for Research ditampilkan di area berikut di konsol Lightsail for Research.

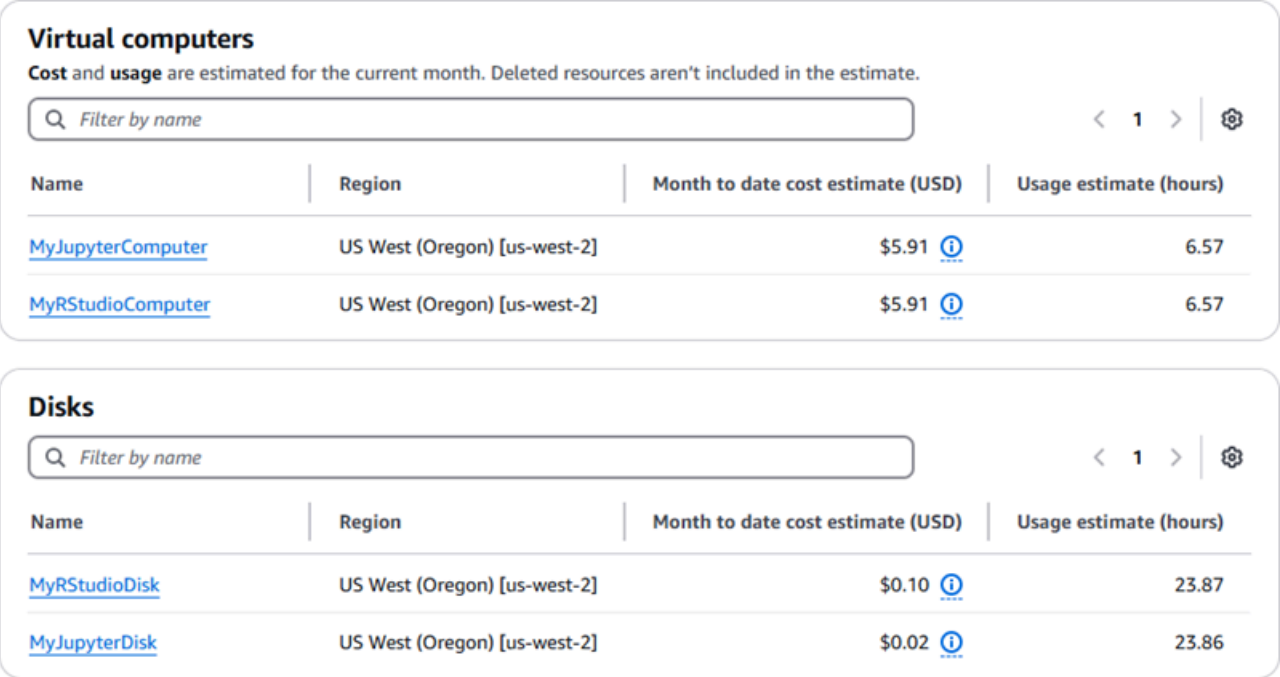
1. Pilih Komputer virtual di panel navigasi konsol Lightsail for Research. Perkiraan biaya bulan hingga saat ini untuk komputer virtual Anda tercantum di bawah setiap komputer virtual yang berjalan.



2. Untuk melihat pemanfaatan CPU untuk komputer virtual, pilih nama komputer virtual, lalu pilih tab Dasbor.



3. Untuk melihat perkiraan biaya dan penggunaan bulan hingga saat ini untuk semua sumber daya Lightsail for Research, pilih Penggunaan di panel navigasi.



Langkah 7: (Opsional) Buat aturan kontrol biaya

Kelola penggunaan dan biaya komputer virtual Anda dengan membuat aturan pengendalian biaya. Anda dapat membuat Stop komputer virtual pada aturan idle yang menghentikan komputer yang berjalan ketika mencapai persentase tertentu dari penggunaan CPU-nya selama periode tertentu. Misalnya, aturan dapat secara otomatis menghentikan komputer tertentu ketika pemanfaatan CPU-nya sama dengan atau kurang dari 5% selama periode 30 menit. Ini mungkin berarti bahwa komputer dalam keadaan idle, dan Lightsail for Research menghentikan komputer sehingga Anda tidak dikenakan biaya untuk sumber daya idle.

> **Important**
>
> Sebelum Anda membuat aturan untuk menghentikan komputer virtual Anda saat idle, kami sarankan untuk memantau pemanfaatan CPU-nya selama beberapa hari. Perhatikan pemanfaatan CPU saat komputer virtual Anda berada di bawah beban yang berbeda. Misalnya, saat mengkompilasi kode, memproses operasi, dan idling. Ini akan membantu Anda menentukan ambang batas yang akurat untuk aturan tersebut. Untuk informasi lebih lanjut, lihat Langkah 6: (Opsional) Pantau penggunaan dan biaya bagian tutorial ini. Jika Anda membuat aturan dengan ambang batas penggunaan CPU yang lebih tinggi dari beban kerja Anda, aturan tersebut dapat menghentikan komputer virtual Anda secara berurutan. Misalnya, jika Anda memulai komputer virtual Anda segera setelah aturan menghentikannya, aturan diaktifkan kembali dan komputer berhenti lagi.

Petunjuk terperinci untuk membuat, dan mengelola aturan pengendalian biaya dapat ditemukan di panduan berikut:

- Mengelola aturan pengendalian biaya di Lightsail for Research
- Buat aturan kontrol biaya untuk Lightsail for Research komputer virtual
- Hapus aturan kontrol biaya untuk Lightsail for Research komputer virtual

Langkah 8: (Opsional) Buat snapshot

Snapshot adalah point-in-time salinan data Anda. Anda dapat membuat snapshot dari komputer virtual Anda dan menggunakannya sebagai garis dasar untuk membuat komputer baru atau untuk cadangan data. Snapshot berisi semua data yang diperlukan untuk memulihkan komputer Anda (dari saat snapshot diambil).

Instruksi terperinci untuk membuat, dan mengelola snapshot dapat ditemukan di panduan berikut:

- Buat snapshot dari Lightsail for Research komputer virtual atau disk
- Lihat dan kelola snapshot komputer dan disk virtual di Lightsail for Research
- Buat komputer virtual atau disk dari snapshot
- Menghapus snapshot di konsol Lightsail for Research

Langkah 9: (Opsional) Hentikan atau hapus komputer virtual Anda

Setelah Anda selesai dengan komputer virtual yang Anda buat untuk tutorial ini, Anda dapat menghapusnya. Ini berhenti menimbulkan biaya untuk komputer virtual jika Anda tidak membutuhkannya.

Menghapus komputer virtual tidak menghapus snapshot terkait atau disk terlampir. Jika Anda membuat snapshot dan disk, Anda harus menghapusnya secara manual untuk menghentikan biaya untuk mereka.

Untuk menyimpan komputer virtual Anda untuk nanti, tetapi untuk menghindari dikenakan biaya dengan harga per jam standar, Anda dapat menghentikan komputer virtual alih-alih menghapusnya. Kemudian Anda bisa memulainya lagi nanti. Untuk informasi selengkapnya, lihat Lihat Lightsail for Research detail komputer virtual. Untuk informasi selengkapnya tentang harga, lihat harga Lightsail for Research.

> **Important**
>
> Menghapus sumber daya Lightsail for Research adalah tindakan permanen. Data yang dihapus tidak dapat dipulihkan. Jika Anda mungkin memerlukan data nanti, buat snapshot komputer virtual Anda sebelum Anda menghapusnya. Untuk informasi selengkapnya, lihat Membuat snapshot.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi.
3. Pilih komputer virtual yang akan dihapus.
4. Pilih Tindakan, lalu pilih Hapus komputer virtual.
5. Ketik konfirmasi di blok teks. Kemudian, pilih Hapus komputer virtual.

Luncurkan dan gunakan RStudio pada Lightsail untuk Penelitian

Dalam tutorial ini, kami menunjukkan kepada Anda cara memulai mengelola dan menggunakan komputer RStudio virtual Anda di Amazon Lightsail for Research.

> **Note**
>
> Tutorial mendalam untuk memulai dengan Lightsail for Research RStudio dan dipublikasikan ke AWS Blog Sektor Publik. Untuk informasi selengkapnya, lihat Memulai Amazon Lightsail for Research: Tutorial menggunakan. RStudio

Topik

Langkah 1: Selesaikan prasyarat

Buat komputer virtual menggunakan RStudio aplikasi jika Anda belum melakukannya. Untuk informasi selengkapnya, lihat Buat Lightsail untuk Penelitian komputer virtual.

Langkah 2: (Opsional) Tambahkan ruang penyimpanan

Komputer virtual Anda dilengkapi dengan disk sistem. Namun, karena kebutuhan penyimpanan Anda berubah, Anda dapat melampirkan disk tambahan ke komputer virtual Anda untuk menambah ruang penyimpanannya.

Anda juga dapat menyimpan file kerja Anda ke disk yang terpasang. Kemudian Anda dapat melepaskan disk dan melampirkannya ke komputer virtual yang berbeda untuk memindahkan file Anda dengan cepat dari satu komputer ke komputer lain.

Atau, Anda dapat membuat snapshot dari disk terlampir yang memiliki file kerja Anda, dan kemudian membuat disk duplikat dari snapshot. Kemudian Anda dapat melampirkan disk duplikat baru ke komputer lain untuk menduplikasi pekerjaan Anda di komputer virtual yang berbeda. Untuk informasi selengkapnya, lihat Buat disk penyimpanan di konsol Lightsail for Research dan Tambahkan penyimpanan ke komputer virtual di Lightsail for Research.

> **Note**
>
> Saat Anda memasang disk ke komputer virtual Anda menggunakan konsol, Lightsail for Research secara otomatis memformat dan memasang disk. Proses ini memakan waktu beberapa menit, jadi Anda harus mengonfirmasi bahwa disk telah mencapai status pemasangan yang dipasang sebelum Anda mulai menggunakannya. Secara default, Lightsail for Research memasang disk ke `/home/lightsail-user/<disk-name>` direktori adalah nama yang Anda berikan pada disk Anda.

Langkah 3: Unggah dan unduh file

Anda dapat mengunggah file ke komputer RStudio virtual Anda, dan mengunduh file darinya. Untuk melakukannya, Anda harus menyelesaikan langkah-langkah berikut:

1. Dapatkan key pair dari Amazon Lightsail. Untuk informasi selengkapnya, lihat Dapatkan key pair untuk komputer virtual Lightsail for Research.
2. Setelah Anda memiliki key pair, Anda dapat menggunakannya untuk membuat koneksi menggunakan utilitas Secure Copy (SCP). SCP memungkinkan Anda mengunggah dan mengunduh file menggunakan Command Prompt atau Terminal. Untuk informasi selengkapnya, lihat Transfer file ke Lightsail untuk Penelitian komputer virtual menggunakan Secure Copy.
3. (Opsional) Anda juga dapat menggunakan key pair untuk terhubung ke komputer virtual Anda dengan SSH. Untuk informasi selengkapnya, lihat Connect ke komputer virtual Lightsail for Research menggunakan Secure Shell.

> **Note**
>
> Anda juga dapat mengakses antarmuka baris perintah komputer virtual Anda dan mentransfer file dengan menggunakan klien Amazon DCV berbasis browser. Amazon DCV tersedia di konsol Lightsail for Research. Untuk informasi selengkapnya, lihat Akses Lightsail for Research aplikasi komputer virtual dan Akses Lightsail for Research sistem operasi komputer virtual.

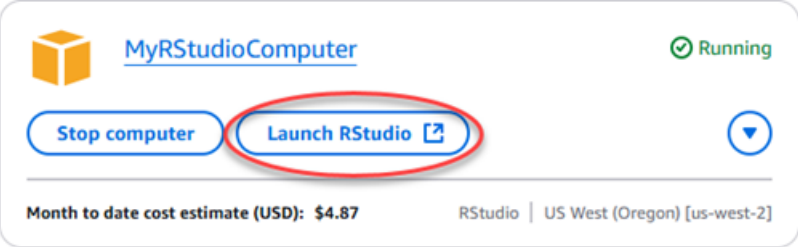
Langkah 4: Luncurkan RStudio aplikasi

Selesaikan prosedur berikut untuk meluncurkan RStudio aplikasi di komputer virtual baru Anda.

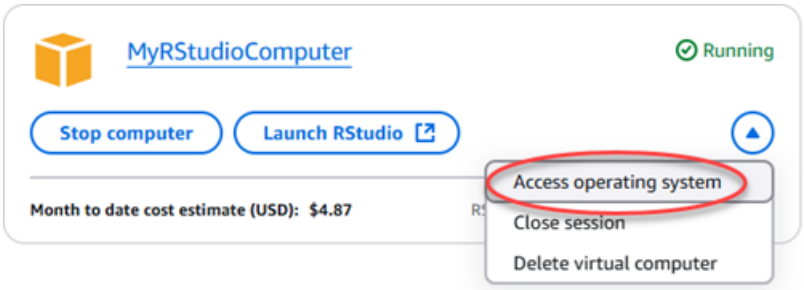
> **Important**
>
> Jangan memperbarui sistem operasi atau RStudio aplikasi bahkan jika Anda diminta untuk melakukannya. Sebagai gantinya, pilih opsi untuk menutup atau mengabaikan petunjuk tersebut. Selain itu, jangan memodifikasi file apa pun yang ada di direktori /home/lightsail-admin/. Tindakan ini mungkin membuat komputer virtual tidak dapat digunakan.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi untuk melihat komputer virtual yang tersedia di akun Anda.
3. Di halaman Komputer virtual, temukan komputer virtual Anda dan pilih salah satu opsi berikut untuk menghubungkannya:

   a. (Disarankan) Pilih Luncurkan RStudio untuk meluncurkan RStudio aplikasi dalam mode terfokus. Jika Anda belum terhubung ke komputer virtual Anda baru-baru ini, Anda mungkin harus menunggu beberapa menit sementara Lightsail for Research mempersiapkan sesi Anda.



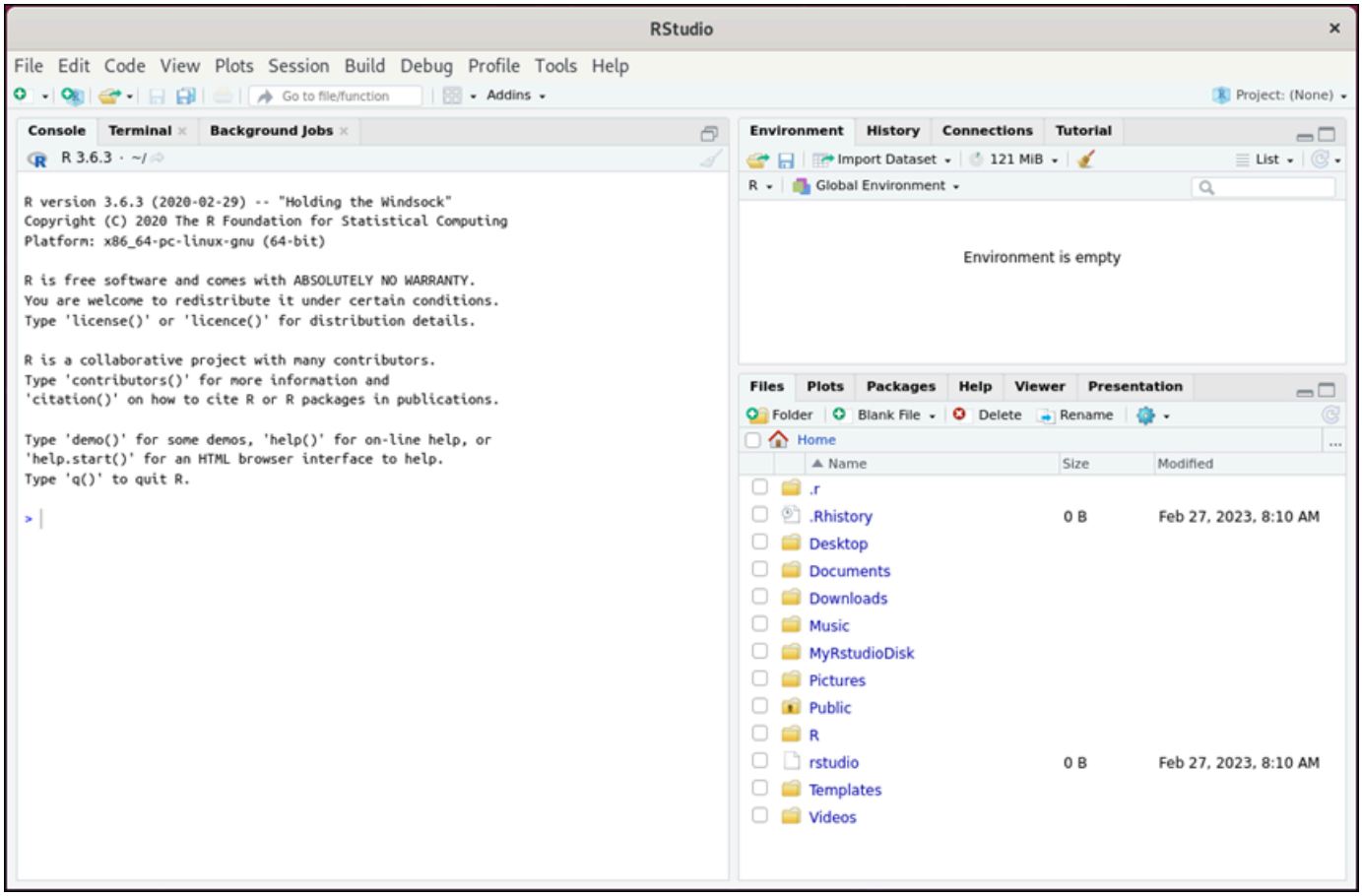
b. Pilih menu tarik-turun untuk komputer, lalu pilih Access sistem operasi untuk mengakses desktop komputer virtual Anda. Lakukan ini jika Anda ingin menginstal aplikasi yang berbeda pada sistem operasi.



Lightsail for Research menjalankan beberapa perintah untuk memulai koneksi protokol tampilan jarak jauh. Setelah beberapa saat, jendela tab browser baru terbuka dengan koneksi desktop virtual yang dibuat ke komputer virtual Anda. Jika Anda memilih opsi Luncurkan aplikasi, lanjutkan ke langkah selanjutnya dari prosedur ini untuk membuka file di RStudio aplikasi. Jika Anda memilih opsi sistem operasi Access, Anda dapat membuka aplikasi lain melalui desktop Ubuntu.

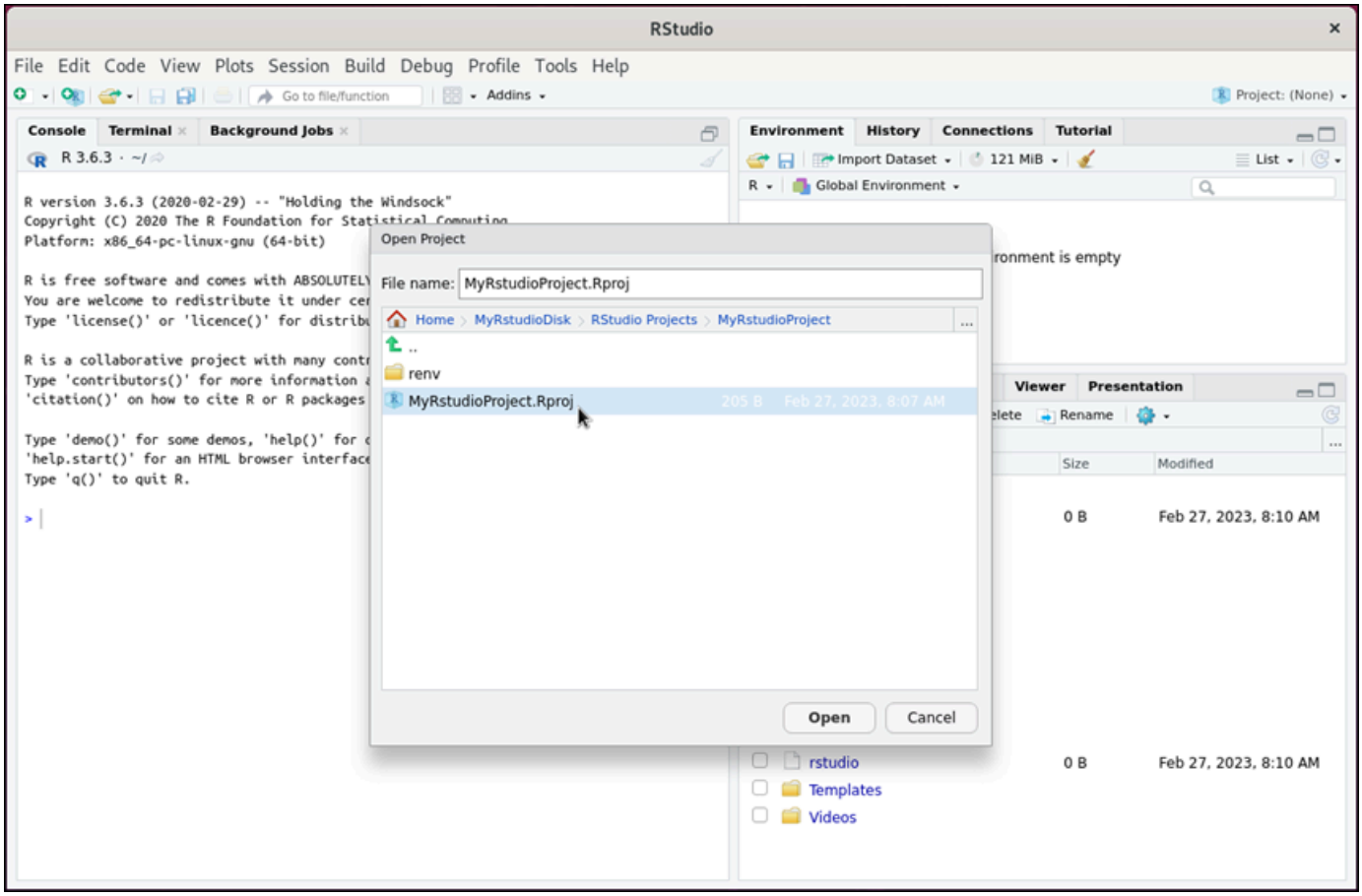
> **Note**
>
> Browser Anda mungkin meminta Anda untuk mengotorisasi berbagi clipboard Anda. Memungkinkan ini memungkinkan Anda menyalin dan menempel antara komputer lokal Anda dan komputer virtual Anda.
> Ubuntu mungkin juga meminta Anda untuk pengaturan awal. Ikuti petunjuknya sampai Anda menyelesaikan pengaturan dan dapat menggunakan sistem operasi.

4. RStudio Aplikasi terbuka.

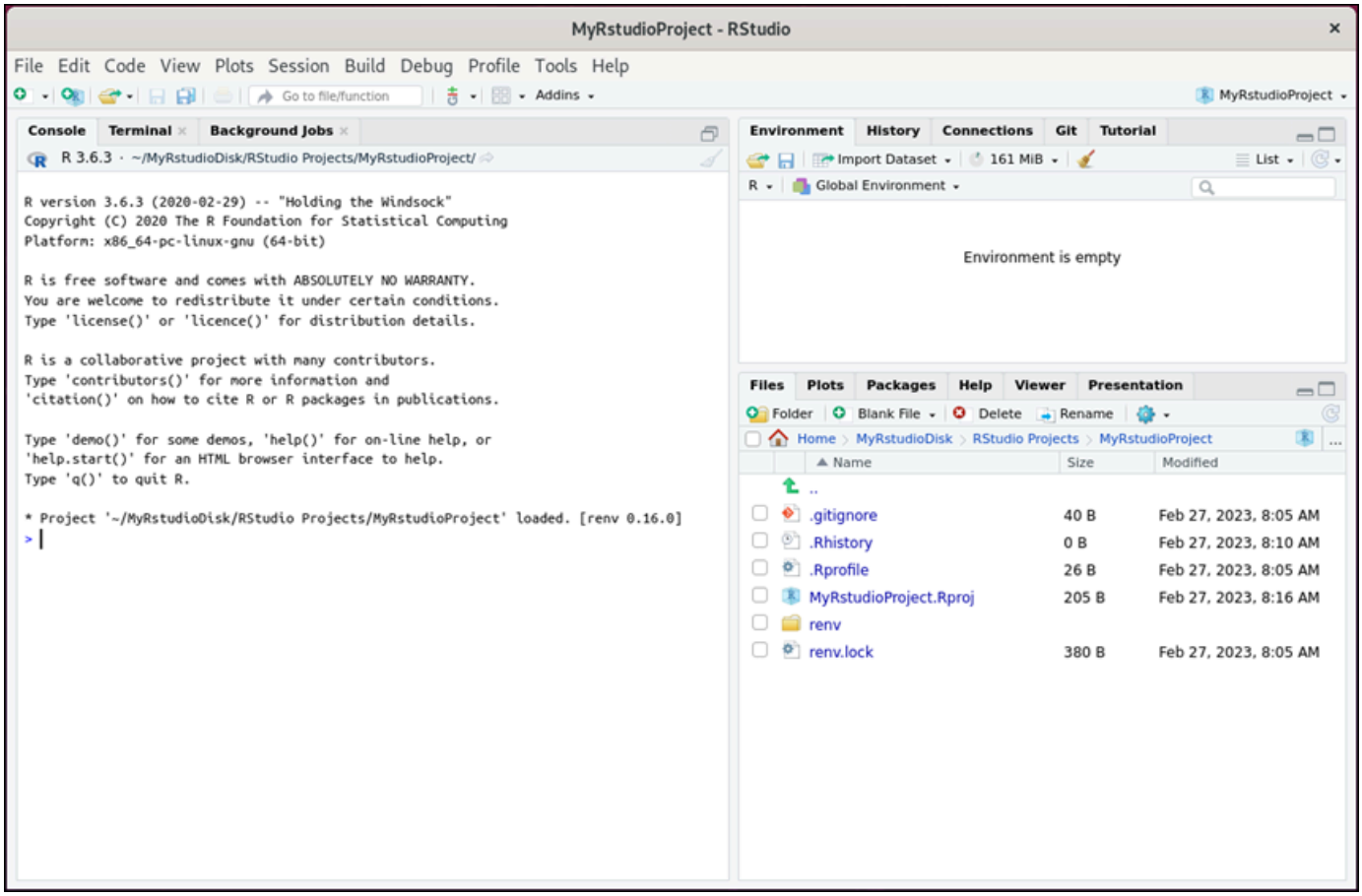


5. Untuk membuka proyek RStudio, pilih menu File, lalu pilih Open project. Jelajahi direktori atau folder tempat file proyek Anda disimpan. Kemudian pilih file yang akan dibuka.

   Jika Anda mengunggah file proyek Anda ke disk yang terpasang, cari direktori tempat disk dipasang. Secara default, Lightsail for Research memasang disk ke direktori. `/home/lightsail-user/<disk-name>` *<disk-name>*adalah nama yang Anda berikan pada disk Anda. Dalam contoh berikut, `MyRstudioDisk` direktori mewakili disk yang dipasang, dan `Projects` subdirektori berisi file RStudio proyek kami.



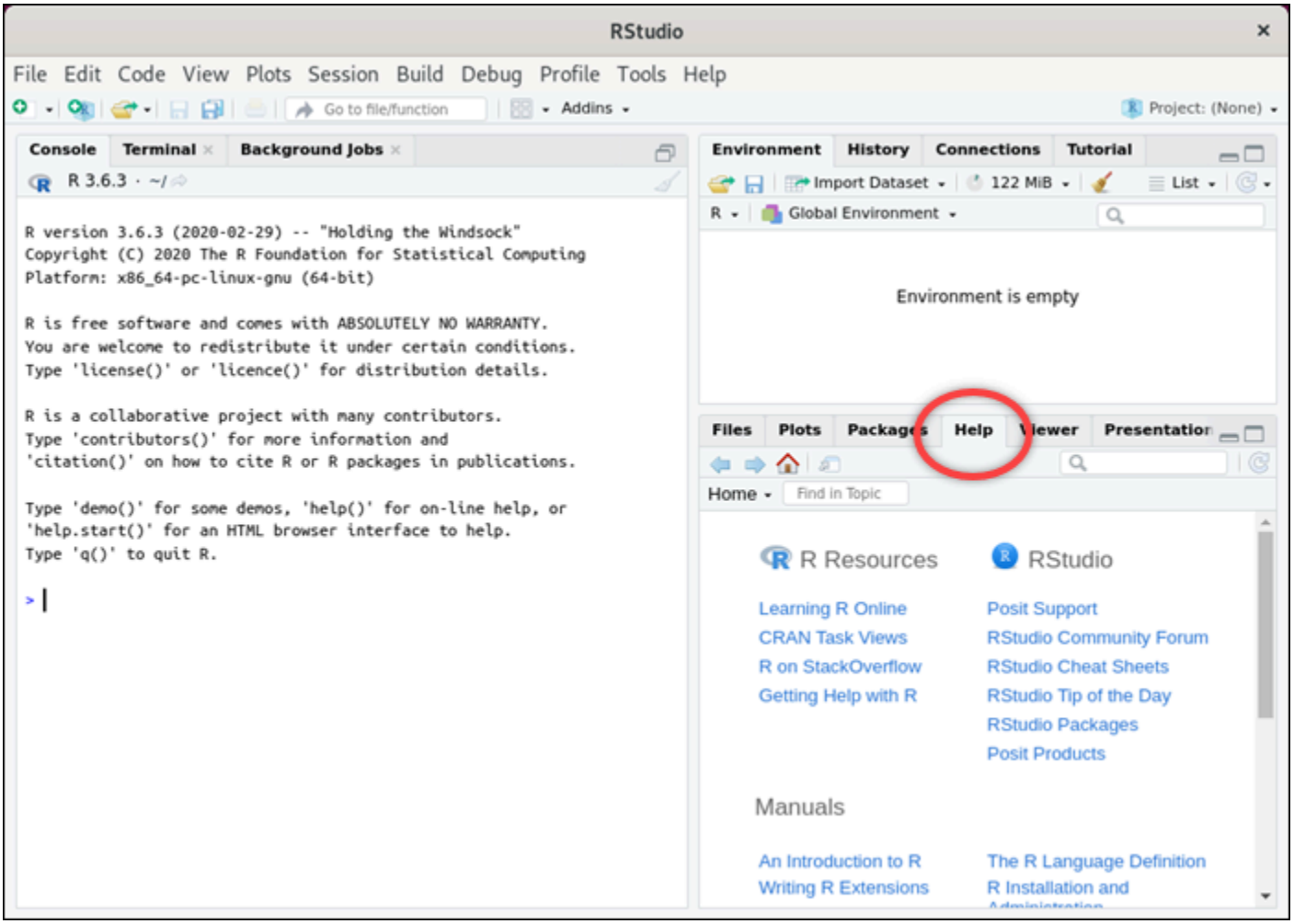
Dalam contoh berikut, kami telah membuka file `MyRstudioProject.Rproj` proyek.



Untuk informasi tentang cara memulai RStudio, lanjutkan ke Langkah 5: Baca RStudio dokumentasi bagian tutorial ini.

Langkah 5: Baca RStudio dokumentasi

RStudio Aplikasi ini dibundel dengan paket dokumentasi yang komprehensif. Untuk memulai pembelajaran RStudio, sebaiknya Anda mengakses tab Bantuan RStudio seperti yang ditunjukkan pada contoh berikut.



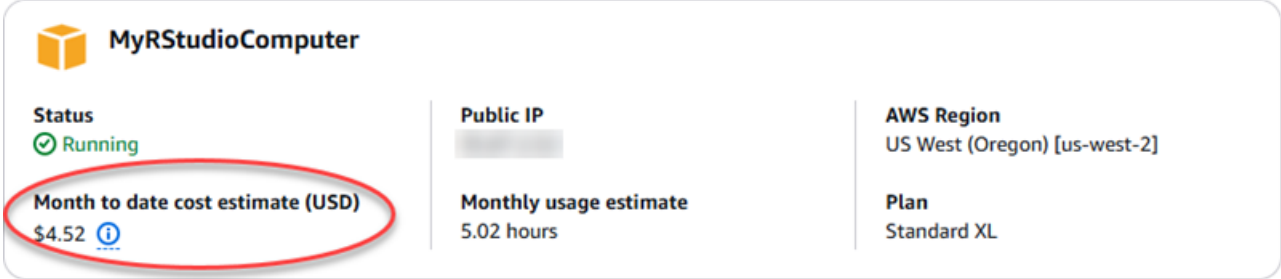
Sumber daya RStudio online berikut juga tersedia:

- Belajar R Online
- R pada StackOverflow
- Mendapatkan Bantuan dengan R
- Support Posit
- RStudioForum Komunitas
- RStudio Lembar Cheat
- RStudio Tip Hari Ini (Twitter)
- RStudioPaket

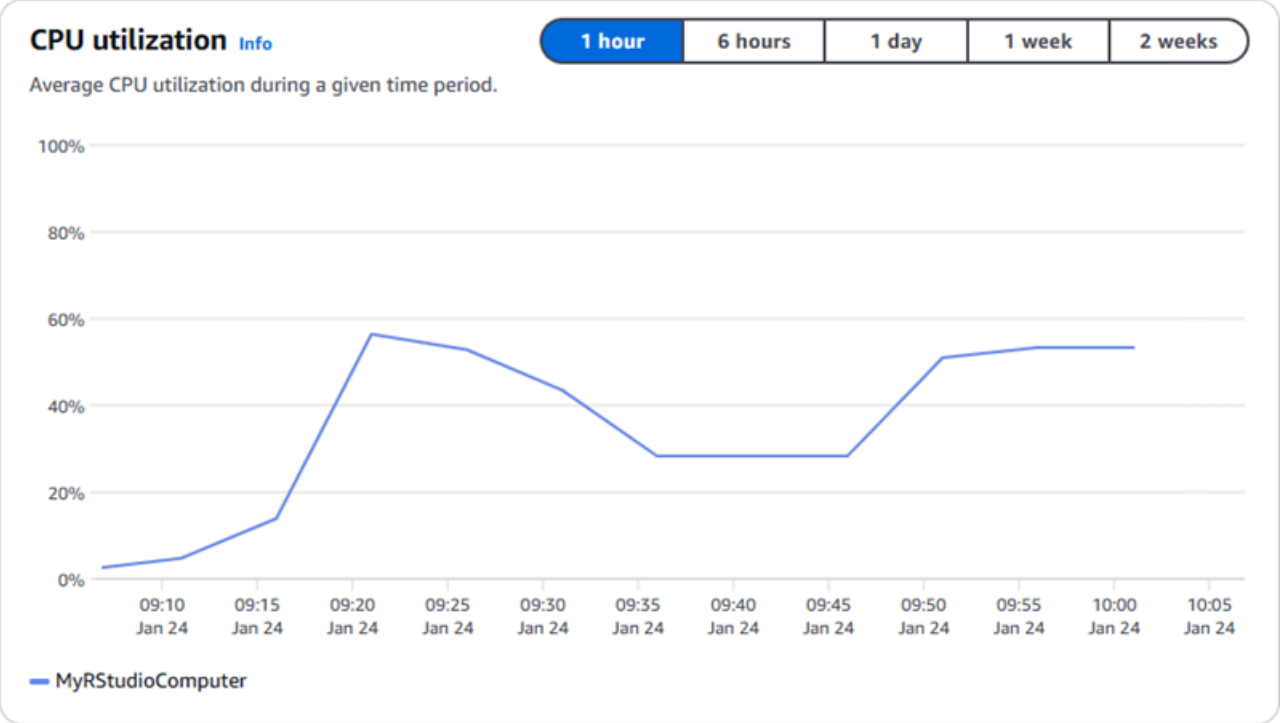
Langkah 6: (Opsional) Pantau penggunaan dan biaya

Perkiraan biaya dan penggunaan bulan hingga saat ini untuk sumber daya Lightsail for Research ditampilkan di area berikut di konsol Lightsail for Research.

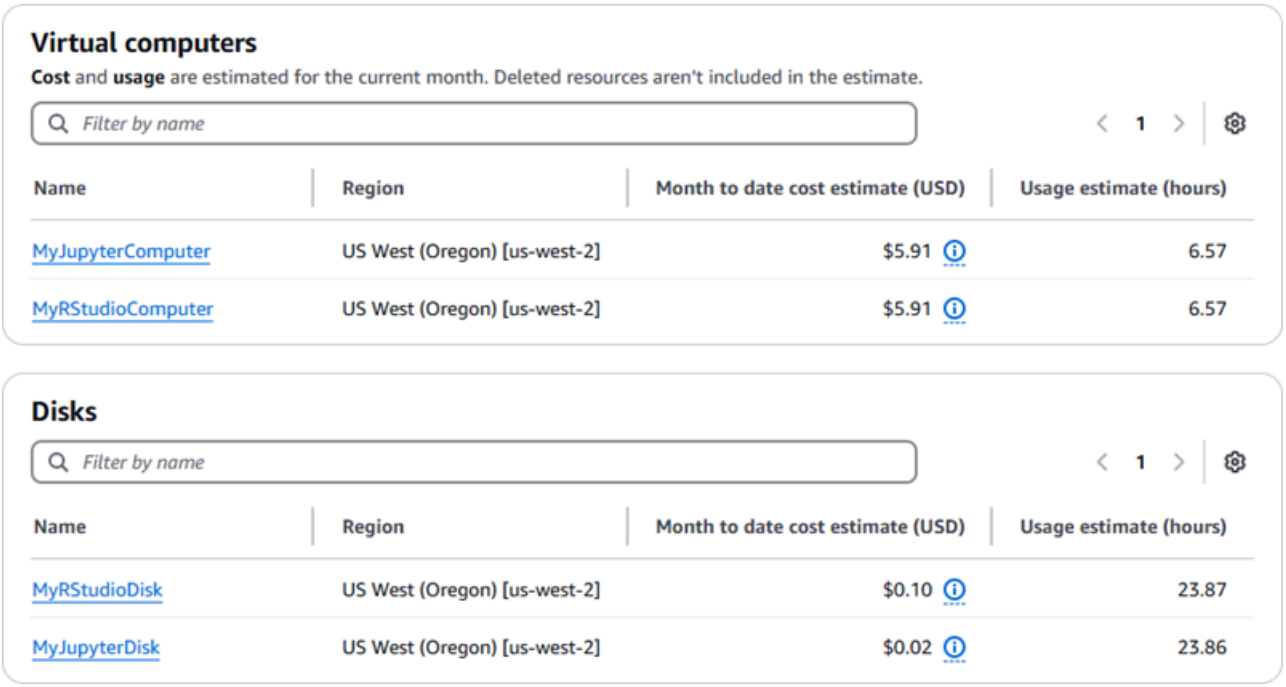
1. Pilih Komputer virtual di panel navigasi konsol Lightsail for Research. Perkiraan biaya bulan hingga saat ini untuk komputer virtual Anda tercantum di bawah setiap komputer virtual yang berjalan.



2. Untuk melihat pemanfaatan CPU untuk komputer virtual, pilih nama komputer virtual, lalu pilih tab Dasbor.



3. Untuk melihat perkiraan biaya dan penggunaan bulan hingga saat ini untuk semua sumber daya Lightsail for Research, pilih Penggunaan di panel navigasi.



Langkah 7: (Opsional) Buat aturan kontrol biaya

Kelola penggunaan dan biaya komputer virtual Anda dengan membuat aturan pengendalian biaya. Anda dapat membuat Stop komputer virtual pada aturan idle yang menghentikan komputer yang berjalan ketika mencapai persentase tertentu dari penggunaan CPU-nya selama periode tertentu. Misalnya, aturan dapat secara otomatis menghentikan komputer tertentu ketika pemanfaatan CPU-nya sama dengan atau kurang dari 5% selama periode 30 menit. Ini mungkin berarti bahwa komputer dalam keadaan idle, dan Lightsail for Research menghentikan komputer sehingga Anda tidak dikenakan biaya untuk sumber daya idle.

> **Important**
>
> Sebelum Anda membuat aturan untuk menghentikan komputer virtual Anda saat idle, kami sarankan untuk memantau pemanfaatan CPU-nya selama beberapa hari. Perhatikan pemanfaatan CPU saat komputer virtual Anda berada di bawah beban yang berbeda. Misalnya, saat mengkompilasi kode, memproses operasi, dan idling. Ini akan membantu Anda menentukan ambang batas yang akurat untuk aturan tersebut. Untuk informasi lebih lanjut, lihat Langkah 6: (Opsional) Pantau penggunaan dan biaya bagian tutorial ini.
> Jika Anda membuat aturan dengan ambang batas penggunaan CPU yang lebih tinggi dari beban kerja Anda, aturan tersebut dapat menghentikan komputer virtual Anda secara

berurutan. Misalnya, jika Anda memulai komputer virtual Anda segera setelah aturan menghentikannya, aturan diaktifkan kembali dan komputer berhenti lagi.

Petunjuk terperinci untuk membuat, dan mengelola aturan pengendalian biaya dapat ditemukan di panduan berikut:

- Mengelola aturan pengendalian biaya di Lightsail for Research
- Buat aturan kontrol biaya untuk Lightsail for Research komputer virtual
- Hapus aturan kontrol biaya untuk Lightsail for Research komputer virtual

Langkah 8: (Opsional) Buat snapshot

Snapshot adalah point-in-time salinan data Anda. Anda dapat membuat snapshot dari komputer virtual Anda dan menggunakannya sebagai garis dasar untuk membuat komputer baru atau untuk cadangan data. Snapshot berisi semua data yang diperlukan untuk memulihkan komputer Anda (dari saat snapshot diambil).

Instruksi terperinci untuk membuat, dan mengelola snapshot dapat ditemukan di panduan berikut:

- Buat snapshot dari Lightsail for Research komputer virtual atau disk
- Lihat dan kelola snapshot komputer dan disk virtual di Lightsail for Research
- Buat komputer virtual atau disk dari snapshot
- Menghapus snapshot di konsol Lightsail for Research

Langkah 9: (Opsional) Hentikan atau hapus komputer virtual Anda

Setelah Anda selesai dengan komputer virtual yang Anda buat untuk tutorial ini, Anda dapat menghapusnya. Ini berhenti menimbulkan biaya untuk komputer virtual jika Anda tidak membutuhkannya.

Menghapus komputer virtual tidak menghapus snapshot terkait atau disk terlampir. Jika Anda membuat snapshot dan disk, Anda harus menghapusnya secara manual untuk menghentikan biaya untuk mereka.

Untuk menyimpan komputer virtual Anda untuk nanti, tetapi untuk menghindari dikenakan biaya dengan harga per jam standar, Anda dapat menghentikan komputer virtual alih-alih menghapusnya.

Kemudian Anda bisa memulainya lagi nanti. Untuk informasi selengkapnya, lihat Lihat Lightsail for Research detail komputer virtual. Untuk informasi selengkapnya tentang harga, lihat harga Lightsail for Research.

> **Important**
>
> Menghapus sumber daya Lightsail for Research adalah tindakan permanen. Data yang dihapus tidak dapat dipulihkan. Jika Anda mungkin memerlukan data nanti, buat snapshot komputer virtual Anda sebelum Anda menghapusnya. Untuk informasi selengkapnya, lihat Membuat snapshot.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi.
3. Pilih komputer virtual yang akan dihapus.
4. Pilih Tindakan, lalu pilih Hapus komputer virtual.
5. Ketik konfirmasi di blok teks. Kemudian, pilih Hapus komputer virtual.

Membuat dan mengelola komputer virtual di Lightsail untuk Penelitian

Dengan Amazon Lightsail for Research, Anda dapat membuat komputer virtual di. AWS Cloud

Saat Anda membuat komputer virtual, Anda memilih aplikasi dan rencana perangkat keras untuk digunakan. Anda dapat menetapkan batas pengeluaran untuk komputer virtual Anda, dan memilih apa yang terjadi ketika komputer virtual mencapai batas itu. Misalnya, Anda dapat memilih untuk menghentikan komputer virtual secara otomatis sehingga Anda tidak dikenakan biaya lebih dari anggaran yang dikonfigurasi.

> **Important**
>
> Pada 22 Maret 2024, komputer virtual Lightsail for Research akan IMDSv2 diberlakukan secara default.

Topik

Pilih gambar aplikasi dan paket perangkat keras untuk Lightsail for Research

Saat Anda membuat komputer virtual Amazon Lightsail for Research, Anda memilih aplikasi dan paket perangkat keras (paket) untuknya.

Aplikasi menyediakan konfigurasi perangkat lunak (misalnya, aplikasi dan sistem operasi). Sebuah rencana menyediakan perangkat keras komputer virtual, seperti jumlah vCPUs, memori, ruang penyimpanan, dan tunjangan transfer data bulanan. Bersama-sama, aplikasi dan rencana membentuk konfigurasi komputer virtual.

> **Note**
>
> Anda tidak dapat mengubah aplikasi atau paket komputer virtual Anda setelah dibuat. Namun, Anda dapat membuat snapshot dari komputer virtual, dan kemudian memilih paket baru saat membuat komputer virtual baru dari snapshot. Untuk informasi selengkapnya tentang snapshot, lihatBackup komputer virtual dan disk dengan snapshot Lightsail for Research.

Topik

Aplikasi

Amazon Lightsail for Research menyediakan dan mengelola gambar mesin yang berisi aplikasi dan sistem operasi yang diperlukan untuk meluncurkan komputer virtual. Anda memilih dari daftar aplikasi saat Anda membuat komputer virtual di Lightsail for Research. Semua gambar aplikasi Lightsail for Research menggunakan sistem operasi Ubuntu (Linux).

Aplikasi berikut tersedia di Lightsail for Research:

- JupyterLab— JupyterLab adalah Integrated Development Environment (IDE) berbasis web untuk notebook, kode, dan data. Dengan antarmuka yang fleksibel, Anda dapat mengonfigurasi dan mengatur alur kerja dalam ilmu data, komputasi ilmiah, jurnalisme komputasi, dan pembelajaran mesin. Untuk informasi selengkapnya, lihat Dokumentasi Proyek Jupyter.

- RStudio— RStudio adalah open source Integrated Development Environment (IDE) untuk R, bahasa pemrograman untuk komputasi statistik dan grafik, dan Python. Ini menggabungkan editor kode sumber, membangun alat otomatisasi dan debugger, serta alat untuk merencanakan dan manajemen ruang kerja. Untuk informasi lebih lanjut, lihat RStudioIDE.
- VSCodium— VSCodium adalah distribusi biner berbasis komunitas dari editor Microsoft VS Code. Untuk informasi selengkapnya, lihat VSCodium.
- Scilab — Scilab adalah paket komputasi numerik open source, dan bahasa pemrograman berorientasi numerik tingkat tinggi. Untuk informasi lebih lanjut, lihat Scilab.
- Ubuntu 20.04 LTS — Ubuntu adalah distribusi Linux open source berbasis Debian. Lean, cepat dan kuat, Ubuntu Server memberikan layanan yang andal, dapat diprediksi, dan ekonomis. Ini adalah dasar yang bagus untuk membangun komputer virtual Anda. Untuk informasi selengkapnya, lihat rilis Ubuntu.

Rencana

Paket menyediakan spesifikasi perangkat keras dan menentukan harga untuk komputer virtual Lightsail for Research Anda. Paket mencakup jumlah memori tetap (RAM), komputasi (vCPUs), ruang volume penyimpanan (disk) berbasis SSD, dan tunjangan transfer data bulanan. Paket dibebankan setiap jam, berdasarkan permintaan, jadi Anda hanya membayar waktu komputer virtual Anda berjalan.

Rencana yang Anda pilih mungkin bergantung pada sumber daya yang dibutuhkan beban kerja Anda. Lightsail for Research menawarkan jenis paket berikut:

- Standar — Paket standar dioptimalkan untuk komputasi dan ideal untuk aplikasi terikat komputasi yang mendapat manfaat dari prosesor berkinerja tinggi.
- GPU - Paket GPU menyediakan platform berkinerja tinggi yang hemat biaya untuk komputasi GPU tujuan umum. Anda dapat menggunakan rencana ini untuk mempercepat aplikasi dan beban kerja ilmiah, teknik, dan rendering.

Paket standar

Berikut ini adalah spesifikasi perangkat keras dari paket standar yang tersedia di Lightsail for Research.

Nama rencana	v CPUs	Memori	Ruang penyimpanan	Tunjangan transfer data bulanan
Standar XL	4	8 GB	50 GB	512 GB
Standar 2XL	8	16 GB	50 GB	512 GB
Standar 4XL	16	32 GB	50 GB	512 GB

Paket GPU

Berikut ini adalah spesifikasi perangkat keras dari paket GPU yang tersedia di Lightsail for Research.

Nama rencana	v CPUs	Memori	Ruang penyimpanan	Tunjangan transfer data bulanan
GPU XL	4	16 GB	50 GB	1 TB
GPU 2XL	8	32 GB	50 GB	1 TB
GPU 4XL	16	64 GB	50 GB	1 TB

Buat Lightsail untuk Penelitian komputer virtual

Selesaikan langkah-langkah berikut untuk membuat Lightsail for Research komputer virtual yang menjalankan aplikasi.

1. Masuk ke konsol Lightsail for Research.
2. Di halaman beranda, pilih Buat komputer virtual.
3. Pilih Wilayah AWS untuk komputer virtual Anda yang dekat dengan lokasi fisik Anda.
4. Pilih paket aplikasi dan perangkat keras. Untuk informasi selengkapnya, lihat Pilih gambar aplikasi dan paket perangkat keras untuk Lightsail for Research.
5. Masukkan nama untuk komputer virtual Anda. Karakter yang valid termasuk karakter alfanumerik, angka, titik, tanda hubung, dan garis bawah.

Nama komputer virtual juga harus memenuhi persyaratan berikut:

- Jadilah unik Wilayah AWS di masing-masing akun Lightsail for Research Anda.
- Berisi 2—255 karakter.
- Mulai dan akhiri dengan karakter atau angka alfanumerik.

6. Pilih Buat komputer virtual di panel Ringkasan.

Dalam beberapa menit, komputer virtual Lightsail for Research Anda siap dan Anda dapat menghubungkannya melalui sesi antarmuka pengguna grafis (GUI). Untuk informasi selengkapnya tentang menghubungkan ke komputer virtual Lightsail for Research, lihat. Akses Lightsail for Research aplikasi komputer virtual

> **Important**
>
> Komputer virtual yang baru dibuat memiliki satu set port firewall yang terbuka secara default. Untuk informasi lebih lanjut tentang port ini, lihatKelola port firewall untuk Lightsail for Research komputer virtual.

Lihat Lightsail for Research detail komputer virtual

Lengkapi langkah-langkah berikut untuk melihat daftar komputer virtual dan detailnya di akun Lightsail for Research Anda.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi untuk melihat daftar komputer virtual di akun Anda.

Pilih nama komputer virtual untuk menavigasi ke halaman manajemennya. Berikut ini adalah informasi yang disediakan halaman manajemen:

- Nama komputer virtual — Nama komputer virtual Anda.
- Status — Komputer virtual Anda dapat memiliki salah satu kode status berikut:
  - Membuat
  - Berjalan
  - Stopping

  - Dihentikan
  - Tidak Diketahui
- Wilayah AWS— Wilayah AWS Komputer virtual Anda dibuat di.
- Aplikasi & Perangkat Keras — Rencana aplikasi dan perangkat keras komputer virtual.
- Perkiraan penggunaan bulanan — Perkiraan penggunaan per jam untuk komputer virtual ini, untuk siklus penagihan saat ini.
- Perkiraan biaya bulan ke saat ini — Perkiraan biaya (dalam USD) untuk komputer virtual, untuk siklus penagihan ini.
- Dasbor — Dari tab Dasbor, Anda dapat meluncurkan sesi untuk mengakses aplikasi komputer virtual. Anda juga dapat melihat pemanfaatan CPU. Pemanfaatan CPU mengidentifikasi kekuatan pemrosesan yang digunakan oleh aplikasi komputer virtual. Setiap titik data yang ditunjukkan dalam grafik mewakili pemanfaatan CPU rata-rata selama periode waktu tertentu.
- Aturan pengendalian biaya — Aturan yang Anda tetapkan untuk membantu mengelola penggunaan dan biaya komputer virtual Anda.
- Penggunaan komputer virtual — Perkiraan biaya dan penggunaan untuk siklus penagihan yang diberikan. Anda dapat memfilter ini berdasarkan tanggal dan waktu.
- Penyimpanan — Membuat, melampirkan, dan melepaskan disk komputer virtual dari tab Penyimpanan. Disk adalah volume penyimpanan yang dapat Anda pasang ke komputer virtual dan dipasang sebagai hard drive.
- Tag - Kelola tag komputer virtual Anda dari tab tag. Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tag terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tag untuk mencari dan memfilter sumber daya Anda, atau melacak AWS biaya Anda.

Akses Lightsail for Research aplikasi komputer virtual

Selesaikan langkah-langkah berikut untuk meluncurkan aplikasi yang berjalan di komputer virtual Lightsail for Research Anda.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi.
3. Temukan nama komputer virtual tempat Anda ingin meluncurkan aplikasi.

> **Note**
>
> Jika komputer virtual dihentikan, pertama-tama pilih tombol Mulai komputer untuk menyalakannya.

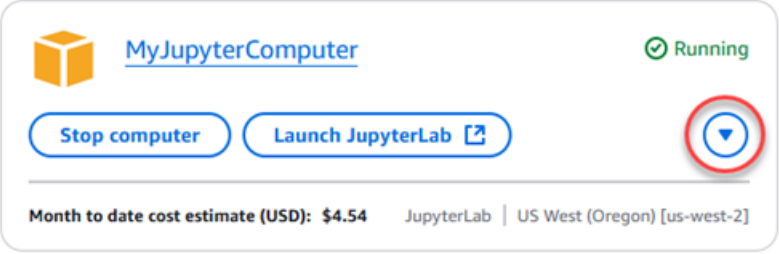
4. Pilih Luncurkan aplikasi. Misalnya, Luncurkan JupyterLab. Sesi aplikasi akan terbuka di jendela browser web baru.

> **Important**
>
> Jika browser web Anda memiliki pemblokir pop-up yang diinstal, Anda mungkin perlu mengizinkan pop-up dari domain aws.amazon.com sebelum membuka sesi Anda.

Akses Lightsail for Research sistem operasi komputer virtual

Selesaikan langkah-langkah berikut untuk mengakses sistem operasi untuk komputer virtual Lightsail for Research Anda.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi.
3. Temukan nama komputer virtual Anda dan kemudian pilih dropdown tombol tindakan di bawah status komputer.



> **Note**
>
> Jika komputer virtual dihentikan, pertama-tama pilih tombol Start untuk menyalakannya.

4. Pilih Access sistem operasi. Sesi sistem operasi akan terbuka di jendela browser baru.

> **Important**
>
> Jika browser web Anda memiliki pemblokir pop-up yang diinstal, Anda mungkin perlu mengizinkan pop-up dari domain aws.amazon.com sebelum membuka sesi Anda.

Kelola port firewall untuk Lightsail for Research komputer virtual

Firewall di Amazon Lightsail for Research mengontrol lalu lintas yang diizinkan untuk terhubung ke komputer virtual Anda. Anda menambahkan aturan ke firewall komputer virtual Anda yang menentukan protokol, port, dan sumber IPv4 atau IPv6 alamat yang diizinkan untuk terhubung dengannya. Aturan firewall selalu bersifat permisif; Anda tidak dapat menciptakan aturan yang menolak akses. Anda menambahkan aturan ke firewall komputer virtual Anda untuk memungkinkan lalu lintas mencapai komputer virtual Anda. Setiap komputer virtual memiliki dua firewall; satu untuk IPv4 alamat dan satu lagi untuk IPv6 alamat. Kedua firewall independen satu sama lain, dan berisi seperangkat aturan yang telah dikonfigurasi sebelumnya yang menyaring lalu lintas yang masuk ke instance.

Protokol

Protokol adalah format di mana data ditransmisikan antara dua komputer. Anda dapat menentukan protokol berikut dalam aturan firewall:

- Transmission Control Protocol (TCP) terutama digunakan untuk membangun dan memelihara koneksi antara klien dan aplikasi yang berjalan di komputer virtual Anda. Ini adalah protokol yang banyak digunakan, dan salah satu yang mungkin sering Anda tentukan dalam aturan firewall Anda.
- User Datagram Protocol (UDP) terutama digunakan untuk membangun koneksi latensi rendah dan toleransi kerugian antara klien dan aplikasi yang berjalan di komputer virtual Anda. Penggunaan idealnya adalah untuk aplikasi jaringan di mana latensi yang dirasakan sangat penting, seperti komunikasi game, suara, dan video.
- Protokol Pesan Kontrol Internet (ICMP) terutama digunakan untuk mendiagnosis masalah komunikasi jaringan, seperti untuk menentukan apakah data mencapai tujuan yang dimaksudkan pada waktu yang tepat atau tidak. Penggunaan idealnya adalah untuk utilitas Ping, yang dapat Anda gunakan untuk menguji kecepatan koneksi antara komputer lokal Anda dan komputer virtual Anda. Ini melaporkan berapa lama waktu yang dibutuhkan data untuk mencapai komputer virtual Anda dan kembali ke komputer lokal Anda.

- Semua digunakan untuk memungkinkan semua lalu lintas protokol mengalir ke komputer virtual Anda. Tentukan protokol ini ketika Anda tidak yakin protokol mana yang akan ditentukan. Ini mencakup semua protokol internet, tidak hanya yang ditentukan di sini. Untuk informasi selengkapnya, lihat Angka Protokol di situs web Internet Assigned Numbers Authority.

Port

Mirip dengan port fisik di komputer Anda, yang memungkinkan komputer Anda berkomunikasi dengan periferal seperti keyboard dan pointer Anda, port firewall berfungsi sebagai titik akhir komunikasi internet untuk komputer virtual Anda. Ketika klien berusaha untuk terhubung dengan komputer virtual Anda, itu akan mengekspos port untuk membangun komunikasi.

Port yang dapat Anda tentukan dalam aturan firewall dapat berkisar dari 0 sampai 65535. Saat Anda membuat aturan firewall untuk memungkinkan klien membuat koneksi dengan komputer virtual Anda, Anda menentukan protokol yang akan digunakan. Anda juga menentukan nomor port di mana koneksi dapat dibuat dan alamat IP yang diizinkan untuk membuat koneksi.

Port berikut terbuka secara default untuk komputer virtual yang baru dibuat.

- TCP
  - 22 - Digunakan untuk Secure Shell (SSH).
  - 80 - Digunakan untuk Hypertext Transfer Protocol (HTTP).
  - 443 - Digunakan untuk Hypertext Transfer Protocol Secure (HTTPS).
  - 8443 - Digunakan untuk Hypertext Transfer Protocol Secure (HTTPS).

Mengapa membuka dan menutup port

Ketika Anda membuka port, Anda mengizinkan klien untuk membuat koneksi dengan komputer virtual Anda. Ketika Anda menutup port, Anda memblokir koneksi ke komputer virtual Anda. Misalnya, untuk memungkinkan klien SSH terhubung ke komputer virtual Anda, Anda mengonfigurasi aturan firewall yang memungkinkan TCP melalui port 22 hanya dari alamat IP komputer yang perlu membuat koneksi. Dalam hal ini, Anda tidak ingin mengizinkan alamat IP apa pun untuk membuat koneksi SSH ke komputer virtual Anda. Melakukan hal itu dapat menyebabkan risiko keamanan. Jika aturan ini sudah dikonfigurasi pada firewall instans Anda, maka Anda dapat menghapusnya untuk memblokir klien SSH agar tidak terhubung ke komputer virtual Anda.

Prosedur berikut menunjukkan cara mendapatkan port yang saat ini terbuka di komputer virtual Anda, membuka port baru, dan menutup port.

Topik

Lengkapi prasyarat

Lengkapi prasyarat berikut sebelum Anda memulai.

- Buat komputer virtual di Lightsail for Research. Untuk informasi selengkapnya, lihat Buat Lightsail untuk Penelitian komputer virtual.
- Unduh dan instal AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat Menginstal atau memperbarui versi terbaru dari Panduan AWS Command Line Interface Pengguna untuk Versi 2. AWS CLI
- Konfigurasikan AWS CLI untuk mengakses Anda Akun AWS. Untuk informasi selengkapnya, lihat Dasar-dasar konfigurasi di Panduan AWS Command Line Interface Pengguna untuk Versi 2.

Dapatkan status port untuk komputer virtual

Selesaikan prosedur berikut untuk mendapatkan status port untuk komputer virtual. Prosedur ini menggunakan `get-instance-port-states` AWS CLI perintah untuk mendapatkan status port firewall untuk komputer virtual Lightsail for Research tertentu, alamat IP yang diizinkan untuk terhubung ke komputer virtual melalui port, dan protokol. Untuk informasi selengkapnya, lihat get-instance-port-states dalam AWS CLI Referensi Perintah.

1. Langkah ini ditentukan oleh sistem operasi komputer lokal Anda.

   - Jika komputer lokal Anda menggunakan sistem operasi Windows, buka jendela Command Prompt.
   - Jika komputer lokal Anda menggunakan sistem operasi berbasis Linux atau Unix (termasuk macOS), buka jendela Terminal.

2. Masukkan perintah berikut untuk mendapatkan status port firewall dan alamat IP dan protokol yang diizinkan. Dalam perintah, ganti *REGION* dengan kode AWS Wilayah di mana komputer virtual dibuat, sepertius-east-2. Ganti *NAME* dengan nama komputer virtual Anda.

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

Contoh

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

Respons akan menampilkan port dan protokol terbuka, dan rentang IP CIDR yang diizinkan untuk terhubung ke komputer virtual Anda.

```
[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
```

Untuk informasi tentang cara membuka port, lanjutkan ke bagian berikutnya.

Buka port untuk komputer virtual

Selesaikan prosedur berikut untuk membuka port untuk komputer virtual. Prosedur ini menggunakan `open-instance-public-ports` AWS CLI perintah. Buka port firewall untuk memungkinkan koneksi dibuat dari alamat IP tepercaya atau rentang alamat IP. Misalnya, untuk mengizinkan alamat IP`192.0.2.44`, tentukan `192.0.2.44` atau`192.0.2.44/32`. Untuk mengizinkan alamat `192.0.2.0` IP`192.0.2.255`, tentukan`192.0.2.0/24`. Untuk informasi selengkapnya, lihat open-instance-public-ports dalam AWS CLI Referensi Perintah.

1. Langkah ini ditentukan oleh sistem operasi komputer lokal Anda.

   - Jika komputer lokal Anda menggunakan sistem operasi Windows, buka jendela Command Prompt.

- Jika komputer lokal Anda menggunakan sistem operasi berbasis Linux atau Unix (termasuk macOS), buka jendela Terminal.

2. Masukkan perintah berikut untuk membuka port.

   Dalam perintah, ganti item berikut:

   - Ganti *REGION* dengan kode AWS Wilayah tempat komputer virtual dibuat, seperti`us-east-2`.
   - Ganti *NAME* dengan nama komputer virtual Anda.
   - Ganti *FROM-PORT* dengan port pertama di berbagai port yang ingin Anda buka.
   - Ganti *PROTOCOL* dengan nama protokol IP. Misalnya, TCP.
   - Ganti *TO-PORT* dengan port terakhir di berbagai port yang ingin Anda buka.
   - Ganti *IP* dengan alamat IP atau rentang alamat IP yang ingin Anda izinkan untuk terhubung ke komputer virtual Anda.

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

   Contoh

   ```
   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
   ```

   Respons akan menampilkan port, protokol, dan rentang IP CIDR yang baru ditambahkan yang diizinkan untuk terhubung ke komputer virtual Anda.

   Untuk informasi tentang cara menutup port, lanjutkan ke bagian berikutnya.

Tutup port untuk komputer virtual

Selesaikan prosedur berikut untuk menutup port untuk komputer virtual. Prosedur ini menggunakan `close-instance-public-ports` AWS CLI perintah. Untuk informasi selengkapnya, lihat close-instance-public-ports dalam AWS CLI Referensi Perintah.

1. Langkah ini ditentukan oleh sistem operasi komputer lokal Anda.
   - Jika komputer lokal Anda menggunakan sistem operasi Windows, buka jendela Command Prompt.
   - Jika komputer lokal Anda menggunakan sistem operasi berbasis Linux atau Unix (termasuk macOS), buka jendela Terminal.
2. Masukkan perintah berikut untuk menutup port.

   Dalam perintah, ganti item berikut:

   - Ganti *REGION* dengan kode AWS Wilayah tempat komputer virtual dibuat, sepertius-east-2.
   - Ganti *NAME* dengan nama komputer virtual Anda.
   - Ganti *FROM-PORT* dengan port pertama di berbagai port yang ingin Anda tutup.
   - Ganti *PROTOCOL* dengan nama protokol IP. Misalnya, TCP.
   - Ganti *TO-PORT* dengan port terakhir di berbagai port yang ingin Anda tutup.
   - Ganti *IP* dengan alamat IP atau rentang alamat IP yang ingin Anda hapus.

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

   Contoh

   ```
   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
   ```

   Respons akan menampilkan port, protokol, dan rentang IP CIDR yang telah ditutup dan tidak lagi diizinkan untuk terhubung ke komputer virtual Anda.

Lanjutkan ke langkah selanjutnya

Anda dapat menyelesaikan langkah-langkah tambahan berikutnya setelah Anda berhasil mengelola port firewall untuk komputer virtual Anda:

- Dapatkan key pair komputer virtual Anda. Dengan key pair, Anda dapat membuat koneksi menggunakan banyak klien SSH, seperti OpenSSH, Putty, dan Windows Subsystem untuk Linux. Untuk informasi selengkapnya, lihat Dapatkan key pair untuk komputer virtual Lightsail for Research.
- Connect ke komputer virtual Anda menggunakan SSH untuk mengelolanya menggunakan command line. Untuk informasi selengkapnya, lihat Transfer file ke Lightsail untuk Penelitian komputer virtual menggunakan Secure Copy.
- Connect ke komputer virtual Anda menggunakan SCP untuk mentransfer file dengan aman. Untuk informasi selengkapnya, lihat Transfer file ke Lightsail untuk Penelitian komputer virtual menggunakan Secure Copy.

Dapatkan key pair untuk komputer virtual Lightsail for Research

Key pair, yang terdiri dari kunci publik dan kunci pribadi, adalah seperangkat kredensyal keamanan yang Anda gunakan untuk membuktikan identitas Anda saat menghubungkan ke komputer virtual Amazon Lightsail for Research. Kunci publik disimpan di setiap komputer virtual di Lightsail for Research, dan Anda menyimpan kunci pribadi di komputer lokal Anda. Kunci pribadi memungkinkan Anda untuk membuat Secure Shell Protocol (SSH) dengan aman dengan komputer virtual Anda. Siapa pun yang memiliki kunci pribadi dapat terhubung ke komputer virtual Anda, jadi penting bagi Anda untuk menyimpan kunci pribadi Anda di tempat yang aman.

Amazon Lightsail default key pair (DKP) dibuat secara otomatis saat pertama kali Anda membuat instance Lightsail atau komputer virtual Lightsail for Research. DKP khusus untuk setiap AWS Wilayah tempat Anda membuat instance atau komputer virtual. Misalnya, DKP Lightsail untuk Wilayah AS Timur (Ohio) (us-east-2) berlaku untuk semua komputer yang Anda buat di AS Timur (Ohio) di Lightsail dan Lightsail untuk Penelitian yang dikonfigurasi untuk menggunakan DKP saat dibuat. Lightsail for Research secara otomatis menyimpan kunci publik DKP di komputer virtual yang Anda buat. Anda dapat mengunduh kunci pribadi DKP kapan saja dengan melakukan panggilan API ke layanan Lightsail.

Dalam dokumen ini, kami menunjukkan kepada Anda cara mendapatkan DKP untuk komputer virtual. Setelah Anda memiliki DKP, Anda dapat membuat koneksi menggunakan banyak klien SSH, seperti OpenSSH, Putty, dan Windows Subsystem untuk Linux. Anda juga dapat menggunakan Secure Copy (SCP) untuk mentransfer file dengan aman dari komputer lokal Anda ke komputer virtual Anda.

> **Note**
>
> Anda juga dapat membuat koneksi protokol tampilan jarak jauh ke komputer virtual Anda menggunakan klien Amazon DCV berbasis browser. Amazon DCV tersedia di konsol Lightsail for Research. Klien RDP itu tidak mengharuskan Anda mendapatkan key pair untuk komputer Anda. Untuk informasi selengkapnya, lihat Akses Lightsail for Research aplikasi komputer virtual dan Akses Lightsail for Research sistem operasi komputer virtual.

Topik

Lengkapi prasyarat

Lengkapi prasyarat berikut sebelum Anda memulai.

- Buat komputer virtual di Lightsail for Research. Untuk informasi selengkapnya, lihat Buat Lightsail untuk Penelitian komputer virtual.
- Unduh dan instal AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat Menginstal atau memperbarui versi terbaru dari Panduan AWS Command Line Interface Pengguna untuk Versi 2. AWS CLI

- Konfigurasikan AWS CLI untuk mengakses Anda Akun AWS. Untuk informasi selengkapnya, lihat Dasar-dasar konfigurasi di Panduan AWS Command Line Interface Pengguna untuk Versi 2.
- Unduh dan instal jq. Ini adalah prosesor JSON baris perintah yang ringan dan fleksibel yang digunakan dalam prosedur berikut untuk mengekstrak detail key pair dari output JSON. AWS CLI Untuk informasi lebih lanjut tentang mengunduh dan menginstal jq, lihat Unduh jq di situs web jq.

Dapatkan key pair untuk komputer virtual

Lengkapi salah satu prosedur berikut untuk mendapatkan Lightsail DKP untuk komputer virtual di Lightsail for Research.

Dapatkan key pair untuk komputer virtual menggunakan komputer lokal Windows

Prosedur ini berlaku untuk Anda jika komputer lokal Anda menggunakan sistem operasi Windows. Prosedur ini menggunakan `download-default-key-pair` AWS CLI perintah untuk mendapatkan DKP Lightsail untuk suatu Wilayah. AWS Untuk informasi selengkapnya, lihat download-default-key-pair dalam AWS CLI Referensi Perintah.

1. Buka jendela Prompt Perintah.
2. Masukkan perintah berikut untuk mendapatkan DKP Lightsail untuk Wilayah tertentu. AWS Perintah ini menyimpan informasi ke `dkp-details.json` file. Dalam perintah, ganti *region-code* dengan kode AWS Wilayah di mana komputer virtual dibuat, seperti`us-east-2`.

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

   Contoh

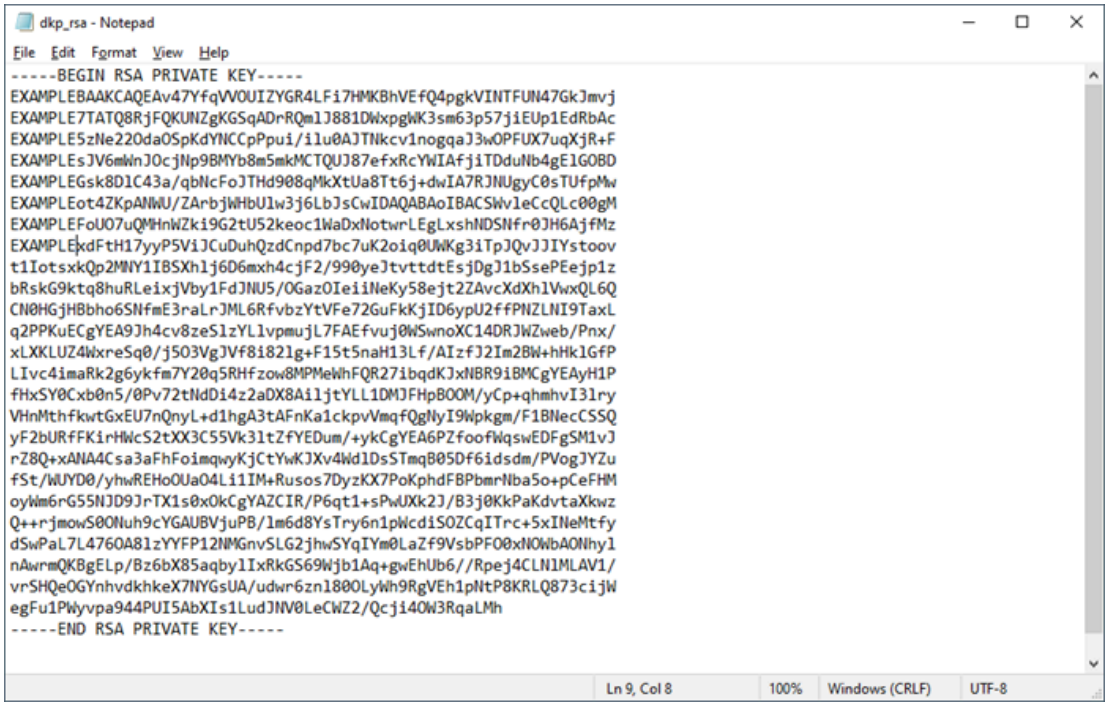
   ```
   aws lightsail download-default-key-pair --region us-east-2 > dkp-details.json
   ```

   Tidak ada tanggapan terhadap perintah. Anda dapat mengonfirmasi apakah perintah berhasil dengan membuka `dkp-details.json` file dan melihat apakah informasi DKP Lightsail disimpan. Isi `dkp-details.json` file akan terlihat seperti contoh berikut. Perintah gagal jika file kosong.

3. Masukkan perintah berikut untuk mengekstrak informasi kunci pribadi dari `dkp-details.json` file dan menambahkannya ke file kunci `dkp_rsa` pribadi baru.

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

Tidak ada tanggapan terhadap perintah. Anda dapat mengonfirmasi apakah perintah berhasil dengan membuka `dkp_rsa` file dan melihat apakah itu berisi informasi. Isi `dkp_rsa` file akan terlihat seperti contoh berikut. Perintah gagal jika file kosong.



Anda sekarang memiliki kunci pribadi yang diperlukan untuk membuat koneksi SSH atau SCP ke komputer virtual Anda. Lanjutkan ke bagian berikutnya untuk langkah tambahan selanjutnya.

Dapatkan key pair untuk komputer virtual menggunakan Linux, Unix, atau komputer lokal macOS

Prosedur ini berlaku untuk Anda jika komputer lokal Anda menggunakan Linux, Unix, atau sistem operasi macOS. Prosedur ini menggunakan `download-default-key-pair` AWS CLI perintah untuk mendapatkan DKP Lightsail untuk suatu Wilayah. AWS Untuk informasi selengkapnya, lihat download-default-key-pair dalam AWS CLI Referensi Perintah.

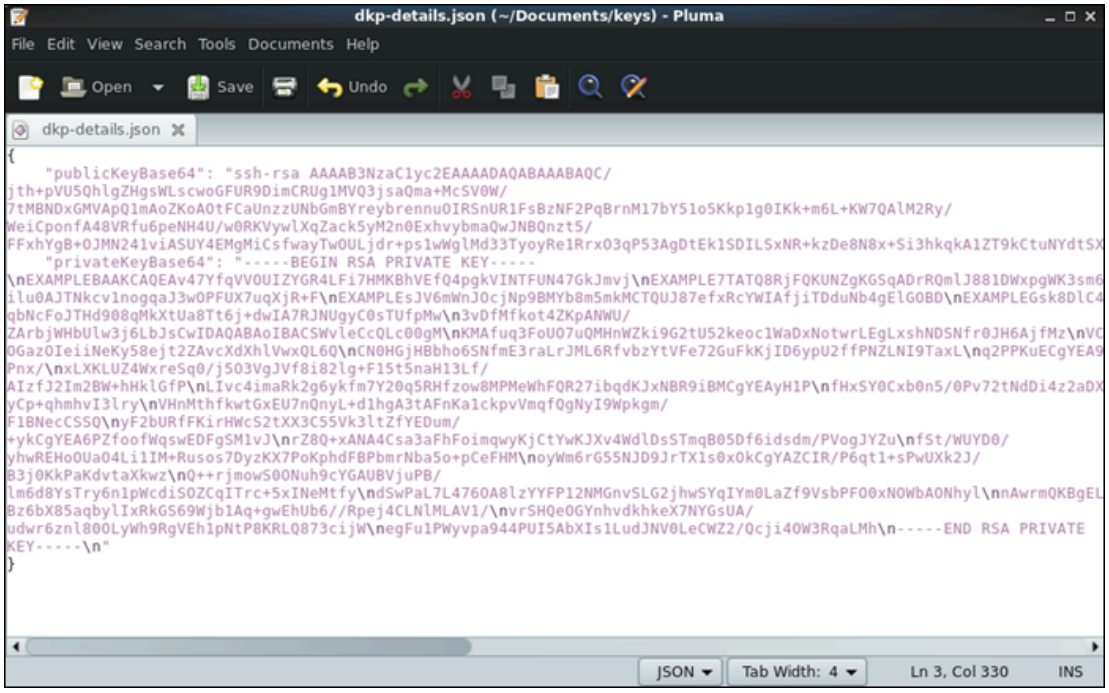
1. Buka jendela Terminal.
2. Masukkan perintah berikut untuk mendapatkan DKP Lightsail untuk Wilayah tertentu. AWS Perintah ini menyimpan informasi ke `dkp-details.json` file. Dalam perintah, ganti *`region-code`* dengan kode AWS Wilayah di mana komputer virtual dibuat, sepertius`-east-2`.

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

   Contoh

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

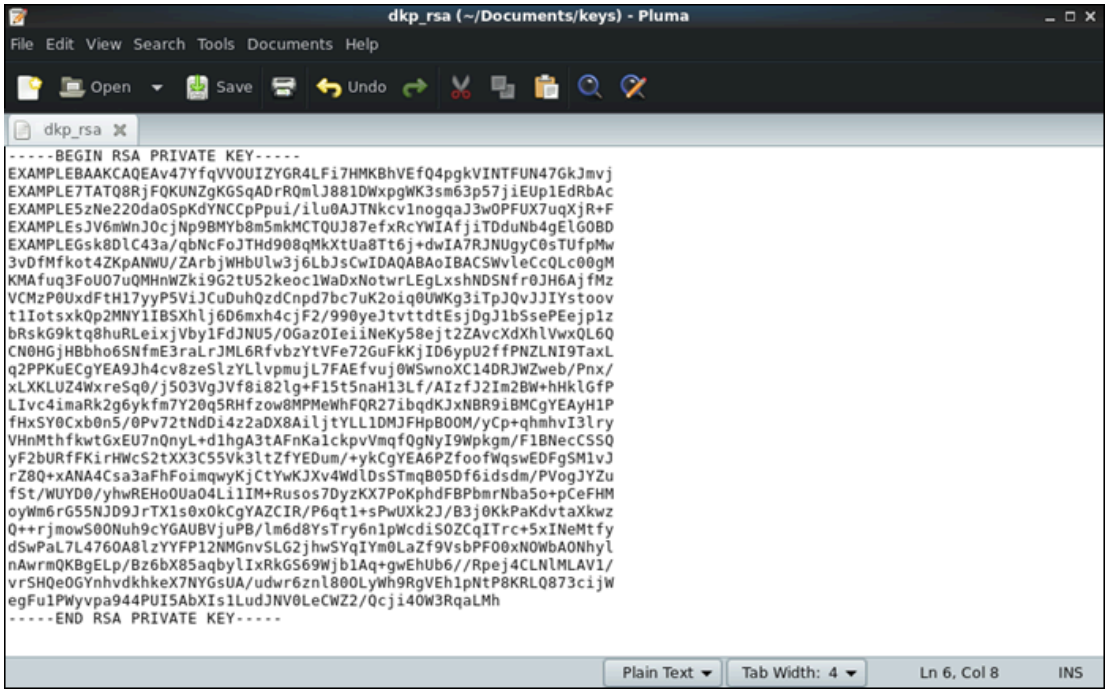
Tidak ada tanggapan terhadap perintah. Anda dapat mengonfirmasi apakah perintah berhasil dengan membuka `dkp-details.json` file dan melihat apakah informasi DKP Lightsail disimpan. Isi `dkp-details.json` file akan terlihat seperti contoh berikut. Perintah gagal jika file kosong.



3. Masukkan perintah berikut untuk mengekstrak informasi kunci pribadi dari `dkp-details.json` file dan menambahkannya ke file kunci `dkp_rsa` pribadi baru.

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

Tidak ada tanggapan terhadap perintah. Anda dapat mengonfirmasi apakah perintah berhasil dengan membuka `dkp_rsa` file dan melihat apakah itu berisi informasi. Isi `dkp_rsa` file akan terlihat seperti contoh berikut. Perintah gagal jika file kosong.



4. Masukkan perintah berikut untuk mengatur izin untuk `dkp_rsa` file.

```
chmod 600 dkp_rsa
```

Anda sekarang memiliki kunci pribadi yang diperlukan untuk membuat koneksi SSH atau SCP ke komputer virtual Anda. Lanjutkan ke bagian berikutnya untuk langkah tambahan selanjutnya.

Lanjutkan ke langkah selanjutnya

Anda dapat menyelesaikan langkah-langkah tambahan berikutnya setelah Anda berhasil mendapatkan pasangan kunci untuk komputer virtual Anda:

- Connect ke komputer virtual Anda menggunakan SSH untuk mengelolanya menggunakan command line. Untuk informasi selengkapnya, lihat Connect ke komputer virtual Lightsail for Research menggunakan Secure Shell.
- Connect ke komputer virtual Anda menggunakan SCP untuk mentransfer file dengan aman. Untuk informasi selengkapnya, lihat Transfer file ke Lightsail untuk Penelitian komputer virtual menggunakan Secure Copy.

Connect ke komputer virtual Lightsail for Research menggunakan Secure Shell

Anda dapat terhubung ke komputer virtual di Amazon Lightsail for Research menggunakan Secure Shell Protocol (SSH). Anda dapat menggunakan SSH untuk mengelola komputer virtual Anda dari jarak jauh sehingga Anda dapat masuk ke komputer Anda melalui internet dan menjalankan perintah.

> **Note**
>
> Anda juga dapat membuat koneksi protokol tampilan jarak jauh ke komputer virtual Anda menggunakan klien Amazon DCV berbasis browser. Amazon DCV tersedia di konsol Lightsail for Research. Untuk informasi selengkapnya, lihat Akses Lightsail for Research sistem operasi komputer virtual.

Topik

Lengkapi prasyarat

Lengkapi prasyarat berikut sebelum Anda memulai.

- Buat komputer virtual di Lightsail for Research. Untuk informasi selengkapnya, lihat Buat Lightsail untuk Penelitian komputer virtual.
- Pastikan komputer virtual yang ingin Anda sambungkan dalam keadaan berjalan. Juga, perhatikan nama komputer virtual dan AWS Wilayah di mana ia dibuat. Anda akan memerlukan informasi ini nanti dalam proses ini. Untuk informasi selengkapnya, lihat Lihat Lightsail for Research detail komputer virtual.
- Pastikan port 22 terbuka di komputer virtual yang ingin Anda sambungkan. Itu adalah port default yang digunakan untuk SSH. Ini terbuka secara default. Tetapi jika Anda menutupnya, Anda harus membukanya kembali sebelum melanjutkan. Untuk informasi selengkapnya, lihat Kelola port firewall untuk Lightsail for Research komputer virtual.

- Dapatkan Lightsail default key pair (DKP) untuk komputer virtual Anda. Untuk informasi selengkapnya, lihat Dapatkan key pair untuk komputer virtual.

> **Tip**
>
> Jika Anda berencana untuk menggunakan AWS CloudShell untuk terhubung ke komputer virtual Anda, lihat Connect ke komputer virtual menggunakan AWS CloudShell di bagian berikutnya. Untuk informasi selengkapnya, lihat Apa itu AWS CloudShell. Jika tidak, lanjutkan ke prasyarat berikutnya.

- Unduh dan instal AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat Menginstal atau memperbarui versi terbaru dari Panduan AWS Command Line Interface Pengguna untuk Versi 2. AWS CLI
- Konfigurasikan AWS CLI untuk mengakses Anda Akun AWS. Untuk informasi selengkapnya, lihat Dasar-dasar konfigurasi di Panduan AWS Command Line Interface Pengguna untuk Versi 2.
- Unduh dan instal jq. Ini adalah prosesor JSON baris perintah yang ringan dan fleksibel yang digunakan dalam prosedur berikut untuk mengekstrak detail key pair. Untuk informasi lebih lanjut tentang mengunduh dan menginstal jq, lihat Unduh jq di situs web jq.

Connect ke komputer virtual menggunakan SSH

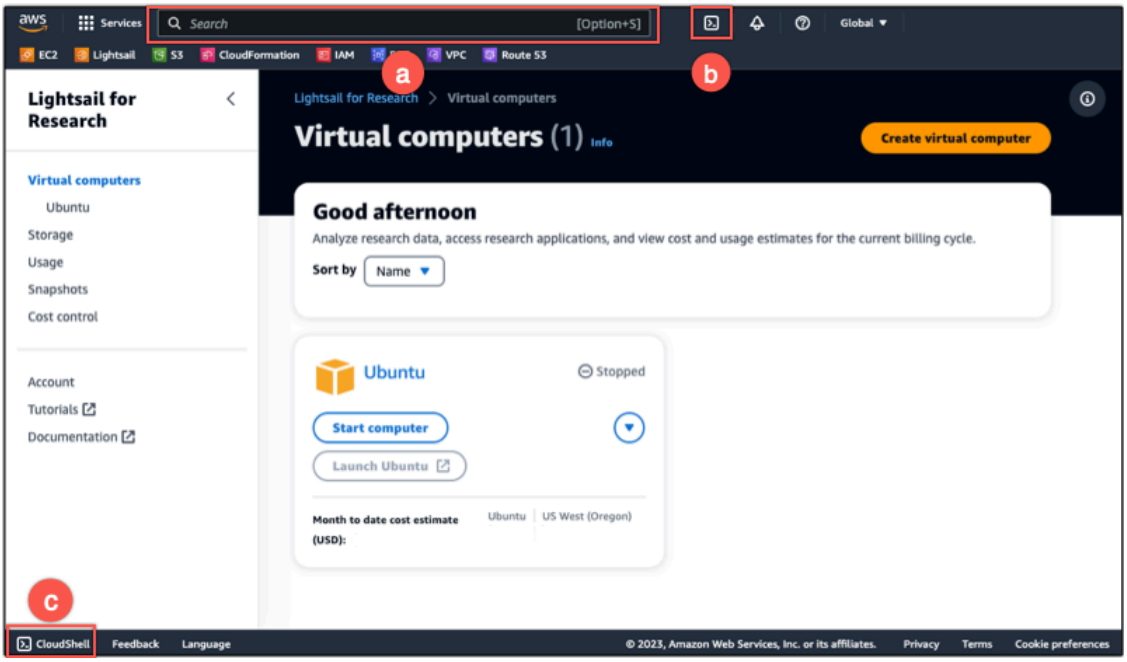
Lengkapi salah satu prosedur berikut untuk membuat koneksi SSH ke komputer virtual Anda di Lightsail for Research.

Connect ke komputer virtual menggunakan AWS CloudShell

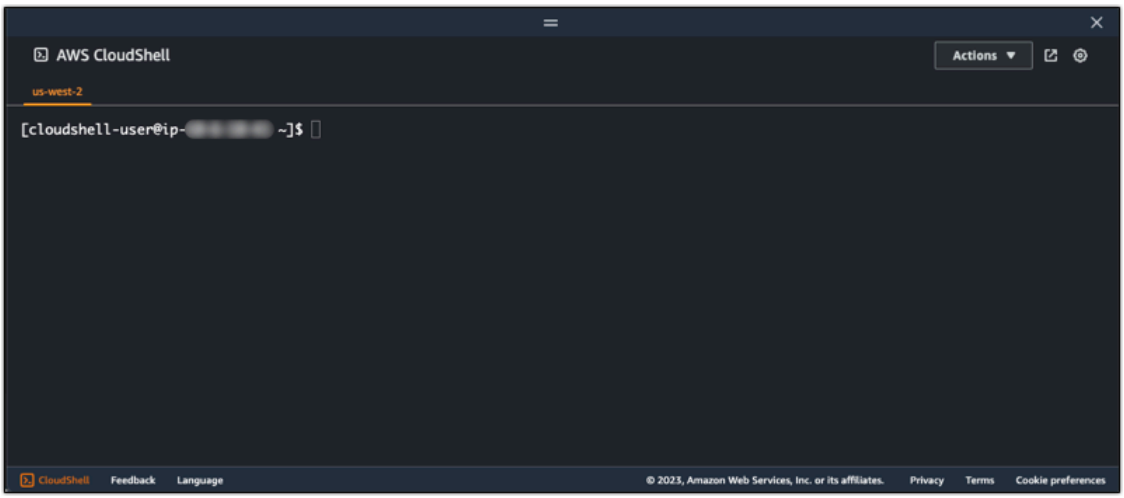
Prosedur ini berlaku jika Anda lebih suka pengaturan minimal untuk terhubung ke komputer virtual Anda. AWS CloudShell menggunakan shell pra-otentikasi berbasis browser yang dapat Anda luncurkan langsung dari file. Konsol Manajemen AWS Anda dapat menjalankan AWS CLI perintah menggunakan shell pilihan Anda, seperti Bash, PowerShell, atau Z shell. Anda dapat melakukan ini tanpa mengunduh atau menginstal alat baris perintah. Untuk informasi selengkapnya, lihat Memulai dengan AWS CloudShell dalam Panduan Pengguna AWS CloudShell .

> **Important**
>
> Sebelum memulai, pastikan untuk mendapatkan Lightsail default key pair (DKP) untuk komputer virtual yang Anda sambungkan. Untuk informasi selengkapnya, lihat Dapatkan key pair untuk komputer virtual Lightsail for Research.

1. Dari konsol Lightsail for Research, CloudShell luncurkan dengan memilih salah satu opsi berikut:
   a. Di kotak Pencarian, ketik "CloudShell“, lalu pilih CloudShell.
   b. Pada bilah navigasi, pilih CloudShellikon.
   c. Pilih CloudShellpada Console Toolbar di kiri bawah konsol.



Ketika command prompt ditampilkan, shell siap untuk interaksi.



2. Pilih shell yang sudah diinstal sebelumnya untuk digunakan. Untuk mengubah shell default, masukkan salah satu nama program berikut di prompt baris perintah. Bashadalah shell default yang berjalan saat Anda meluncurkan AWS CloudShell.

   Bash

   ```
   bash
   ```

   Jika Anda beralih keBash, simbol pada prompt perintah diperbarui ke$.

   PowerShell

   ```
   pwsh
   ```

   Jika Anda beralih ke PowerShell, simbol pada prompt perintah diperbarui kePS>.

   Z shell

   ```
   zsh
   ```

   Jika Anda beralih keZ shell, simbol pada prompt perintah diperbarui ke%.

3. Untuk terhubung ke komputer virtual dari jendela CloudShell terminal, lihatConnect ke komputer virtual menggunakan SSH di Linux, Unix, atau komputer lokal macOS.

Untuk informasi tentang perangkat lunak pra-instal di CloudShell lingkungan, lihat lingkungan AWS CloudShell komputasi di AWS CloudShell Panduan Pengguna.

Connect ke komputer virtual menggunakan SSH pada komputer lokal Windows

Prosedur ini berlaku jika komputer lokal Anda menggunakan sistem operasi Windows. Prosedur ini menggunakan `get-instance` AWS CLI perintah untuk mendapatkan nama pengguna dan alamat IP publik dari instance yang ingin Anda sambungkan. Untuk informasi selengkapnya, lihat get-instance di AWS CLI Command Reference.

> **Important**
>
> Pastikan Anda mendapatkan Lightsail default key pair (DKP) untuk komputer virtual yang Anda coba sambungkan sebelum memulai prosedur ini. Untuk informasi selengkapnya, lihat Dapatkan key pair untuk komputer virtual Lightsail for Research. Prosedur itu mengeluarkan kunci pribadi dari Lightsail DKP ke file `dkp_rsa` yang digunakan dalam salah satu perintah berikut.

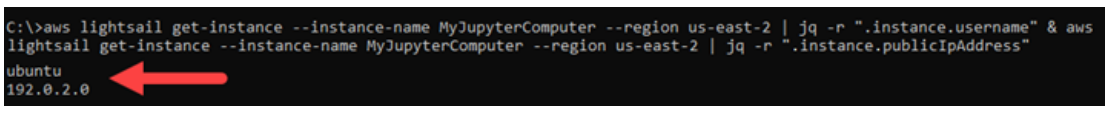
1. Buka jendela Prompt Perintah.
2. Masukkan perintah berikut untuk menampilkan alamat IP publik dan nama pengguna komputer virtual Anda. Dalam perintah, ganti *`region-code`* dengan kode Wilayah AWS di mana komputer virtual dibuat, seperti`us-east-2`. Ganti *`computer-name`* dengan nama komputer virtual yang ingin Anda sambungkan.

   ```
   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"
   ```

   Contoh

   ```
   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"
   ```

   Respons akan menampilkan nama pengguna dan alamat IP publik dari komputer virtual seperti yang ditunjukkan pada contoh berikut. Perhatikan nilai-nilai ini, karena Anda membutuhkannya dalam langkah berikut dari prosedur ini.

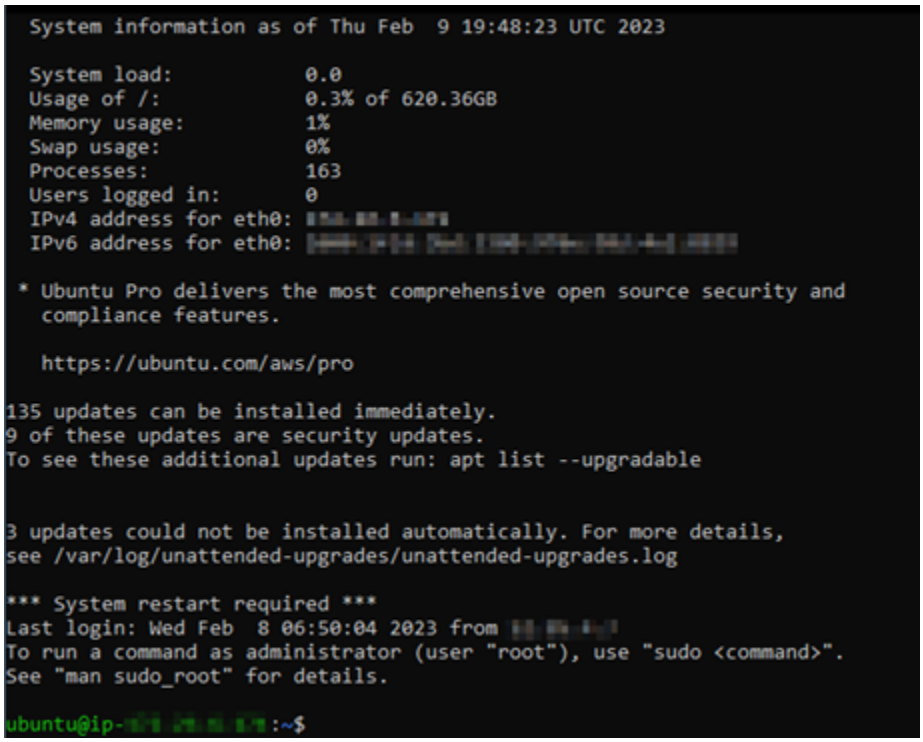
3. Masukkan perintah berikut untuk membuat koneksi SSH dengan komputer virtual Anda. Dalam perintah, ganti *user-name* dengan nama pengguna masuk, dan ganti *public-ip-address* dengan alamat IP publik komputer virtual Anda.

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

Contoh

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

Anda akan melihat respons yang mirip dengan contoh berikut, yang menunjukkan koneksi SSH yang dibuat dengan komputer virtual Ubuntu di Lightsail for Research.



Sekarang setelah Anda berhasil membuat koneksi SSH ke komputer virtual Anda, lanjutkan ke bagian berikutnya untuk langkah selanjutnya.

Connect ke komputer virtual menggunakan SSH di Linux, Unix, atau komputer lokal macOS

Prosedur ini berlaku jika komputer lokal Anda menggunakan Linux, Unix, atau sistem operasi macOS. Prosedur ini menggunakan `get-instance` AWS CLI perintah untuk mendapatkan nama pengguna

dan alamat IP publik dari instance yang ingin Anda sambungkan. Untuk informasi selengkapnya, lihat get-instance di AWS CLI Command Reference.

> **Important**
>
> Pastikan Anda mendapatkan Lightsail default key pair (DKP) untuk komputer virtual yang Anda coba sambungkan sebelum memulai prosedur ini. Untuk informasi selengkapnya, lihat Dapatkan key pair untuk komputer virtual Lightsail for Research. Prosedur itu mengeluarkan kunci pribadi dari Lightsail DKP ke file `dkp_rsa` yang digunakan dalam salah satu perintah berikut.

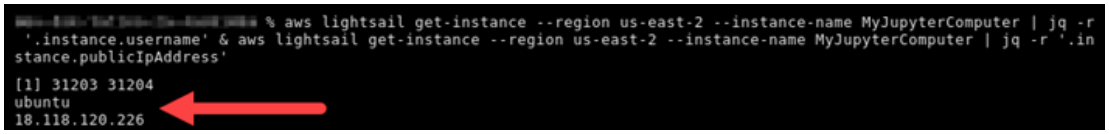
1. Buka jendela Terminal.
2. Masukkan perintah berikut untuk menampilkan alamat IP publik dan nama pengguna komputer virtual Anda. Dalam perintah, ganti *`region-code`* dengan kode AWS Wilayah di mana komputer virtual dibuat, seperti`us-east-2`. Ganti *`computer-name`* dengan nama komputer virtual yang ingin Anda sambungkan.

   ```
   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'
   ```

   Contoh

   ```
   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'
   ```

   Respons akan menampilkan nama pengguna dan alamat IP publik dari komputer virtual seperti yang ditunjukkan pada contoh berikut. Perhatikan nilai-nilai ini, karena Anda membutuhkannya dalam langkah berikut dari prosedur ini.

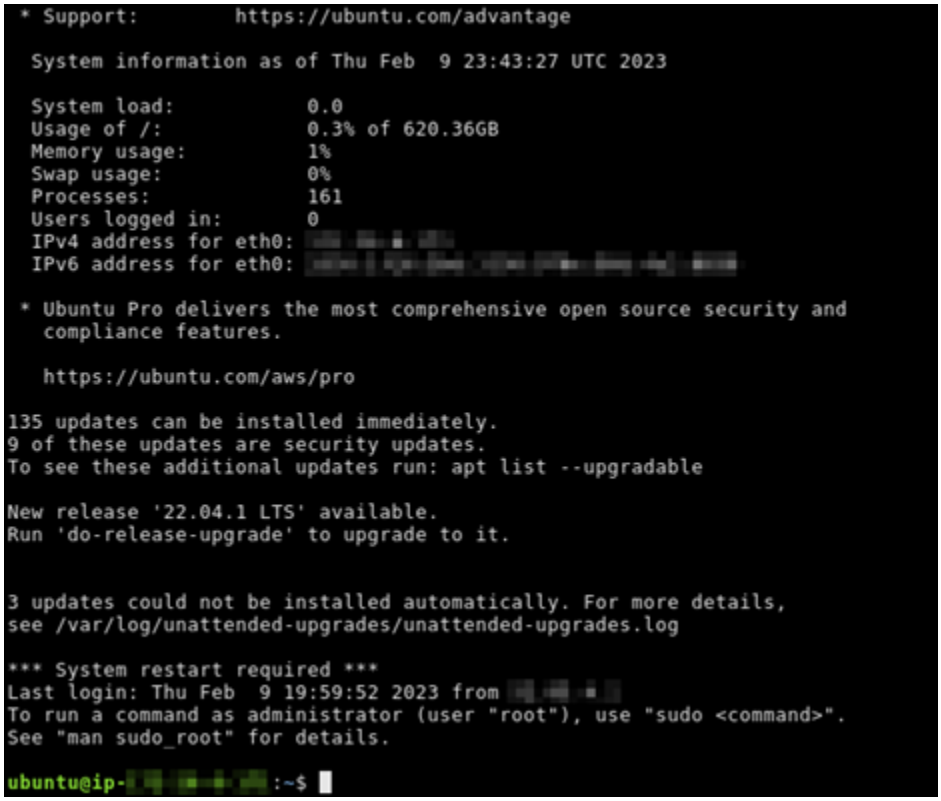
3. Masukkan perintah berikut untuk membuat koneksi SSH dengan komputer virtual Anda. Dalam perintah, ganti *`user-name`* dengan nama pengguna masuk, dan ganti *`public-ip-address`* dengan alamat IP publik komputer virtual Anda.

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

Contoh

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

Anda akan melihat respons yang mirip dengan contoh berikut, yang menunjukkan koneksi SSH yang dibuat dengan komputer virtual Ubuntu di Lightsail for Research.



Sekarang setelah Anda berhasil membuat koneksi SSH ke komputer virtual Anda, lanjutkan ke bagian berikutnya untuk langkah selanjutnya.

Lanjutkan ke langkah selanjutnya

Anda dapat menyelesaikan langkah-langkah tambahan berikutnya setelah Anda berhasil membuat koneksi SSH ke komputer virtual Anda:

- Connect ke komputer virtual Anda menggunakan SCP untuk mentransfer file dengan aman. Untuk informasi selengkapnya, lihat Transfer file ke Lightsail untuk Penelitian komputer virtual menggunakan Secure Copy.

Transfer file ke Lightsail untuk Penelitian komputer virtual menggunakan Secure Copy

Anda dapat mentransfer file dari komputer lokal Anda ke komputer virtual di Amazon Lightsail for Research menggunakan Secure Copy (SCP). Dengan proses ini, Anda dapat mentransfer banyak file, atau seluruh direktori, sekaligus.

> **Note**
>
> Anda juga dapat membuat koneksi protokol tampilan jarak jauh ke komputer virtual Anda menggunakan klien Amazon DCV berbasis browser yang tersedia di konsol Lightsail for Research. Dengan klien Amazon DCV, Anda dapat dengan cepat mentransfer file individual. Untuk informasi selengkapnya, lihat Akses Lightsail for Research sistem operasi komputer virtual.

Topik

Lengkapi prasyarat

Lengkapi prasyarat berikut sebelum Anda memulai.

- Buat komputer virtual di Lightsail for Research. Untuk informasi selengkapnya, lihat Buat Lightsail untuk Penelitian komputer virtual.
- Pastikan komputer virtual yang ingin Anda sambungkan dalam keadaan berjalan. Juga, catat nama komputer virtual dan AWS Wilayah di mana ia dibuat. Anda akan memerlukan informasi ini nanti dalam proses ini. Untuk informasi selengkapnya, lihat Lihat Lightsail for Research detail komputer virtual.

- Unduh dan instal AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat Menginstal atau memperbarui versi terbaru dari Panduan AWS Command Line Interface Pengguna untuk Versi 2. AWS CLI
- Konfigurasikan AWS CLI untuk mengakses Anda Akun AWS. Untuk informasi selengkapnya, lihat Dasar-dasar konfigurasi di Panduan AWS Command Line Interface Pengguna untuk Versi 2.
- Unduh dan instal jq. Ini adalah prosesor JSON baris perintah yang ringan dan fleksibel yang digunakan dalam prosedur berikut untuk mengekstrak detail key pair. Untuk informasi lebih lanjut tentang mengunduh dan menginstal jq, lihat Unduh jq di situs web jq.
- Pastikan port 22 terbuka di komputer virtual yang ingin Anda sambungkan. Itu adalah port default yang digunakan untuk SSH. Ini terbuka secara default. Tetapi jika Anda menutupnya, Anda harus membukanya kembali sebelum melanjutkan. Untuk informasi selengkapnya, lihat Kelola port firewall untuk Lightsail for Research komputer virtual.
- Dapatkan Lightsail default key pair (DKP) untuk komputer virtual Anda. Untuk informasi selengkapnya, lihat Buat Lightsail untuk Penelitian komputer virtual.

Connect ke komputer virtual menggunakan SCP

Lengkapi salah satu prosedur berikut untuk terhubung ke komputer virtual Anda di Lightsail for Research menggunakan SCP.

Connect ke komputer virtual menggunakan SCP pada komputer lokal Windows

Prosedur ini berlaku untuk Anda jika komputer lokal Anda menggunakan sistem operasi Windows. Prosedur ini menggunakan `get-instance` AWS CLI perintah untuk mendapatkan nama pengguna dan alamat IP publik dari instance yang ingin Anda sambungkan. Untuk informasi selengkapnya, lihat get-instance di AWS CLI Command Reference.

> **Important**
>
> Pastikan Anda mendapatkan Lightsail default key pair (DKP) untuk komputer virtual yang Anda coba sambungkan sebelum memulai prosedur ini. Untuk informasi selengkapnya, lihat Dapatkan key pair untuk komputer virtual Lightsail for Research. Prosedur itu mengeluarkan kunci pribadi dari Lightsail DKP ke file `dkp_rsa` yang digunakan dalam salah satu perintah berikut.

1. Buka jendela Prompt Perintah.

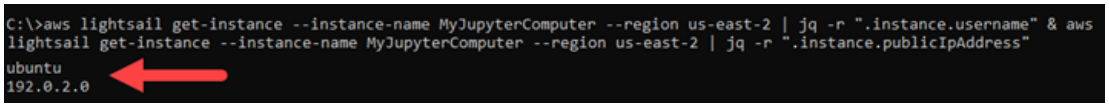
2. Masukkan perintah berikut untuk menampilkan alamat IP publik dan nama pengguna komputer virtual Anda. Dalam perintah, ganti *region-code* dengan kode AWS Wilayah di mana komputer virtual dibuat, sepertius-east-2. Ganti *computer-name* dengan nama komputer virtual yang ingin Anda sambungkan.

```
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"
```

Contoh

```
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"
```

Respons akan menampilkan nama pengguna dan alamat IP publik dari komputer virtual seperti yang ditunjukkan pada contoh berikut. Perhatikan nilai-nilai ini, karena Anda membutuhkannya dalam langkah berikut dari prosedur ini.



3. Masukkan perintah berikut untuk membuat koneksi SCP dengan komputer virtual Anda dan mentransfer file ke sana.

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

Dalam perintah itu, ganti:

- *source-folder*dengan folder di komputer lokal Anda yang berisi file yang ingin Anda transfer.
- *user-name*dengan nama pengguna dari langkah sebelumnya dari prosedur ini (sepertiubuntu).
- *public-ip-address*dengan alamat IP publik komputer virtual Anda dari langkah sebelumnya dari prosedur ini.
- *destination-directory*dengan jalur ke direktori di komputer virtual tempat Anda ingin menyalin file Anda.

Contoh berikut menyalin semua file dari `C:\Files` folder di komputer lokal ke `/home/lightsail-user/Uploads/` direktori di komputer virtual jarak jauh.

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

Anda akan melihat respons yang mirip dengan contoh berikut. Ini menunjukkan setiap file yang ditransfer dari folder asal ke direktori tujuan. Anda sekarang harus dapat mengakses file-file itu di komputer virtual Anda.

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

Connect ke komputer virtual menggunakan SCP di Linux, Unix, atau komputer lokal macOS

Prosedur ini berlaku untuk Anda jika komputer lokal Anda menggunakan Linux, Unix, atau sistem operasi macOS. Prosedur ini menggunakan `get-instance` AWS CLI perintah untuk mendapatkan nama pengguna dan alamat IP publik dari instance yang ingin Anda sambungkan. Untuk informasi selengkapnya, lihat get-instance di AWS CLI Command Reference.

> **Important**
>
> Pastikan Anda mendapatkan Lightsail default key pair (DKP) untuk komputer virtual yang Anda coba sambungkan sebelum memulai prosedur ini. Untuk informasi selengkapnya, lihat Dapatkan key pair untuk komputer virtual Lightsail for Research. Prosedur itu mengeluarkan kunci pribadi dari Lightsail DKP ke file `dkp_rsa` yang digunakan dalam salah satu perintah berikut.

1. Buka jendela Terminal.
2. Masukkan perintah berikut untuk menampilkan alamat IP publik dan nama pengguna komputer virtual Anda. Dalam perintah, ganti *`region-code`* dengan kode AWS Wilayah di mana komputer

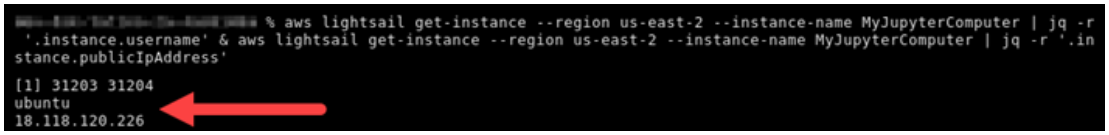
virtual dibuat, sepertius-east-2. Ganti *computer-name* dengan nama komputer virtual yang ingin Anda sambungkan.

```
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'
```

Contoh

```
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'
```

Respons akan menampilkan nama pengguna dan alamat IP publik dari komputer virtual seperti yang ditunjukkan pada contoh berikut. Perhatikan nilai-nilai ini, karena Anda membutuhkannya dalam langkah berikut dari prosedur ini.



3. Masukkan perintah berikut untuk membuat koneksi SCP dengan komputer virtual Anda dan mentransfer file ke sana.

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

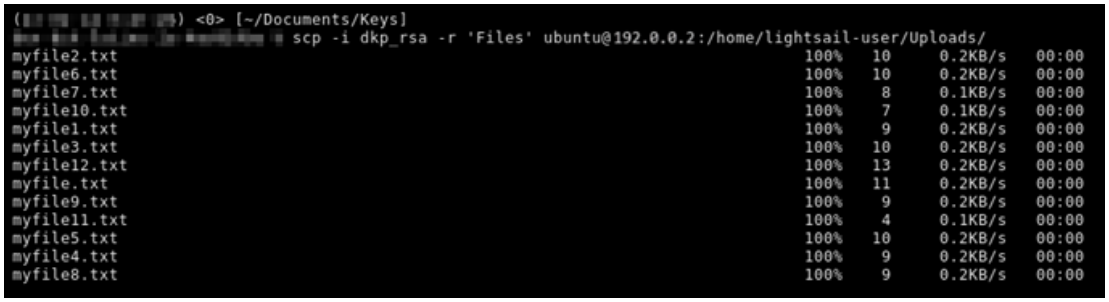
Dalam perintah itu, ganti:

- *source-folder*dengan folder di komputer lokal Anda yang berisi file yang ingin Anda transfer.
- *user-name*dengan nama pengguna dari langkah sebelumnya dari prosedur ini (sepertiubuntu).
- *public-ip-address*dengan alamat IP publik komputer virtual Anda dari langkah sebelumnya dari prosedur ini.
- *destination-directory*dengan jalur ke direktori di komputer virtual tempat Anda ingin menyalin file Anda.

Contoh berikut menyalin semua file dari `C:\Files` folder di komputer lokal ke `/home/lightsail-user/Uploads/` direktori di komputer virtual jarak jauh.

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

Anda akan melihat respons yang mirip dengan contoh berikut. Ini menunjukkan setiap file yang ditransfer dari folder asal ke direktori tujuan. Anda sekarang harus dapat mengakses file-file itu di komputer virtual Anda.



Hapus Lightsail for Research komputer virtual

Selesaikan langkah-langkah berikut untuk menghapus komputer virtual Lightsail for Research Anda saat Anda tidak lagi membutuhkannya. Anda berhenti menimbulkan biaya untuk komputer virtual segera setelah dihapus. Sumber daya yang dilampirkan ke komputer yang dihapus, seperti snapshot, terus dikenakan biaya hingga Anda menghapusnya.

> **Important**
>
> Menghapus komputer virtual adalah tindakan permanen, dan komputer tidak dapat dipulihkan. Jika Anda mungkin memerlukan data Anda nanti, buat snapshot komputer virtual Anda sebelum Anda menghapusnya. Untuk informasi selengkapnya, lihat Membuat snapshot.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi.
3. Pilih komputer virtual yang akan dihapus.
4. Pilih Tindakan, lalu pilih Hapus komputer virtual.

5. Ketik konfirmasi di blok teks. Kemudian, pilih Hapus komputer virtual.

Mengamankan dan menyimpan data dengan Lightsail for Research volume

Amazon Lightsail for Research menyediakan volume penyimpanan tingkat blok (disk) yang dapat Anda lampirkan ke komputer virtual Lightsail for Research yang sedang berjalan. Anda dapat menggunakan disk sebagai perangkat penyimpanan utama untuk data yang memerlukan pembaruan yang sering dan terperinci. Misalnya, disk adalah opsi penyimpanan yang disarankan saat Anda menjalankan database di komputer virtual Lightsail for Research.

Disk berperilaku seperti perangkat blok eksternal yang tidak diformat yang dapat Anda lampirkan ke satu komputer virtual. Volume bertahan secara independen dari masa pakai komputer. Setelah Anda memasang disk ke komputer, Anda dapat menggunakannya seperti hard drive fisik lainnya.

Anda dapat melampirkan beberapa disk ke komputer. Anda juga dapat melepaskan disk dari satu komputer dan memasangnya ke komputer lain.

Untuk menyimpan salinan cadangan data Anda, buat snapshot disk. Anda dapat membuat disk baru dari snapshot dan melampirkannya ke komputer lain.

Topik

Buat disk penyimpanan di konsol Lightsail for Research

Selesaikan langkah-langkah berikut untuk membuat disk untuk komputer virtual Lightsail for Research Anda.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Penyimpanan di panel navigasi.
3. Pilih Buat disk.

4. Masukkan nama untuk disk Anda. Karakter yang valid termasuk karakter alfanumerik, angka, titik, tanda hubung, dan garis bawah.

   Nama disk juga harus memenuhi persyaratan berikut:

   - Jadilah unik Wilayah AWS di masing-masing akun Lightsail for Research Anda.
   - Berisi 2—255 karakter.
   - Mulai dan akhiri dengan karakter atau angka alfanumerik.

5. Pilih Wilayah AWS untuk disk Anda.

   Disk harus berada di Wilayah yang sama dengan komputer virtual tempat Anda akan melampirkannya.

6. Pilih ukuran disk Anda dalam GB.

7. Lanjutkan ke bagian Lampirkan disk untuk informasi tentang melampirkan disk ke komputer virtual Anda.

Lihat detail disk penyimpanan di konsol Lightsail for Research

Selesaikan langkah-langkah berikut untuk melihat disk di akun Lightsail for Research Anda dan detailnya.

1. Masuk ke konsol Lightsail for Research.

2. Pilih Penyimpanan di panel navigasi.

   Halaman Penyimpanan memberikan tampilan komprehensif disk di akun Lightsail for Research Anda.

   Informasi berikut ditampilkan di halaman:

   - Nama — Nama disk penyimpanan Anda.
   - Ukuran — Ukuran disk Anda (dalam GB).
   - Wilayah AWS— Disk Wilayah AWS Anda dibuat di.
   - Terlampir ke — Komputer Lightsail tempat disk Anda terpasang.
   - Tanggal dibuat — Tanggal disk Anda dibuat.

Tambahkan penyimpanan ke komputer virtual di Lightsail for Research

Selesaikan langkah-langkah berikut untuk melampirkan disk ke komputer virtual di Lightsail for Research. Anda dapat melampirkan hingga 15 disk ke komputer virtual. Ketika Anda melampirkan disk ke komputer virtual Anda menggunakan konsol Lightsail for Research, itu secara otomatis diformat dan dipasang oleh layanan. Proses ini memakan waktu beberapa menit, jadi Anda harus mengonfirmasi bahwa disk telah mencapai status pemasangan yang dipasang sebelum Anda mulai menggunakannya. Secara default, Lightsail for Research memasang disk ke direktori; *<disk-name>* di mana nama `/home/lightsail-user/`*<disk-name>* yang Anda berikan pada disk Anda.

> **Important**
>
> Sebelum Anda dapat melampirkan disk ke komputer virtual, komputer virtual harus dalam keadaan Running. Jika Anda melampirkan disk ke komputer virtual saat berada dalam keadaan Berhenti, disk akan terpasang tetapi gagal dipasang. Jika status Mount disk Gagal, Anda harus melepaskan disk kemudian memasangnya kembali saat komputer virtual dalam keadaan Running.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi.
3. Pilih komputer untuk memasang disk.
4. Pilih tab Penyimpanan.
5. Pilih Lampirkan disk.
6. Pilih nama disk untuk dilampirkan ke komputer.
7. Pilih Lampirkan.

Lepaskan disk dari komputer virtual di Lightsail for Research

Selesaikan langkah-langkah berikut untuk melepaskan disk dari komputer.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Penyimpanan di panel navigasi.

3. Temukan disk untuk dilepas. Di bawah kolom Terlampir ke, pilih nama komputer tempat disk terpasang.
4. Pilih Berhenti untuk menghentikan komputer. Anda harus menghentikan komputer sebelum Anda dapat melepaskan disk.
5. Konfirmasikan Anda ingin menghentikan komputer, lalu pilih Hentikan komputer komputer.
6. Pilih tab Penyimpanan.
7. Pilih disk yang akan dilepas, lalu pilih Lepaskan.
8. Konfirmasikan bahwa Anda ingin melepaskan disk Anda dari komputer, lalu pilih Lepaskan.

Hapus disk penyimpanan yang tidak digunakan di Lightsail for Research

Selesaikan langkah-langkah berikut untuk menghapus disk penyimpanan saat Anda tidak membutuhkannya lagi. Anda berhenti menimbulkan biaya untuk disk segera setelah dihapus.

Jika disk terpasang ke komputer, Anda harus melepaskannya terlebih dahulu sebelum Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat Lepaskan disk dari komputer virtual di Lightsail for Research.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Penyimpanan di panel navigasi.
3. Temukan dan pilih disk yang akan dihapus.
4. Pilih Hapus disk.
5. Konfirmasikan bahwa Anda ingin menghapus disk Anda. Lalu, pilih Hapus.

Backup komputer virtual dan disk dengan snapshot Lightsail for Research

Snapshot adalah point-in-time salinan data Anda. Anda dapat membuat snapshot dari Amazon Lightsail for Research komputer virtual dan disk penyimpanan, dan menggunakannya sebagai garis dasar untuk membuat komputer baru atau untuk cadangan data.

Snapshot berisi semua data yang diperlukan untuk memulihkan komputer Anda (dari saat snapshot diambil). Ketika Anda membuat komputer virtual baru dari snapshot, itu dimulai sebagai replika yang tepat dari komputer asli yang digunakan untuk membuat snapshot.

Karena sumber daya Anda mungkin gagal kapan saja, sebaiknya buat snapshot yang sering untuk menghindari kehilangan data permanen.

Topik

Buat snapshot dari Lightsail for Research komputer virtual atau disk

Selesaikan langkah-langkah berikut untuk membuat snapshot dari Lightsail for Research komputer virtual atau disk Anda.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Snapshot di panel navigasi.
3. Selesaikan langkah-langkah berikut:
   - Di bawah Snapshot komputer virtual, temukan nama komputer yang ingin Anda snapshot dan pilih Buat snapshot.
   - Di bawah Snapshot disk, temukan nama disk yang ingin Anda snapshot dan pilih Buat snapshot.
4. Masukkan nama untuk snapshot Anda. Karakter yang valid termasuk karakter alfanumerik, angka, titik, tanda hubung, dan garis bawah.

Nama snapshot juga harus memenuhi persyaratan berikut:

- Jadilah unik Wilayah AWS di masing-masing akun Lightsail for Research Anda.
- Berisi 2—255 karakter.
- Mulai dan akhiri dengan karakter atau angka alfanumerik.

5. Pilih Buat snapshot.

Lihat dan kelola snapshot komputer dan disk virtual di Lightsail for Research

Selesaikan langkah-langkah berikut untuk melihat snapshot komputer dan disk virtual Anda.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Snapshot di panel navigasi.

   Halaman Snapshots menampilkan snapshot komputer dan disk virtual yang telah Anda buat.

   Snapshot yang diarsipkan juga terdapat di halaman ini. Snapshot yang diarsipkan adalah snapshot sumber daya yang telah dihapus dari akun Anda.

Buat komputer virtual atau disk dari snapshot

Selesaikan langkah-langkah berikut untuk membuat Lightsail for Research komputer virtual atau disk baru dari snapshot.

Saat Anda membuat komputer virtual dari snapshot, gunakan paket yang ukurannya sama atau lebih besar dari yang digunakan untuk komputer asli. Anda tidak dapat menggunakan paket yang lebih kecil dari komputer virtual asli.

Saat Anda membuat disk dari snapshot, pilih ukuran disk yang lebih besar dari disk asli. Anda tidak dapat menggunakan disk yang lebih kecil dari aslinya.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Snapshot di panel navigasi.

3. Pada halaman Snapshots, cari nama snapshot komputer atau disk yang akan Anda gunakan untuk membuat komputer atau disk baru. Pilih menu dropdown Snapshots untuk melihat daftar snapshot yang tersedia untuk sumber daya tersebut.
4. Pilih snapshot yang ingin Anda gunakan untuk membuat komputer virtual.
5. Pilih menu dropdown Actions. Kemudian, pilih Buat komputer virtual atau Buat disk.

Menghapus snapshot di konsol Lightsail for Research

Selesaikan langkah-langkah berikut untuk menghapus snapshot.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Snapshot di panel navigasi.
3. Pada halaman Snapshots, cari nama komputer atau snapshot disk yang ingin dihapus. Pilih menu dropdown Snapshots untuk melihat daftar snapshot yang tersedia untuk sumber daya tersebut.
4. Pilih snapshot yang ingin Anda hapus.
5. Pilih menu dropdown Actions. Kemudian, pilih Hapus snapshot.
6. Verifikasi bahwa nama snapshot sudah benar. Kemudian, pilih Hapus snapshot.

Estimasi biaya dan penggunaan di Lightsail for Research

Amazon Lightsail for Research menawarkan perkiraan biaya dan penggunaan untuk sumber daya Anda. AWS Anda dapat menggunakan perkiraan ini untuk membantu Anda merencanakan pengeluaran Anda, menemukan peluang penghematan biaya, dan membuat keputusan berdasarkan informasi saat menggunakan Lightsail for Research.

Saat Anda membuat komputer virtual atau disk, perkiraan biaya dan penggunaan ditampilkan untuk sumber daya tersebut. Estimasi biaya dan penggunaan mulai melacak segera setelah sumber daya dibuat, dan berada dalam status Tersedia atau Berjalan. Perkiraan akan muncul di AWS Management Console dalam waktu 15 menit setelah sumber daya dibuat. Sumber daya yang telah dihapus tidak termasuk dalam perkiraan.

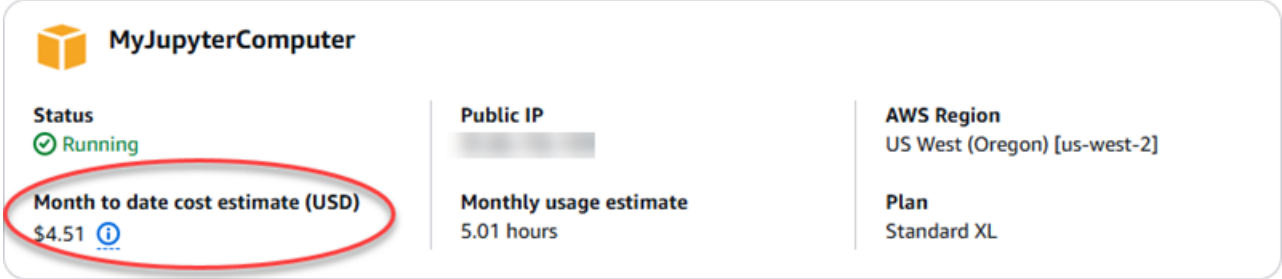
> **Important**
>
> Perkiraan adalah perkiraan biaya yang didasarkan pada penggunaan sumber daya. Biaya aktual Anda akan didasarkan pada penggunaan sumber daya Anda yang sebenarnya, bukan perkiraan yang ditampilkan di konsol Lightsail for Research. Biaya aktual ditampilkan pada laporan AWS Billing akun Anda.
> Masuk ke Konsol Manajemen AWS dan buka AWS Manajemen Penagihan dan Biaya konsol di https://console.aws.amazon.com/costmanagement/.

Topik

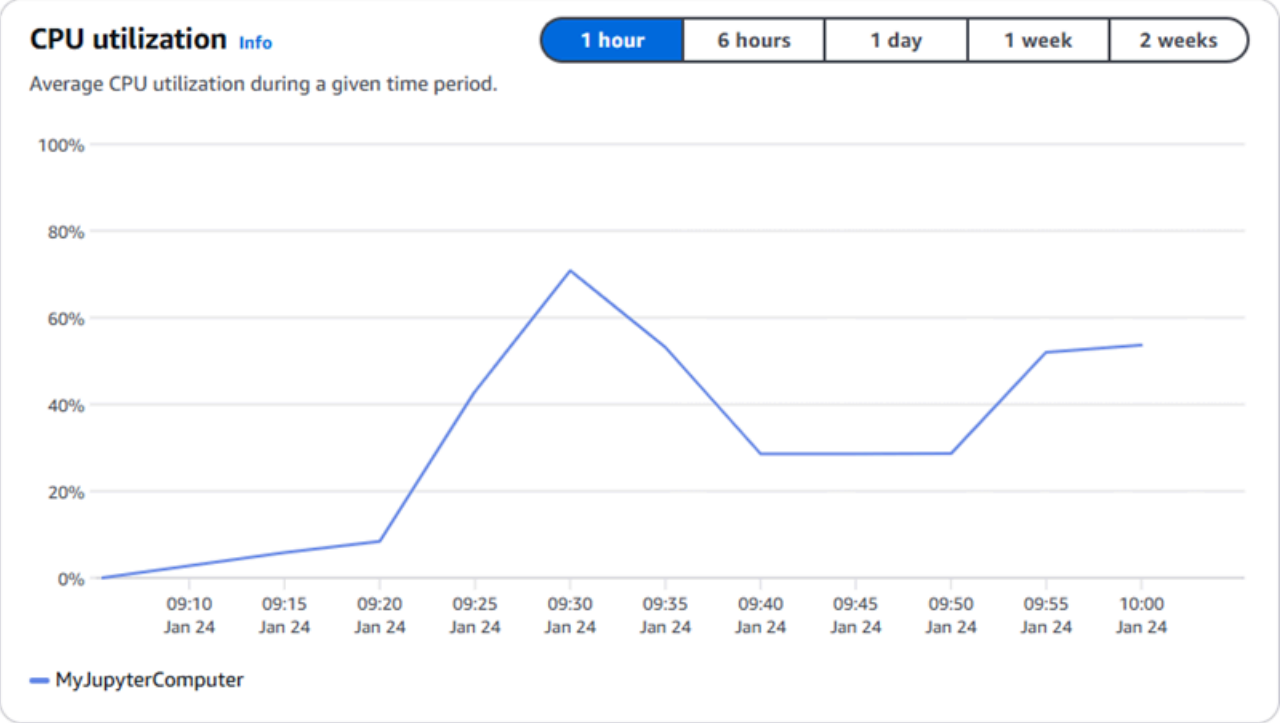
Lihat perkiraan biaya dan penggunaan untuk sumber daya Anda di Lightsail for Research

Perkiraan biaya dan penggunaan bulan hingga saat ini untuk sumber daya Lightsail for Research ditampilkan di area berikut di konsol Lightsail for Research.

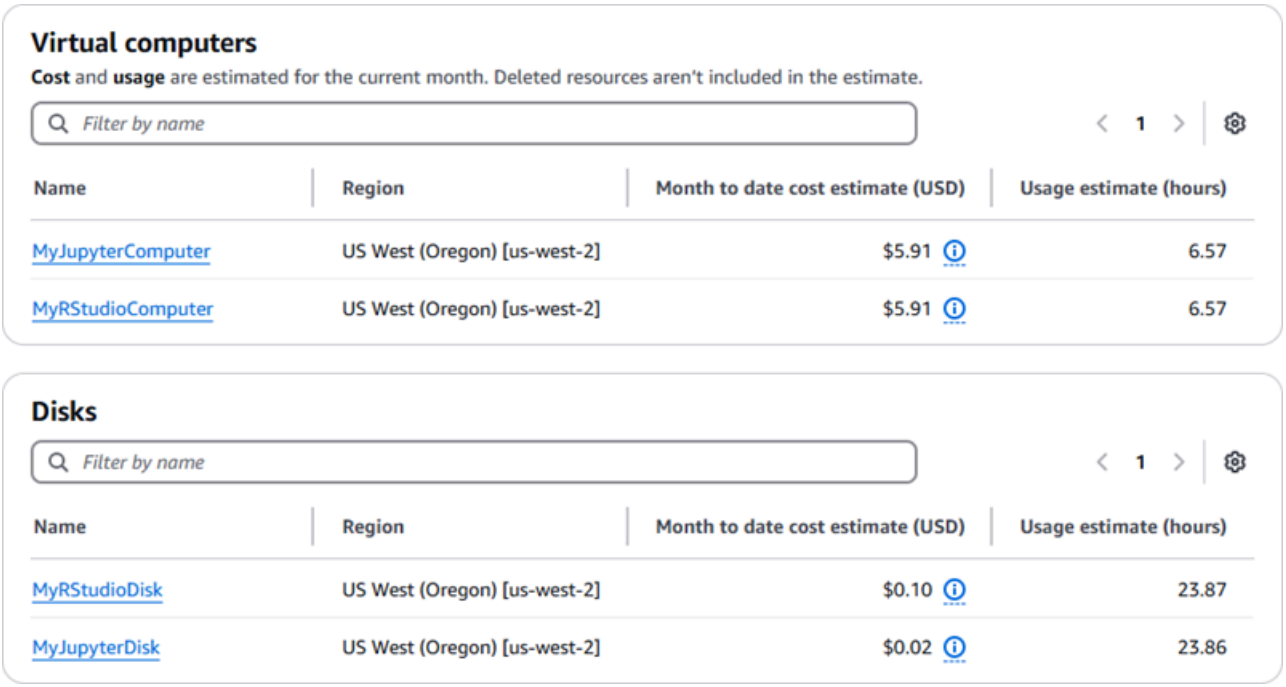
1. Pilih Komputer virtual di panel navigasi konsol Lightsail for Research. Perkiraan biaya bulan hingga saat ini untuk komputer virtual Anda tercantum di bawah setiap komputer virtual yang berjalan.



2. Untuk melihat pemanfaatan CPU untuk komputer virtual, pilih nama komputer virtual, lalu pilih tab Dasbor.



3. Untuk melihat perkiraan biaya dan penggunaan bulan hingga saat ini untuk semua sumber daya Lightsail for Research, pilih Penggunaan di panel navigasi.



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

Mengelola aturan pengendalian biaya di Lightsail for Research

Kontrol biaya menggunakan aturan yang Anda tetapkan untuk membantu mengelola penggunaan dan biaya komputer virtual Lightsail for Research Anda.

Anda dapat membuat Stop komputer virtual pada aturan idle yang menghentikan komputer yang berjalan ketika mencapai persentase tertentu dari penggunaan CPU-nya selama periode tertentu. Misalnya, aturan dapat secara otomatis menghentikan komputer tertentu ketika pemanfaatan CPU-nya sama dengan atau kurang dari 5% selama periode 30 menit. Ini menandakan bahwa komputer dalam keadaan idle, dan Lightsail for Research menghentikan komputer. Anda tidak lagi dikenakan biaya per jam standar setelah komputer virtual dihentikan.

Topik

Buat aturan kontrol biaya untuk Lightsail for Research komputer virtual

Selesaikan langkah-langkah berikut untuk membuat aturan untuk komputer virtual Lightsail for Research Anda.

> **Note**
>
> Satu-satunya tindakan aturan yang didukung saat ini adalah menghentikan komputer virtual. Pemanfaatan CPU adalah satu-satunya metrik yang saat ini dipantau oleh aturan, dan satu-satunya operasi yang didukung kurang dari atau sama dengan.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Kontrol biaya di panel navigasi.
3. Pilih Buat aturan.
4. Pilih sumber daya untuk menerapkan aturan.

5. Tentukan persentase pemanfaatan CPU dan periode waktu di mana aturan harus dijalankan.

   Misalnya, Anda dapat menentukan 5 persen dan 30 menit. Lightsail for Research secara otomatis menghentikan komputer ketika pemanfaatan CPU-nya kurang dari atau sama dengan 5 persen selama periode 30 menit.
6. Pilih Buat aturan.
7. Konfirmasikan bahwa informasi untuk aturan baru Anda sudah benar, lalu pilih Konfirmasi.

Hapus aturan kontrol biaya untuk Lightsail for Research komputer virtual

Selesaikan langkah-langkah berikut untuk menghapus aturan untuk komputer virtual Lightsail for Research Anda.

1. Masuk ke konsol Lightsail for Research.
2. Pilih Kontrol biaya di panel navigasi.
3. Pilih aturan yang akan dihapus.
4. Pilih Hapus.
5. Verifikasi bahwa Anda ingin menghapus aturan, dan pilih Hapus.

Mengatur Lightsail untuk sumber daya Penelitian dengan tag

Dengan Amazon Lightsail for Research, Anda dapat menetapkan tag ke sumber daya Anda. Setiap tag adalah label yang terdiri dari kunci dan nilai opsional yang dapat membuatnya efisien untuk mengelola sumber daya Anda. Kunci tanpa nilai disebut sebagai tag kunci saja, dan kunci dengan nilai disebut sebagai tag nilai kunci. Meskipun tidak ada jenis tag yang melekat, mereka memungkinkan Anda mengkategorikan sumber daya Anda berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Hal ini berguna jika Anda memiliki banyak sumber daya dengan jenis yang sama. Anda dapat mengidentifikasi sumber daya tertentu dengan cepat berdasarkan tag yang Anda tetapkan padanya. Misalnya, Anda dapat menentukan satu set tag yang membantu Anda melacak setiap proyek sumber daya, atau prioritas.

Sumber daya berikut dapat ditandai di konsol Amazon Lightsail for Research:

- Komputer virtual
- Disk penyimpanan
- Snapshot

Pembatasan berikut berlaku untuk tag:

- Jumlah maksimum tanda per sumber daya adalah 50.
- Untuk setiap sumber daya, setiap kunci tanda harus unik. Setiap kunci tanda hanya dapat memiliki satu nilai.
- Panjang kunci maksimum adalah 128 karakter Unicode di UTF-8.
- Panjang nilai maksimum adalah 256 karakter Unicode di UTF-8.
- Jika skema penandaan Anda digunakan di beberapa layanan dan sumber daya, harap perhatikan bahwa layanan lain mungkin memiliki pembatasan pada karakter yang diizinkan. Karakter yang diizinkan secara umum adalah: huruf, angka, dan spasi, dan karakter berikut: `+ - = . _ : / @`
- Kunci dan nilai tag peka huruf besar dan kecil.
- Jangan gunakan `aws:` awalan untuk kunci atau nilai. Awalan itu dicadangkan untuk AWS digunakan.

Topik

Tag Lightsail untuk sumber daya Penelitian

Selesaikan langkah-langkah berikut untuk membuat tag untuk komputer virtual Lightsail for Research Anda. Langkah-langkahnya serupa untuk Lightsail for Research disk dan snapshot.

1. Masuk ke konsol Lightsail for Research di konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi.
3. Pilih komputer virtual yang ingin Anda buat tag.
4. Pilih tab Tanda.
5. Pilih Kelola tanda.
6. Pilih Tambahkan tag baru.
7. Masukkan nama kunci ke dalam bidang Kunci. Misalnya, Proyek.
8. (Opsional) Masukkan nama nilai ke dalam bidang nilai. Misalnya, Blog.
9. Pilih Simpan perubahan untuk menyimpan kunci ke komputer virtual Anda.

Hapus tag dari Lightsail untuk sumber Penelitian

Selesaikan langkah-langkah berikut untuk menghapus tag dari komputer virtual Lightsail for Research Anda. Langkah-langkahnya serupa untuk Lightsail for Research disk dan snapshot.

1. Masuk ke konsol Lightsail for Research di konsol Lightsail for Research.
2. Pilih Komputer virtual di panel navigasi.
3. Pilih komputer virtual tempat Anda ingin menghapus tag.
4. Pilih tab Tanda.
5. Pilih Kelola tanda.
6. Pilih Hapus untuk menghapus tag dari sumber daya.

> **Note**
>
> Jika Anda hanya ingin menghapus Nilai tag, cari nilainya, lalu pilih ikon X yang ada di sebelahnya.

7. Pilih Simpan perubahan.

Keamanan di Amazon Lightsail untuk Penelitian

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon Lightsail for Research, AWS lihat Layanan dalam Lingkup menurut Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Lightsail for Research. Topik berikut menunjukkan cara mengonfigurasi Lightsail for Research untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Lightsail for Research Anda.

Topik

Perlindungan data di Amazon Lightsail untuk Penelitian

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon Lightsail for Research. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Lightsail for Research atau Layanan AWS lainnya menggunakan konsol, API AWS CLI, atau. AWS SDKs Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log

penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Identity and Access Management untuk Amazon Lightsail untuk Penelitian

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Lightsail for Research. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

> **Note**
>
> Amazon Lightsail dan Lightsail for Research berbagi parameter kebijakan IAM yang sama. Perubahan yang dilakukan pada kebijakan Lightsail for Research juga akan memengaruhi kebijakan Lightsail. Misalnya, jika pengguna memiliki izin untuk membuat disk di Lightsail for Research, pengguna yang sama dapat membuat disk di Lightsail juga.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Memecahkan Masalah Amazon Lightsail untuk identitas dan akses Penelitian)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Bagaimana Amazon Lightsail for Research bekerja dengan IAM)
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Contoh kebijakan berbasis identitas untuk Amazon Lightsail for Research)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredensil dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensional. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensil dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat Mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredensi sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat berupa kebijakan inline (disematkan langsung ke dalam satu identitas) atau kebijakan terkelola (kebijakan mandiri yang dilampirkan pada banyak identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — Tentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .

- Kebijakan kontrol sumber daya (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Amazon Lightsail for Research bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Lightsail for Research, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Lightsail for Research.

Fitur IAM yang dapat Anda gunakan dengan Amazon Lightsail for Research

Fitur IAM	Lightsail untuk dukungan Penelitian
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Parsial
Kredensial sementara	Ya

Fitur IAM	Lightsail untuk dukungan Penelitian
Izin principal	Tidak
Peran layanan	Tidak
Peran terkait layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara Lightsail for Research dan layanan AWS lainnya bekerja dengan sebagian besar fitur IAM, AWS lihat layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Lightsail for Research

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Lightsail for Research

Untuk melihat contoh kebijakan berbasis identitas Lightsail for Research, lihat. Contoh kebijakan berbasis identitas untuk Amazon Lightsail for Research

Kebijakan berbasis sumber daya dalam Lightsail for Research

Mendukung kebijakan berbasis sumber daya: Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan

kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Lightsail untuk Penelitian

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Lightsail for Research, lihat Tindakan yang Ditentukan oleh Amazon Lightsail untuk Penelitian dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di Lightsail for Research menggunakan awalan berikut sebelum tindakan:

```
lightsail
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

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

Untuk melihat contoh kebijakan berbasis identitas Lightsail for Research, lihat. Contoh kebijakan berbasis identitas untuk Amazon Lightsail for Research

Sumber daya kebijakan untuk Lightsail untuk Penelitian

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya Lightsail for Research dan ARNs jenisnya, lihat Sumber Daya yang Ditentukan oleh Amazon Lightsail untuk Penelitian dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang Ditentukan oleh Amazon Lightsail for Research.

Untuk melihat contoh kebijakan berbasis identitas Lightsail for Research, lihat. Contoh kebijakan berbasis identitas untuk Amazon Lightsail for Research

Kunci kondisi kebijakan untuk Lightsail for Research

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama

dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Lightsail for Research, lihat Kunci Kondisi untuk Amazon Lightsail untuk Penelitian di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang Ditentukan oleh Amazon Lightsail for Research.

Untuk melihat contoh kebijakan berbasis identitas Lightsail for Research, lihat. Contoh kebijakan berbasis identitas untuk Amazon Lightsail for Research

ACLs di Lightsail untuk Penelitian

Mendukung ACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan JSON.

ABAC dengan Lightsail untuk Penelitian

Mendukung ABAC (tag dalam kebijakan): Sebagian

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut tanda. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensil sementara dengan Lightsail for Research

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Izin utama lintas layanan untuk Lightsail for Research

Mendukung sesi akses maju (FAS): Tidak

Sesi akses teruskan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Peran layanan untuk Lightsail for Research

Mendukung peran layanan: Tidak

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas Lightsail for Research. Edit peran layanan hanya ketika Lightsail for Research memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Lightsail for Research

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul

di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Amazon Lightsail for Research

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Lightsail for Research. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Lightsail for Research, termasuk format untuk setiap jenis sumber daya, lihat Kunci Tindakan, Sumber Daya, dan Kondisi untuk Amazon Lightsail for Research dalam Referensi Otorisasi Layanan. ARNs

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Lightsail for Research
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Lightsail for Research di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi

selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan konsol Lightsail for Research

Untuk mengakses konsol Amazon Lightsail for Research, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Lightsail for Research di sumber daya Anda. Akun AWS Jika Anda membuat kebijakan berbasis

identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Lightsail for Research, lampirkan juga Lightsail for Research atau kebijakan terkelola ke entitas. *ConsoleAccessReadOnly* AWS Untuk informasi selengkapnya, lihat Menambah izin untuk pengguna dalam Panduan Pengguna IAM.

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI 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": "*"
        }
    ]
}
```

Memecahkan Masalah Amazon Lightsail untuk identitas dan akses Penelitian

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Lightsail for Research dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Lightsail for Research
- Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Lightsail for Research saya

Saya tidak berwenang untuk melakukan tindakan di Lightsail for Research

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya *`my-example-widget`* rekaan, tetapi tidak memiliki izin `lightsail:`*`GetWidget`* rekaan.

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

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `lightsail:`*`GetWidget`*.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Lightsail for Research saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACLs), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Lightsail for Research mendukung fitur-fitur ini, lihat. Bagaimana Amazon Lightsail for Research bekerja dengan IAM
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk Amazon Lightsail untuk Penelitian

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi

selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat Dokumentasi AWS Keamanan.

Ketahanan di Amazon Lightsail untuk Penelitian

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, Lightsail for Research menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda. Untuk informasi selengkapnya, lihat Backup komputer virtual dan disk dengan snapshot Lightsail for Research dan Buat snapshot dari Lightsail for Research komputer virtual atau disk.

Keamanan infrastruktur di Amazon Lightsail untuk Penelitian

Sebagai layanan terkelola, Amazon Lightsail for Research dilindungi oleh keamanan jaringan global AWS . Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Lightsail for Research melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan principal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Analisis konfigurasi dan kerentanan di Amazon Lightsail for Research

Konfigurasi dan kontrol TI adalah tanggung jawab bersama antara AWS dan Anda, pelanggan kami. Untuk informasi lebih lanjut, lihat model tanggung jawab AWS bersama.

Praktik terbaik keamanan untuk Amazon Lightsail for Research

Lightsail for Research menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau tidak memadai untuk lingkungan Anda, perlakukan itu sebagai pertimbangan yang bermanfaat, bukan sebagai resep.

Untuk mencegah potensi peristiwa keamanan yang terkait dengan penggunaan Lightsail for Research, ikuti praktik terbaik berikut:

- Akses konsol Lightsail for Research dengan mengautentikasi ke konsol pertama. Konsol Manajemen AWS Jangan berbagi berbagi kredenal konsol pribadi Anda. Siapa pun di internet dapat menjelajah ke konsol, tetapi mereka tidak dapat masuk atau memulai sesi kecuali mereka memiliki kredensil yang valid ke konsol.

Riwayat dokumen untuk Panduan Pengguna Lightsail for Research

Tabel berikut menjelaskan rilis dokumentasi untuk Lightsail for Research.

Perubahan	Deskripsi	Tanggal
Rilis awal	Rilis awal Panduan Pengguna Lightsail for Research.	28 Februari 2023

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.